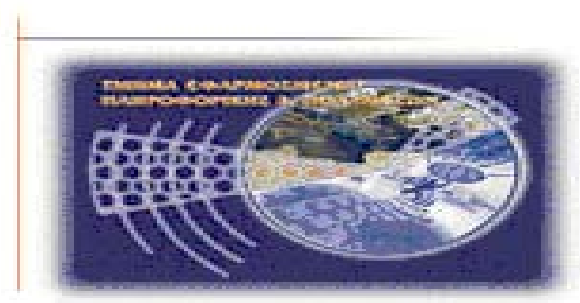
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή Εργασία

«Ηλεκτρονικό εμπόριο, Έξυπνες Κάρτες

&

Ασφάλεια Συναλλαγών »

Ξουραφάς Γεώργιος Α.Μ 271

Σπυροπούλου Δέσποινα Α.Μ 702

Ηράκλειο 17-09-2008

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

ΠΕΡΙΕΧΟΜΕΝΑ

Κεφαλαιο 3 ο

Ευρέως Διαδεδομένα Κρυπτογραφικά Συστήματα

3.1 Data Encryption Standard (DES)

3.1.1 Ιστορία του DES

3. 2 Περιγραφή του DES

3.2.1 Κρυπταναλυτικές μέθοδοι

3.2.2 Η αρχική μετάθεση

3.2.3 Τα κουτιά αντικατάστασης (S-boxes)

3.2.4 Το κουτί μετάθεσης (P-box)

3.2.5 Η τελική μετάθεση

3.3 Αποκρυπτογράφηση του DES

3.4 Τρόποι λειτουργίας του DES (modes)

3.5 Ασφάλεια του DES

3.5.1 Αδύναμα κλειδιά

3.5.2 Συμπληρωματικά κλειδιά

3.5.3 Μήκος κλειδιού

3.6 Διαφορική και γραμμική κρυπτανάλυση (differential and linear cryptanalysis)

3.6.1 Διαφορική κρυπτανάλυση

3.6.2 Κρυπτανάλυση συσχετιζόμενων κλειδιών

Κεφαλαιο 4ο

Η Ανάγκη Προστασίας Των Δικτύων & Αρχιτεκτονική Ασφάλειας Internet

Ασφαλεια δικτύων και ασφαλείς συναλλαγές

4.1 Η σημασία των δικτύων

4.1.1 Η κοινωνία της πληροφορίας

4.1.2 Το ηλεκτρονικό εμπόριο

4.2 Πρωτόκολλα ασφάλειας επιπέδου μεταφοράς

4.2.1 ΤΟ ΠΡΩΤΟΚΟΛΛΟ Secure Shell

4.2.2 ΤΟ ΠΡΟΤΟΚΟΛΛΟ SSL/TLS

4.3 Ηλεκτρονικό χρήμα

4.4 Πληρωμές με πιστωτικές κάρτες

4.4.4 Μικροπληρωμές

4.5 Ασφάλεια EDI

Κεφάλαιο 5ο

Τεχνολογία Έξυπνων Καρτών

ΠΕΡΙΛΗΨΗ ΠΤΥΧΙΑΚΗΣ

Η εργασία αυτή έχει ως στόχο, πρώτα, να μας εισαγάγει στις βασικές έννοιες της Κρυπτογραφίας όπως Κρυπτογραφία, Κρυπτανάλυση, Κρυπτολογία, Κρυπτογραφικός αλγόριθμος και σύστημα, Κρυπτογράφηση, Αποκρυπτογράφηση,

Κρυπτογραφικό Κλειδί, Κρυπτογραφικοί Μηχανισμοί και Πρωτόκολλα, Ψηφιακές

Υπογραφές και Συναρτήσεις Κατακερματισμού,της ασφάλειας των δικτύων και την ραγδαία εξέλιξη των e-commerce ιστοτόπων και, στη συνέχεια, να μας εισάγει στο κόσμο του ηλεκτρονικού εμπορίου.

Η συνεχώς αυξανόμενη εμπορευματοποίηση του Internet, και η χρήση του Web έχουν ωθήσει τις επιχειρήσεις στην εύρεση μεθόδων και συστημάτων πληρωμών για την υποστήριξη του Ηλεκτρονικού Εμπορίου. Η πρακτική εφαρμογή του Ηλεκτρονικού Εμπορίου στο σύγχρονο επιχειρηματικό περιβάλλον απαιτεί την ύπαρξη συστημάτων ηλεκτρονικών πληρωμών μέσο των οποίων θα διεκπεραιώνονται ηλεκτρονικά οι οφειλές των εμπλεκόμενων μερών. Ήδη έχουν υιοθετηθεί διάφορα συστήματα ηλεκτρονικών πληρωμών (π.χ. πιστωτικές κάρτες ηλεκτρονικό χρήμα κλπ) κατάλληλα για την εξυπηρέτηση των συναλλαγών, ενώ επίσης υπάρχουν πρότυπα ασφάλειας και προστασίας

Το οποίο συνεπάγεται ότι στην εργασία αυτή θα παρουσιαστούν και θα αναλυθούν έννοιες και τρόποι χρησιμοποίησης του διαδικτύου για συναλλαγές και αγορές όπου πρωταρχικό ρόλο παίζουν η προστασία προσωπικών δεδομένων αφού ο χρήστης εκθέτει κατά την επικοινωνία του με ένα ηλεκτρονικό κατάστημα ευαίσθητα δεδομένα τα οποία για σοβαρούς λόγους δε πρέπει να πέσουν στην αντίληψη και χρήση προσώπων χωρίς εξουσιοδότηση, ενώ επίσης θα δώσουμε ιδιαίτερο βάρος στο βασικό κομμάτι του ηλεκτρονικού εμπορίου που είναι η συναλλαγή, το οποίο περιλαμβάνει αποστολή δεδομένων χρηματικού λογαριασμού ή κωδικού κάρτας και τις δικλίδες ασφαλείας που προσφέρει ή μπορεί να προσφέρει ένα ηλεκτρονικό κατάστημα ώστε η συναλλαγή αυτή να γίνει επιτυχής και φυσικά με ασφάλεια.

Επίσης γίνεται αναφορά για την ασφαλή χρήση καρτών και ιδιαιτέρως γίνεται ανάλυση της χρήσης έξυπνων καρτών οι οποίες εκτός από την κοινή τους χρήση ως ηλεκτρονικό πορτοφόλι μπορούν να χρησιμοποιηθούν ευρύτερα στη σύγχρονη κοινωνία που ζούμε σε αρκετές εφαρμογές.

Τέλος η εργασία αυτή συνοδεύεται από ένα ηλεκτρονικό κατάστημα με τις αντίστοιχες οδηγίες κατασκευής του ,το οποίο ξεκινά με ασφαλή είσοδο του πελάτη

Και τελειώνει με την επίτευξη ασφαλούς συναλλαγής και φυσικά της χρέωσης του. Με τη χρήση κρυπτογράφησης δεδομένων DES και των πρωτοκόλλων και προτύπων τα οποία εκθέτουμε στην αντίστοιχη ενότητα.

ΚΕΦΑΛΑΙΟ 1ο

Κρυπτογραφία & Αναγκαιότητα αυτής

Εισαγωγικές παρατηρήσεις

1.1 Κρυπτογραφία και Κρυπτανάλυση

1.1.1 Βασικοί Όροι

Κρυπτογραφία είναι ο επιστημονικός κλάδος που πραγματεύεται τη μελέτη και σχεδίαση κρυπτογραφικών τεχνικών, συστημάτων και πρωτοκόλλων. Μαζί με τον κλάδο της **Κρυπτανάλυσης**, που ασχολείται με τη μελέτη τρόπων παραβίασης αυτών, απαρτίζουν την Επιστήμη της **Κρυπτολογίας**.

Η επιθυμία προστασίας του περιεχομένου μηνυμάτων οδήγησε στην επινόηση και χρήση κρυπτογραφικών τεχνικών και συστημάτων τα οποία επιτρέπουν το μετασχηματισμό μηνυμάτων ή δεδομένων κατά τέτοιον τρόπο ώστε να είναι αδύνατη η υποκλοπή του περιεχομένου τους κατά τη μετάδοσή ή αποθήκευσή τους και, βεβαίως, την αντιστροφή του μετασχηματισμού. Η διαδικασία μετασχηματισμού καλείται **κρυπτογράφηση** και η αντίστροφή της **αποκρυπτογράφηση**.

Η συνάρτηση ή το σύνολο των κανόνων, στοιχείων και βημάτων που καθορίζουν την κρυπτογράφηση και την αποκρυπτογράφηση ονομάζεται **κρυπτογραφικός αλγόριθμος**. Η υλοποίηση του κρυπτογραφικού αλγόριθμου καλείται **κρυπτογραφικό σύστημα.** Μερικές φορές, ο κρυπτογραφικός αλγόριθμος καλείται και **κωδικοποιητής (cipher)**. Πρωτόκολλα που χρησιμοποιούν κρυπτογραφικούς αλγόριθμους καλούνται **κρυπτογραφικά πρωτόκολλα**. Επειδή η αποθήκευση μπορεί να θεωρηθεί ως μετάδοση στη διάσταση του χρόνου, εφεξής θα μιλάμε για μετάδοση εννοώντας μετάδοση ή αποθήκευση.

1.1.2 Κρυπτογραφικοί Αλγόριθμοι

Οι κρυπτογραφικοί αλγόριθμοι χρησιμοποιούν, κατά κανόνα, (κρυπτογραφικά) **κλειδιά (keys)**, η τιμή των οποίων επηρεάζει την κρυπτογράφηση και την αποκρυπτογράφηση. Το σύνολο των δυνατών τιμών των κλειδιών λέγεται **πεδίο τιμών** αυτών **(keyspace)**. Υπάρχουν δύο κατηγορίες κρυπτογραφικών

αλγόριθμων, και κατά συνέπεια συστημάτων: **οι συμμετρικοί και οι ασύμμετροι** αλγόριθμοι.

Οι συμμετρικοί αλγόριθμοι χρησιμοποιούν το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση, και για το λόγο αυτό καλούνται, επίσης, **αλγόριθμοι μυστικού κλειδιού** ή **αλγόριθμοι μονού κλειδιού**.
Οι ασύμμετροι αλγόριθμοι χρησιμοποιούν διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση ενός μηνύματος. Αυτά είναι το ***δημόσιο κλειδί (public key)*** και το ***ιδιωτικό κλειδί (private key)***, τα οποία έχουν τις εξής πολύ σημαντικές ιδιότητες :

- Ένα μήνυμα που έχει κρυπτογραφηθεί με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το αντίστοιχο ιδιωτικό κλειδί και αντίστροφα.

- Αν μας είναι γνωστό το ένα κλειδί δεν μπορούμε να δημιουργήσουμε το άλλο κλειδί.

Η αρχική ιδέα για την κρυπτογράφηση με τη χρήση δημόσιου και ιδιωτικού κλειδιού διατυπώθηκε το 1976 και το 1977 υλοποιήθηκε το κρυπτοσύστημα *RSA*, που ήταν η πρώτη εφαρμογή ενός συστήματος κρυπτογραφίας που ήταν βασισμένο σε δημόσιο κλειδί. Το δημόσιο κλειδί δεν είναι μυστικό και μπορεί να το αποκτήσει ο οποιοσδήποτε ενδιαφέρεται, ενώ το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον κάτοχό του και δεν κοινοποιείται σε κανέναν άλλον.

Ο κάθε χρήστης κατέχει ένα ζεύγος κλειδιών, δημόσιο και ιδιωτικό, και όταν στέλνει ένα μήνυμα κωδικοποιημένο με το ιδιωτικό του κλειδί, το μήνυμα αυτό θα μπορεί να αποκωδικοποιηθεί από οποιονδήποτε γνωρίζει το δημόσιο κλειδί του, έχουμε δηλαδή πιστοποίηση του αποστολέα και ακεραιότητα του μηνύματος. Για την πρόσβαση στο ιδιωτικό κλειδί είναι απαραίτητη η χρήση μιας συνθηματικής φράσης (pass-phrase), που είναι κάτι ανάλογο του γνωστού μας κωδικού ή συνθηματικού (password), αλλά πολύ πιο ασφαλές.

Ενώ όταν ένας χρήστης στέλνει ένα μήνυμα κωδικοποιημένο με το δημόσιο κλειδί του παραλήπτη, το μήνυμα αυτό θα μπορεί να αποκωδικοποιηθεί μόνο με το αντίστοιχο ιδιωτικό του κλειδί του παραλήπτη, οπότε μόνο ο παραλήπτης θα μπορέσει να το διαβάσει και κανένας άλλος και στην περίπτωση αυτή έχουμε εμπιστευτικότητα του μηνύματος. Η ασύμμετρη κρυπτογράφηση μπορεί να παρέχει πολύ μεγαλύτερη ασφάλεια στις επικοινωνίες σε σχέση με τη συμμετρική

κρυπτογράφηση, έχει όμως το μειονέκτημα ότι οι αλγόριθμοί της είναι πολύ βραδύτεροι καθώς απαιτούνται πάρα πολλοί υπολογισμοί.

1.2 Αναγκαιότητα της Κρυπτογραφίας

1.2.1 Απειλές και επιπτώσεις παραβίασης της ασφάλειας

Οι δυνατές απόπειρες παραβίασης της ασφάλειας (απειλές), ακούσιες ή εκ προθέσεως, και οι αντίστοιχες επιπτώσεις διακρίνονται στις εξής κατηγορίες: διακοπής ή άρνησης υπηρεσίας, παρεμπόδισης, τροποποίησης, κατασκευής πλαστών αντικειμένων.

- Η ***Διακοπή (interruption)***. Τα αντικείμενα του συστήματος χάνονται, δεν είναι διαθέσιμα ή είναι μη χρησιμοποιήσιμα. Παραδείγματα είναι η ηθελημένη καταστροφή μιας συσκευής, το σβήσιμο ενός προγράμματος ή ενός αρχείου δεδομένων, ή η δυσλειτουργία του διαχειριστή αρχείων του λειτουργικού συστήματος, έτσι ώστε να μην μπορεί να βρεθεί ένα συγκεκριμένο αρχείο στο δίσκο.

- Η ***Παρεμπόδιση (interception)***. Σημαίνει πως μια μη εξουσιοδοτημένη ομάδα έχει κερδίσει το δικαίωμα πρόσβασης σε ένα αντικείμενο. Αυτή η εξωτερική ομάδα μπορεί να είναι είτε πρόσωπα, είτε προγράμματα ή ακόμα και παρέμβαση ενός άλλου πληροφοριακού συστήματος. Παραδείγματα αυτού του είδους της αποτυχίας είναι η παράνομη αντιγραφή των προγραμμάτων ή των αρχείων δεδομένων ή οι υποκλοπές των τηλεφωνημάτων για την απόκτηση δεδομένων από το δίκτυο. Παρόλο που μια απώλεια μπορεί να αποκαλυφθεί σχετικά γρήγορα, ο υποκλοπέας μπορεί να μην αφήσει καθόλου ίχνη για την ανίχνευση της ύπαρξης του.

- Εάν μια μη εξουσιοδοτημένη ομάδα όχι μόνο προσπελάσει τα δεδομένα, αλλά ανακατευτεί και με κάποια αντικείμενα, τότε μιλάμε για ***τροποποίηση (modification)***. Για παράδειγμα κάποιος μπορεί να αλλάξει τις τιμές σε μια βάση δεδομένων ή να μετατρέψει ένα πρόγραμμα έτσι ώστε να εκτελεί επιπλέον υπολογισμούς ή να τροποποιεί τα δεδομένα που μεταφέρονται ηλεκτρονικά. Είναι ακόμα δυνατό να τροποποιηθεί και το υλικό μέρος του συστήματος.

- Τέλος μια μη εξουσιοδοτημένη ομάδα μπορεί να ***κατασκευάσει (fabricate)*** πλαστά αντικείμενα. Ο εισβολέας μπορεί να προσθέσει εγγραφές σε μια υπάρχουσα βάση δεδομένων. Μερικές φορές αυτές οι προσθέσεις ανιχνεύονται σαν πλαστές, αλλά εάν έχουν γίνει περίτεχνα τότε είναι αδιαχώριστες από τα πραγματικά αντικείμενα.

1.2.2 Βασικοί Στόχοι Ασφάλειας

Στο πλαίσιο της ασφάλειας υπολογιστικών και επικοινωνιακών συστημάτων τίθενται ως βασικοί στόχοι η διατήρηση (διασφάλιση) τριών ιδιοτήτων ή χαρακτηριστικών (δηλαδή η αντιμετώπιση των αντίστοιχων κινδύνων): της «εμπιστευτικότητας», της «ακεραιότητας» και της «διαθεσιμότητας». Στη συνέχεια θα δούμε συνοπτικά τις τρεις αυτές ιδιότητες.

• ***Εμπιστευτικότητα (Confidentiality)***

Εμπιστευτικότητα είναι η ιδιότητα των δεδομένων ή πληροφοριών να είναι προσπελάσιμα μόνο από τις εξουσιοδοτημένες προς αυτά λογικά ή φυσικά αντικείμενα (π. χ. προγράμματα, άνθρωποι κ.ά.). Η εμπιστευτικότητα αναφέρεται στο περιεχόμενο ηλεκτρονικών εγγράφων ή, γενικά, αρχείων και μηνυμάτων, στην ύπαρξή τους και στην ταυτότητα αυτών που εκτελούν ενέργειες και ανταλλάσσουν μηνύματα. Επίσης, αναφέρεται στο χρόνο και την ποσό-τητα μηνυμάτων που ανταλλάσσονται. Η εμπιστευτικότητα, μερικές φορές, καλείται και «ιδιωτικότητα» ή «μυστικότητα» ή «προστασία του απορρήτου».

• ***Ακεραιότητα (Integrity)***

Η ακεραιότητα είναι η ιδιότητα των δεδομένων και πληροφοριών και των υπολογιστικών και επικοινωνιακών πόρων να τροποποιούνται μόνο από εξουσιοδοτημένες οντότητες κατά εξουσιοδοτημένο τρόπο. Η ακεραιότητα έχει να κάνει με την ακρίβεια και τη συνέπεια στη λειτουργία συστημάτων και διεργασιών. Τα δεδομένα σε κάθε σύστημα πρέπει να παραμένουν πλήρη και ορθά. Η ακεραιότητα διατηρείται όταν διατηρούνται και οι ιδιότητες: η ακρίβεια, η μη τροποποίηση ή τροποποίηση από εξουσιοδοτημένους χρήστες ή διεργασίες, με συνέπεια, κατά αποδεκτό τρόπο. Έχουν αναγνωριστεί τρεις καθοριστικές συνιστώσες του όρου ακεραιότητα: οι «εξουσιοδοτημένες ενέργειες», ο «διαχωρισμός και η προστασία αγαθών» και, τέλος, «η ανίχνευση και διόρθωση σφαλμάτων».

• ***Διαθεσιμότητα (Availability)***

Η διαθεσιμότητα είναι η ιδιότητα των δεδομένων ή πληροφοριών και των υπολογιστικών και επικοινωνιακών πόρων να είναι διαθέσιμα στους εξουσιοδοτημένους προς τούτο χρήστες σύμφωνα με τα δικαιώματά τους.

Η διαθεσιμότητα –όπως και η ακεραιότητα– είναι μια σύνθετη έννοια. Η διαθεσιμότητα αναφέρεται τόσο στα δεδομένα όσο και στις υπηρεσίες που πρέπει να παρέχονται.

Οι προσδοκίες του χαρακτηριστικού της Διαθεσιμότητας περιλαμβάνουν:

- Παρουσία του αντικειμένου και της υπηρεσίας με χρησιμοποιήσιμο τρόπο.
- Ικανότητα χειρισμού των απαιτούμενων πόρων
- Συγκεκριμένος χρόνος αναμονής.
- Κατάλληλος χρόνος διάθεσης των πόρων

Σκοπός της Διαθεσιμότητας είναι:

- Δίκαιη κατανομή των πόρων
- Έγκαιρη ανταπόκριση στη διάθεση των δεδομένων
- Ελεγχόμενη συμφωνία, δηλαδή χειρισμός δοσοληψιών, αποκλειστική πρόσβαση, χειρισμός του φαινομένου deadlock.
- Χρησιμότητα, οι πόροι και τα δεδομένα μπορούν να χρησιμοποιηθούν όπως σχεδιάστηκαν.

Πέρα από τα παραπάνω χαρακτηριστικά, στην πράξη υπάρχουν και άλλα, όπως η αυθεντικότητα, η αξιοπιστία, η δυνατότητα ελέγχου κ.α. που πρέπει να λαμβάνονται υπόψιν.

1.2.3 Μέσα προστασίας

Η διατήρηση (διασφάλιση) τριών παραπάνω ιδιοτήτων ή χαρακτηριστικών επιτυγχάνεται με την εφαρμογή φυσικών, οργανωτικών – διοικητικών και λειτουργικών μέτρων. Στα λειτουργικά μέτρα περιλαμβάνονται μηχανισμοί γνησιότητας προέλευσης και περιεχομένου, εμπιστευτικότητας, ελέγχου πρόσβασης και μη αμφι-σβήτησης. Το βασικό συστατικό στοιχείο όλων αυτών των μηχανισμών είναι τα κρυπτογραφικά συστήματα.

- ***Φυσικά μέτρα***
  Αναφέρονται στον έλεγχο φυσικής πρόσβασης στους υπολογιστικούς και επικοινωνιακούς πόρους, όπως επίσης και στην προστασία από φυσικά φαινόμενα ή ατυχήματα, όπως διαρροή νερού ή πλημμύρες, φωτιά, σεισμό κ.ά.

- ***Οργανωτικά – διοικητικά μέτρα***
  Αναφέρονται στη διαχείριση ασφάλειας, στην εκπόνηση ανάλυσης επικινδυνότητας, στην κατάρτιση σχεδίου ασφάλειας, πολιτικής ασφάλειας και σχεδίου έκτακτης ανάγκης. Τα μέτρα αυτά εξετάζονται και αναθεωρούνται σε τακτά χρονικά διαστήματα.

- ***Λειτουργικά μέτρα***
  Αναφέρονται σε όλους εκείνους τους μηχανισμούς που πρέπει να ενεργοποιούνται κατά τη λειτουργία συστημάτων υπολογιστών.

Στα μέτρα αυτά συγκαταλέγονται οι ακόλουθες κατηγορίες:

(a) της *γνησιότητας (authentication)* προέλευσης δεδομένων ή ταυτότητας χρηστών
(b) της *ακεραιότητας* ή *γνησιότητας περιεχομένου (integrity)*
(c) της *εμπιστευτικότητας (confidentiality)* του *ελέγχου πρόσβασης (access control)*
(d) της *μη αμφισβήτησης (non – repudiation)*.

Κεφάλαιο 2ο
Αριθμοθεωρία & Συμμετρικά Συστήματα Κρυπτογραφίας

2.1 Σημαντικά Αποτελέσματα

Στην υποενότητα αυτή θα θυμηθούμε ορισμένα σημαντικά, από τη σκοπιά της Κρυπτογραφίας, αποτελέσματα της Αριθμοθεωρίας. Πιο συγκεκριμένα, θα συζητήσουμε εν συντομία το **Θεώρημα του Fermat**, τη Συνάρτηση του Euler, το Θεώρημα των Euler – Fermat, το Κινέζικο Θεώρημα Υπολοίπων και τις τετραγωνικές ισοτιμίες.

Σύμφωνα με το (μικρό) Θεώρημα του Fermat, για κάθε πρώτο αριθμό, n, και για κάθε α που δεν είναι πολλαπλάσιό του ισχύει: $\alpha^n = \alpha \bmod n$ και επίσης $\alpha^{n-1} = 1 \bmod n$.

Η **Συνάρτηση του Euler**, γνωστή και ως συνάρτηση φ(n), είναι το πλήθος των στοιχείων του ανηγμένου συστήματος υπολοίπων modulo n. Με άλλα λόγια, φ(n) είναι το πλήθος των φυσικών μικρότερων ή ίσων του n οι οποίοι είναι σχετικά πρώτοι με αυτόν.

> **ΣΧΟΛΙΟ**
>
> Μια τελευταία πτυχή παρατήρησης είναι η οικονομική διάσταση των μέτρων προστασίας. Ο επιθυμητός βαθμός ασφάλειας καθορίζεται από την αξία των αγαθών στο χρόνο και το κόστος υλοποίησης των απαιτούμενων μέτρων. Παραδείγματος χάρη, δεδομένα υψηλής αξίας που αποθηκεύονται για μεγάλο χρονικό διάστημα πρέπει να προστατεύονται πολύ καλύτερα απ' ό,τι μηνύματα των οποίων η αξία παραμένει μόνο για λίγο χρόνο μετά τη μετάδοσή τους. Σε μερικές περιπτώσεις, όπως της προστασίας του τηλεοπτικού σήματος συνδρομητικών καναλιών, η ασφάλεια, δηλαδή η κρυπτογράφηση, έχει κόστος μόνο για το κανάλι. Όμως, η αποκρυπτογράφηση έχει κόστος για τους συνδρομητές. Και βέβαια οι νόμιμοι συνδρομητές δεν έχουν όφελος από την παρεχόμενη προστασία. Σε αυτή την περίπτωση είναι προτιμότερη η επιλογή της εφαρμογής ενός κρυπτογραφικού συστήματος που δεν προκαλεί αξιόλογο κόστος στους συνδρομητές. Απαιτεί όμως από μη συνδρομητές να προμηθευτούν εξοπλισμό που στοιχίζει πολύ περισσότερο από την αγορά του αποκωδικοποιητή και το μηνιαίο κόστος.

Αν ο n είναι πρώτος, τότε $\varphi(n) = n - 1$. Αν $n = pq$, όπου p και q πρώτοι, τότε $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$. (Αυτοί οι αριθμοί εμφανίζονται στους αλγόριθμους δημόσιου κλειδιού.)

Σύμφωνα με το **Θεώρημα των Euler – Fermat**, δηλαδή τη γενίκευση του Θεωρήματος του Fermat από τον Euler, αν οι a, n είναι πρώτοι μεταξύ τους, τότε ισχύει: $a^{\varphi(n)} = 1 \bmod n$.

Τώρα, εύκολα μπορούμε να υπολογίσουμε τον αντίστροφο, *x*, ενός αριθμού *a mod n*: $x = a^{\varphi(n)-1} \bmod n$. Για παράδειγμα, ο αντίστροφος του *5 mod 7* είναι το *3*, αφού το *7* είναι πρώτος, $\varphi(7) = 7 - 1 = 6$ και $5^{6-1} \bmod 7 = 5^5 \bmod 7 = 3$.

Επίσης, ένα σημαντικό για την Κρυπτογραφία αποτέλεσμα της Αριθμοθεωρίας είναι το **Κινέζικο Θεώρημα Υπολοίπων**, το οποίο αναφέρεται στις προϋποθέσεις για να έχει μοναδική λύση ένα σύστημα ισοτιμιών με έναν άγνωστο. Το θεώρημα αυτό διατυπώθηκε από έναν Κινέζο μαθηματικό του πρώτου αιώνα, τον Sun Tse.

Μπορεί να δειχτεί ότι υπάρχουν ακριβώς (p – 1)/2 **τετραγωνικά υπόλοιπα** *mod p*, τα οποία ανήκουν στις κλάσεις υπολοίπων των αριθμών $1^2, 2^2, \ldots, ((p-1)/2)^2$, όπως επίσης και τετραγωνικά μη υπόλοιπα *mod p*. Ακόμα, αν *α* είναι ένα τετραγωνικό υπόλοιπο *mod p*, τότε το *α* έχει ακριβώς δύο τετραγωνικές ρίζες: μία από αυτές ανάμεσα στο 0 και στο (p – 1)/2, και η άλλη μεταξύ (p – 1)/2 και (p – 1). Μία από αυτές τις τετραγωνικές ρίζες είναι επίσης τετραγωνικό υπόλοιπο *mod p*. Η ρίζα αυτή λέγεται βασική τετραγωνική ρίζα. Αν n είναι το γινόμενο δύο πρώτων αριθμών, των *p* και *q*, τότε υπάρχουν ακριβώς (p – 1)(q – 1)/4 τετραγωνικά υπόλοιπα mod n. Για παράδειγμα, υπάρχουν έξι τετραγωνικά υπόλοιπα *mod 35*: 1, 4, 9, 11, 16, 29. Κάθε τετραγωνικό υπόλοιπο έχει ακριβώς τέσσερις τετραγωνικές ρίζες.

Για το χαρακτηρισμό των τετραγωνικών υπολοίπων χρησιμοποιούνται τα σύμβολα των Legendre και Jacobi, τα οποία θα ορίσουμε στη συνέχεια.

Το **σύμβολο Legendre L(α,p)** ορίζεται για έναν ακέραιο *α* και έναν πρώτο αριθμό *p* μεγαλύτερο του 2 ως εξής:

$L(\alpha,p) = 0$, αν ο α διαιρείται από τον *p*.

$L(\alpha,p) = 1$, αν ο α είναι ένα τετραγωνικό υπόλοιπο *mod p*.

$L(\alpha,p) = -1$, αν ο α είναι δεν είναι τετραγωνικό υπόλοιπο *mod p*.

Ένας εύκολος τρόπος για τον υπολογισμό του L(α,p) είναι: $L(\alpha,p) = \alpha^{(p-1)/2} \bmod p$.

Ένας άλλος τρόπος υπολογισμού του συμβόλου Legendre είναι ο ακόλουθος αλγόριθμος:

1. Αν $\alpha = 1$, τότε $L(\alpha,p) = 1$,

2. Αν ο α είναι άρτιος, τότε $L(\alpha,p) = L(\alpha/2,p).(-1)^{(p^2-1)/8}$

3. Αν ο α είναι περιττός (και $\alpha \neq 1$), τότε $L(\alpha,p) = L(p \bmod \alpha,\alpha).(-1)^{(\alpha-1)(p-1)/4}$

Το **σύμβολο Jacobi J(α,n)** αποτελεί γενίκευση του συμβόλου Legendre. Είναι μια συνάρτηση στο ανηγμένο σύστημα υπολοίπων *mod n* και ορίζεται για τυχόν ζεύγος ακεραίου α και περιττού ακεραίου n ως εξής:

1. $J(a,n)$ ορίζεται μόνο αν n είναι περιττός αριθμός.

2. $J(0,n) = 0$.

3. $J(\alpha,n) = 0$, αν ο α διαιρείται από τον n και ο n είναι πρώτος αριθμός.

4. $J(\alpha,n) = 1$, αν n είναι πρώτος και ο α είναι ένα τετραγωνικό υπόλοιπο *mod n*

5. $J(\alpha,n) = -1$, αν ο n είναι πρώτος και ο α δεν είναι ένα τετραγωνικό υπόλοιπο *mod n.*

2.1.1 Ανάλυση Φυσικού Αριθμού σε Γινόμενο Πρώτων

Το πρόβλημα της ανάλυσης ενός φυσικού αριθμού n σε γινόμενο πρώτων είναι ένα από τα πιο παλιά στην Αριθμοθεωρία. Προφανώς, ελέγχοντας με τη σειρά τους πρώτους αριθμούς που διαιρούν τον n, μπορούμε να οδηγηθούμε στο γινόμενο πρώτων παραγόντων του. Ωστόσο, αυτός ο τρόπος προσέγγισης δεν είναι δυνατός για ιδιαίτερα μεγάλους αριθμούς, οι οποίοι άλλωστε έχουν πρακτική αξία στην Κρυπτογραφία.

Για την ανάλυση ενός αριθμού σε γινόμενο πρώτων παραγόντων μπορεί να χρησιμοποιηθούν διάφοροι αλγόριθμοι. Στους πιο αποτελεσματικούς αλγόριθμους συγκαταλέγεται ο «Quadratic Sieve» [POM1984] και ο «Number Field Sieve – NFS» ([LEN1990], [ADL1991]). Για την ανάλυση ενός φυσικού αριθμού 116 δεκαδικών ψηφίων απαιτήθηκε παλαιότερα ανενεργός χρόνος διασυνδεδεμένων υπολογιστών για μερικούς μήνες ισοδύναμης υπολογιστικής ισχύος ενός υπολογιστή με 400 MIPS (Million Instructions Per Second) σε λειτουργία ενός χρόνου. Η ανάλυση φυσικών αριθμών 155 δεκαδικών ψηφίων (512 bits), ή και μεγαλύτερων ακόμα, είναι δυνατή με τον αλγόριθμο NFS, ιδιαίτερα με την αξιοποίηση της τεράστιας υπολογιστικής ισχύος πολυεπεξεργαστών και πολυυπολογιστικών συστημάτων.

Αν *n* είναι το γινόμενο δύο πρώτων αριθμών, τότε ο υπολογισμός τετραγωνικών ριζών *mod n* είναι υπολογιστικά ισοδύναμος με την ανάλυση του *n* σε γινόμενο πρώτων. Με άλλα λόγια, αν γνωρίζουμε τους πρώτους παράγοντες του *n*, μπορούμε εύκολα να υπολογίσουμε τις τετραγωνικές ρίζες ενός αριθμού *mod n*. Αν, όμως, δε γνωρίζουμε αυτούς τους παράγοντες, θα αντιμετωπίσουμε την ίδια δυσκολία που έχει η ανάλυση του *n* σε γινόμενο πρώτων παραγόντων.

2.1.2 Δημιουργία (Ψευδο-) Πρώτων Αριθμών

Οι πρώτοι αριθμοί χρησιμοποιούνται κυρίως στα ασύμμετρα κρυπτογραφικά συστήματα, και επομένως και στα συστήματα ηλεκτρονικών υπογραφών που βασίζονται σ' αυτά. Βέβαια, λαμβάνοντας υπόψη την αναμενόμενη ευρεία εφαρμογή συστημάτων ηλεκτρονικών υπογραφών, συμπεραίνουμε ότι θα απαιτηθεί η εύρεση και χρήση πάρα πολλών πρώτων αριθμών. Για το λόγο αυτό μπορεί να αναρωτηθούμε αν υπάρχουν αρκετοί πρώτοι αριθμοί για όλες τις εφαρμογές.

Στην περίπτωση που ένας αριθμός *n*, παρ' όλο που δεν είναι πρώτος, περνά τον έλεγχο με βάση κάποιον φυσικό *a*, τότε ο *n* ονομάζεται **ψευδοπρώτος** με βάση *a*.

Στη συνέχεια θα εξετάσουμε τρεις αλγόριθμους που χρησιμοποιούνται στην πράξη: τον Αλγόριθμο Solovay – Strassen, τον Αλγόριθμο Rabin – Miller και τον Αλγόριθμο Lehmann.

Ο **Αλγόριθμος των Solovay – Strassen** χρησιμοποιεί το σύμβολο του Jacobi. Σύμφωνα με αυτό τον αλγόριθμο, για να ελεγχθεί αν ένας φυσικός *n* είναι πρώτος ακολουθούνται τα εξής βήματα:

1. Επιλογή τυχαίου φυσικού *α*, μικρότερου του *n*.

2. Αν οι *α* και *n* δεν είναι σχετικά πρώτοι μεταξύ τους,
   δηλαδή $\mu\kappa\delta(\alpha,n) \neq 1$, ο *n* είναι σύνθετος και δεν περνά το τεστ.

3. Υπολογισμός του $m = \alpha^{(n-1)/2} \bmod n$. (Αν *n* πρώτος, τότε $m = L(a,n)$.)

4. Υπολογισμός του $J(\alpha,n)$.

5. Αν $m \neq J(\alpha,n)$, τότε ο *n* σίγουρα δεν είναι πρώτος.

6. Αν $m = J(\alpha,n)$, τότε η πιθανότητα ο n να μην είναι πρώτος είναι μικρότερη από 0,5.

7. Επανάληψη αυτού του ελέγχου k φορές, με k διαφορετικές τυχαίες τιμές για το α. Η πιθανότητα ένας σύνθετος αριθμός να περάσει και τους k έλέγχους δεν ξεπερνά το 2^{-k}.

Αν ένας αριθμός n ενώ δεν είναι πρώτος περνά τον έλεγχο $\alpha^{(n-1)/2} \bmod n = J(\alpha,n)$ για κάποιον φυσικό a, τότε ο n ονομάζεται **Euler ψευδοπρώτος** ως προς βάση a. Οι Euler ψευδοπρώτοι είναι ισχυρότεροι των ψευδοπρώτων, αφού ένας Euler ψευδοπρώτος είναι και ψευδοπρώτος, ενώ το αντίστροφο δεν ισχύει (Κεφάλαιο 4 [ΓΑΛ2001]).

Ο **Αλγόριθμος των Rabin – Miller** αναπτύχθηκε από τον Rabin και βασίστηκε σε μια ιδέα του Miller ([MIL1976], [RAB1980]). Καταρχήν επιλέγεται, όπως και στους άλλους αλγόριθμους, ο φυσικός n που θα ελεγχθεί αν είναι πρώτος. Υπολογίζεται ο αριθμός q, που είναι η μεγαλύτερη δύναμη του 2, τέτοια ώστε το 2^q να διαιρεί το $n-1$, και ο αριθμός m, τέτοιος ώστε $k = 1 + 2^q m$, όπου k είναι το πλήθος των επαναλήψεων του ελέγχου.

2.2 Δημιουργία τυχαίων και ψευδό-τυχαίων ακολουθιών

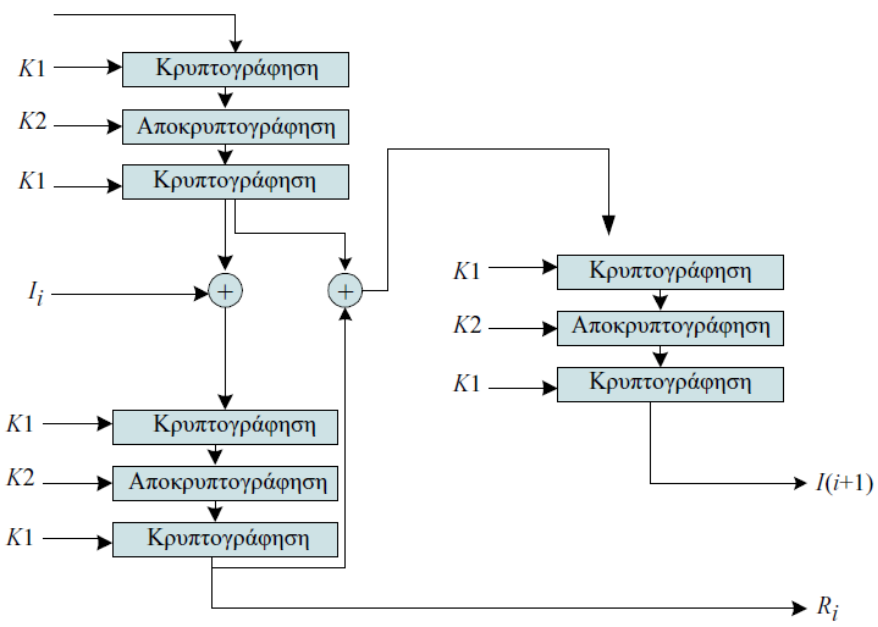
Γιατί, όμως γίνεται τόσος λόγος για ***γεννήτριες τυχαίων αριθμών (random-number generators)*** ή ***γεννήτριες τυχαίων ακολουθιών (random-sequence generators)***;

Είναι αλήθεια ότι σε κάθε γλώσσα προγραμματισμού υπάρχει ενσωματωμένη μια συνάρτηση που έχει ως σκοπό ακριβώς αυτό: την δημιουργία τυχαίων αριθμών. Δυστυχώς όμως, αυτές οι γεννήτριες δεν είναι αρκετά ασφαλείς για την κρυπτογραφία, γιατί το αποτέλεσμα που δίνουν δεν είναι αρκετά τυχαίο.

Οι γεννήτριες τυχαίων αριθμών δεν είναι τυχαίες γιατί δεν χρειάζεται να είναι. Οι περισσότερες εφαρμογές χρειάζονται τόσο λίγους τυχαίους αριθμούς, που είναι υπέρ-ικανοποιημένες με τις γεννήτριες αυτές. Η κρυπτογραφία, όμως, είναι εξαιρετικά ευαίσθητη στο θέμα των τυχαίων αριθμών και απαιτεί η παραγωγή τους να γίνεται με πραγματικά τυχαίο τρόπο.

Αν η γεννήτρια δεν έχει τα χαρακτηριστικά που απαιτεί η κρυπτογραφία, τότε μπορούν να γίνουν συσχετισμοί ανάμεσα στα διαφορετικά αποτελέσματα και αυτό είναι ανεπίτρεπτο.

Το ότι οι γεννήτριες αυτές δεν μας δίνουν αριθμούς με πραγματικά τυχαία χαρακτηριστικά είναι λογικό, επειδή βασίζονται στους υπολογιστές. Οι υπολογιστές είναι ντετερμινιστικά τέρατα: βάζουμε δεδομένα από τη μια μεριά, ο υπολογιστής επιδρά πάνω τους με τελείως προβλέψιμο τρόπο, και παίρνουμε νέα δεδομένα από την άλλη. Πιο συγκεκριμένα, οι υπολογιστές είναι ντετερμινιστικά πεπερασμένα αυτόματα (deterministic finite automata). Υπάρχει ένα πεπερασμένο σύνολο καταστάσεων στις οποίες μπορούν να βρίσκονται κάθε στιγμή. Τα δεδομένα εξόδου θα είναι πάντα μια ντετερμινιστική συνάρτηση των δεδομένων εισόδου. Έτσι, κάθε υλοποίηση γεννήτριας τυχαίων αριθμών σε υπολογιστή, θα είναι εκ των πραγμάτων περιοδική. Οτιδήποτε έχει την ιδιότητα του περιοδικού είναι εξ ορισμού προβλέψιμο. Και αν κάτι είναι προβλέψιμο, δεν είναι τυχαίο. Επομένως μια γεννήτρια τυχαίων αριθμών χρειάζεται τυχαία δεδομένα, κάτι που δεν μπορεί να προσφέρει ο υπολογιστής.



Σχήμα 3.2
Η γεννήτρια (ψευδο –) τυχαίων αριθμών ANSI X9.17

2.2.1 Ψευδό-τυχαίες ακολουθίες (pseudo-random sequences)

Το καλύτερο που μπορεί να μας προσφέρει ένας υπολογιστής είναι μια γεννήτρια ψευδό-τυχαίων ακολουθιών (pseudo-random-sequence generator). Ψευδό-τυχαία ακολουθία είναι αυτή που δείχνει τυχαία.

Η περίοδος της ακολουθίας (ο αριθμός των bit μετά τον οποίο αρχίζει και επαναλαμβάνεται) πρέπει να είναι αρκετά μεγάλη έτσι ώστε μία ακολουθία bit λογικού μήκους (τέτοιου που να ικανοποιεί τις περισσότερες εφαρμογές) να μην είναι περιοδική. Έτσι, αν χρειαζόμαστε 1 δις τυχαίων bit, δεν μας κάνει μια γεννήτρια που επαναλαμβάνεται κάθε 16 χιλιάδες bit.

Η ακολουθία με μήκος μια περίοδο θα πρέπει να πληροί, κατά το δυνατόν, τα χαρακτηριστικά μιας τυχαίας ακολουθίας. Για παράδειγμα, θα πρέπει να έχει τον ίδιο αριθμό μηδέν και ένα. Οι μισές από τις υπό-ακολουθίες με ίδια όλα τους τα στοιχεία θα πρέπει να είναι μήκους ένα, το ένα τέταρτο αυτών να είναι μήκους δύο, το ένα όγδοο μήκους τρία, κοκ. Η κατανομή αυτών των υπό-ακολουθιών θα πρέπει να είναι ίδια για το μηδέν και το ένα. Δεν θα πρέπει η ακολουθία να είναι συμπιεστή. Αυτές οι ιδιότητες μπορούν εμπειρικά να μετρηθούν και έπειτα να συγκριθούν με τις στατιστικές μας απαιτήσεις με τη μέθοδο του χ2.

Για τις ανάγκες μας, μια γεννήτρια είναι ψευδό-τυχαία αν έχει την παρακάτω ιδιότητα:

1. Παράγει ακολουθίες που δείχνουν τυχαίες. Αυτό σημαίνει ότι περνούν όλα τα στατιστικά τεστ που μπορούμε να σκεφτούμε.

Μεγάλη βάση έχει δοθεί στην δημιουργία καλών ψευδό-τυχαίων γεννητριών για υπολογιστές. Όλες οι γεννήτριες είναι περιοδικές, αλλά με περίοδο 2256 ή και μεγαλύτερη, κάνουν για τις περισσότερες εφαρμογές.

Το πρόβλημα όμως παραμένει να είναι οι περίεργοι συσχετισμοί ανάμεσα στα διαδοχικά αποτελέσματα που δίνει η γεννήτρια. Αυτό το στοιχείο θα εκμεταλλευτεί ο κρυπταναλυτής για να προσβάλει το σύστημα.

2.2.2 Κρυπτογραφικά ασφαλείς ψευδό-τυχαίες ακολουθίες

Οι κρυπτογραφικές εφαρμογές απαιτούν πολύ περισσότερα απ’ ότι οι περισσότερες άλλες εφαρμογές. «Κρυπτογραφικά τυχαίο» δεν σημαίνει απλά «στατιστικά τυχαίο», αν και αυτό είναι μέρος του ορισμού. Για να είναι μια ψευδό-τυχαία ακολουθία κρυπτογραφικά ασφαλής (cryptographically secure pseudo-random sequence) θα πρέπει να πληροί και την παρακάτω ιδιότητα:

2. Η ακολουθία θα πρέπει να είναι απρόβλεπτη. Θα πρέπει να είναι υπολογιστικά αδύνατο να προβλέψουμε το επόμενο bit της ακολουθίας, έχοντας πλήρη γνώση του αλγόριθμου (ή του μηχανήματος) που παράγει την ακολουθία και όλων των προηγούμενων bit.

Οι κρυπτογραφικά ασφαλής ψευδό-τυχαίες ακολουθίες δεν πρέπει να είναι συμπιεστές, εκτός κι αν γνωρίζουμε το κλειδί, που γενικά είναι η αναπαραγωγική δομή (seed) που χρησιμοποιήσαμε για να αρχικοποιήσουμε την γεννήτρια.

Όπως ακριβώς οι αλγόριθμοι κρυπτογραφίας, έτσι και οι κρυπτογραφικά ασφαλής ψευδό-τυχαίες γεννήτριες μπορούν να γίνουν αντικείμενα επίθεσης και να σπαστούν από την κρυπτανάλυση.

2.3 Πραγματικά τυχαίες ακολουθίες

Εδώ μπαίνουμε στη σφαίρα της φιλοσοφίας. Υπάρχει η έννοια του «τυχαίου»; Τι είναι «τυχαία ακολουθία»; Είναι το «101110100» πιο τυχαίο από το «101010101»; Η κβαντική μηχανική υποστηρίζει ότι υπάρχει πραγματική αβεβαιότητα στον κόσμο. Αλλά, μπορούμε να μεταφέρουμε αυτή την αβεβαιότητα στο κόσμο των υπολογιστών;

Πάντως, σε ότι αφορά τις γεννήτριες ακολουθιών, πραγματικά τυχαία είναι όταν έχει την παρακάτω τρίτη ιδιότητα:

3. Η ακολουθία δεν μπορεί να αναπαραχθεί με ακρίβεια. Αν χρησιμοποιήσουμε την γεννήτρια δύο φορές με τα ίδια (όσο είναι ανθρωπίνως δυνατό) δεδομένα εισόδου, θα πάρουμε δύο τελείως άσχετες μεταξύ τους ακολουθίες.

Το αποτέλεσμα που παίρνουμε από μια πραγματικά τυχαία γεννήτρια μας κάνει για το one-time pad, την δημιουργία κλειδιών, και ικανοποιεί κάθε άλλη κρυπτογραφική εφαρμογή έχει ανάγκη από πραγματικά τυχαίες ακολουθίες.

2.4 Κρυπτογραφικά πρωτόκολλα

2.4.1 Εισαγωγή στα πρωτόκολλα

Οι αλγόριθμοι κρυπτογράφησης αποτελούν ένα σημαντικό κομμάτι της κρυπτογραφίας, αλλά είναι από μόνοι τους ανεπαρκείς για να λύσουν ένα πρόβλημα. Πρέπει να υπάρχει το κατάλληλο υπόβαθρο πάνω στο οποίο θα χρησιμοποιηθούν. Τον ρόλο αυτό παίζουν τα πρωτόκολλα.

Πρωτόκολλο (protocol) ονομάζουμε μια σειρά βημάτων, που αφορούν δύο ή περισσότερες οντότητες, σχεδιασμένα να φέρουν εις πέρας ένα έργο. Ας αναλύσουμε τον ορισμό αυτό. «Μια σειρά βημάτων» σημαίνει ότι το πρωτόκολλο είναι μια ακολουθία με αρχή και τέλος.

Κάθε βήμα πρέπει να εκτελεστεί κατά σειρά και *αφού* έχει τελειώσει η εκτέλεση του αμέσως προηγούμενου βήματος. Το ότι «αφορά δύο ή περισσότερες οντότητες» σημαίνει ότι απαιτούνται τουλάχιστο δύο πρόσωπα για να εκτελέσουν το πρωτόκολλο· το πρωτόκολλο δεν έχει νόημα για ένα άτομο. Τέλος, «σχεδιασμένο να φέρει εις πέρας ένα έργο» σημαίνει ότι το πρωτόκολλο πρέπει να επιτυγχάνει κάτι.

Τα πρωτόκολλα έχουν και άλλα χαρακτηριστικά:

- Όλοι οι μετέχοντες στην διαδικασία του πρωτοκόλλου πρέπει να γνωρίζουν το πρωτόκολλο και όλα τα βήματα από πριν.
- Όλοι οι μετέχοντες στη διαδικασία του πρωτοκόλλου πρέπει να συμφωνήσουν στην χρήση του.
- Το πρωτόκολλο πρέπει να είναι σαφές και όχι αμφιλεγόμενο· κάθε βήμα πρέπει να είναι καλά ορισμένο, χωρίς να υπάρχει περίπτωση παρεξήγησης.
- Το πρωτόκολλο πρέπει να είναι πλήρες· θα πρέπει να υπάρχουν καθορισμένες ενέργειες για κάθε δυνατή περίπτωση.

Γενικά, τα βήματα εκτελούνται γραμμικά, το ένα μετά το άλλο, εκτός κι αν υπάρχουν οδηγίες για διακλάδωση σε κάποιο συγκεκριμένο βήμα. Κάθε βήμα περιλαμβάνει τουλάχιστο μία από τις δύο παρακάτω ενέργειες: εκτέλεση υπολογισμών από ένα ή περισσότερα εκ των προσώπων, ή αποστολή μηνυμάτων ανάμεσα στα πρόσωπα.

Κρυπτογραφικό πρωτόκολλο (cryptographic protocol) είναι εκείνο που χρησιμοποιεί κρυπτογραφία. Τα πρόσωπα μπορεί να είναι φίλοι και να εμπιστεύονται τυφλά ο ένας τον άλλο ή μπορεί να είναι ορκισμένοι εχθροί. Το κρυπτογραφικό πρωτόκολλο υλοποιεί κάποιο κρυπτογραφικό αλγόριθμο, άλλα συνήθως ο στόχος του πρωτοκόλλου είναι κάτι περισσότερο από απλή μυστικότητα. Οι οντότητες μπορεί να θέλουν να υπολογίζουν από κοινού μία τυχαία ακολουθία ή να πείθουν η μια την άλλη για την ταυτότητά τους ή να υπογράφουν ταυτόχρονα ένα συμβόλαιο. Ο ρόλος της κρυπτογραφίας είναι να εμποδίζει ή να εντοπίζει τις υποκλοπές (eavesdropping) και την απάτη (cheating). Γενικά πρέπει να ισχύει το παρακάτω:

- Θα πρέπει να είναι αδύνατο να επιτευχθούν περισσότερα απ’

  όσα ορίζει το πρωτόκολλο.

Ο περιορισμός αυτός είναι πολύ δυσκολότερος απ’ ότι ακούγεται. Σε μερικά πρωτόκολλα είναι δυνατόν κάποιος από τους μετέχοντες να διαπράξει απάτη. Σε άλλα είναι δυνατόν κάποιος υποκλοπέας να παρακάμψει το πρωτόκολλο και να αποκτήσει μυστικές πληροφορίες. Όπως με τους αλγόριθμους έτσι κι εδώ είναι ευκολότερο να αποδείξουμε την έλλειψη ασφάλειας παρά το αντίθετο.

2.4.2 Ο ρόλος των πρωτοκόλλων

Στην καθημερινή μας ζωή εφαρμόζουμε ανεπίσημα πρωτόκολλα σχεδόν παντού: στα παιχνίδια, στις εκλογές, στα ψώνια κτλ. Τέτοια πρωτόκολλα έχουν εξελιχθεί με τα χρόνια, όλοι ξέρουν να τα ακολουθούν, και δουλεύουν αρκετά καλά.

Στις μέρες μας όλο και περισσότερες ανθρώπινες συναλλαγές γίνονται μέσω υπολογιστών. Οι υπολογιστές χρειάζονται αυστηρώς καθορισμένα πρωτόκολλα για να πετύχουν αυτό που ο άνθρωπος θα έκανε χωρίς πολλή σκέψη.

Πολλά καθημερινά πρωτόκολλα βασίζονται στην ζωντανή παρουσία των εμπλεκόμενων προσώπων για να διασφαλιστεί η ασφάλεια και η ορθότητά τους. Με τους υπολογιστές δεν συμβαίνει το ίδιο.

Είναι αφελές να πιστεύουμε ότι οι άνθρωποι που χρησιμοποιούν ένα δίκτυο υπολογιστών είναι νομιμόφρονες. Είναι αφελές να πιστεύουμε πως οι διαχειριστές τέτοιων δικτύων είναι νομιμόφρονες. Είναι αφελές ακόμη και να πιστεύουμε ότι οι σχεδιαστές των δικτύων είναι νομιμόφρονες. Οι περισσότεροι βέβαια είναι, άλλα οι λίγοι που δεν είναι μπορούν να προξενήσουν σημαντική ζημιά. Ο αυστηρός καθορισμός των πρωτοκόλλων μας βοηθάει να εξετάζουμε τους τρόπους με τους οποίους μπορούν να παρακαμφθούν. Έτσι μπορούμε να αναπτύξουμε πρωτόκολλα που αποτρέπουν τέτοιες παρανομίες.

Εκτός από το να τυποποιούν την συμπεριφορά, τα πρωτόκολλα επιπλέον διαχωρίζουν την διαδικασία διεκπεραίωσης ενός έργου από τον μηχανισμό με τον οποίο επιτυγχάνεται αυτό. Μπορούμε να εξετάσουμε το πρωτόκολλο χωρίς να κουραστούμε από τις λεπτομέρειες τις υλοποίησης. Όταν είμαστε σίγουροι ότι έχουμε ένα καλό πρωτόκολλο, τότε μπορούμε να το εφαρμόσουμε όπου θέλουμε.

2.4.4 Διαιτητευόμενα πρωτόκολλα (arbitrated protocols)

Για να μπορέσουμε να περιγράψουμε τα πρωτόκολλα θα χρησιμοποιήσουμε την βοήθεια διαφόρων φανταστικών προσώπων. Οι βασικοί θα είναι η Μαρία και ο Κώστας. Θα πάρουν μέρος σε όλα τα γενικά πρωτόκολλα δύο ή περισσότερων οντοτήτων. Σ’ ορισμένα πρωτόκολλα μπορεί να λαμβάνουν μέρος και άλλα άτομα, όπως φαίνεται στον παρακάτω πίνακα:

Διαλογή Ρόλων

Μαρία Μετέχει σε όλα τα πρωτόκολλα

Κώστας Μετέχει σε όλα τα πρωτόκολλα

Εύα Μετέχει στα πρωτόκολλα τριών προσώπων

Ήρα Υποκλοπέας (eavesdropper)

Έκτορας Ενεργός αντίπαλος (malicious active attacker)

Δημοσθένης Έμπιστος διαιτητής (trusted arbitrator)

Ο **διαιτητής** (arbitrator) είναι μία αδιάφορη τρίτη οντότητα, που εμπιστευόμαστε για να διεκπεραιωθεί το πρωτόκολλο. «Αδιάφορη» σημαίνει ότι ο διαιτητής δεν έχει κανένα νόμιμο συμφέρον σε ότι αφορά το πρωτόκολλο και καμία προτίμηση σε ότι αφορά τα εμπλεκόμενα μέρη. Τα μέρη θεωρούν ό,τι λέει αληθές, ό,τι κάνει σωστό, και ότι θα αναλάβει να φέρει εις πέρας τον ρόλο του. Οι διαιτητές βοηθούν στο να ολοκληρωθεί ένα πρωτόκολλο ανάμεσα σε δύο αμοιβαία φιλύποπτα μέρη.

Στην καθημερινή μας ζωή τον ρόλο διαιτητή παίζουν συχνά δικηγόροι και συμβολαιογράφοι. Η έννοια του διαιτητή είναι τόσο παλιά όσο και η κοινωνία και παίζει σημαντικό ρόλο σ' αυτήν.

Η έννοια αυτή μπορεί να μεταφερθεί και στον κόσμο των υπολογιστών, αλλά υπάρχουν ορισμένα προβλήματα:

- Είναι ευκολότερο να εμπιστευτείς ένα ουδέτερο τρίτο πρόσωπο αν γνωρίζεις την ταυτότητά του και το έχεις συναντήσει. Δύο πρόσωπα που δεν εμπιστεύονται ο ένας τον άλλο πιθανότατα δεν θα εμπιστευτούν ούτε κάποιον απρόσωπο διαιτητή κάπου μέσα στο δίκτυο.
- Το δίκτυο θα πρέπει να συντηρεί την δαπάνη της μίσθωσης του διαιτητή.
- Το πρωτόκολλο γίνεται πιο αργό με τη χρησιμοποίηση διαιτητή.
- Ο διαιτητής πρέπει να επεμβαίνει σε οποιαδήποτε συναλλαγή γίνεται στο δίκτυο. Αποτελεί, λοιπόν, κώλυμα για μια ευρεία εφαρμογή ενός πρωτοκόλλου. Αύξηση των διαιτητών μετριάζει το πρόβλημα, αλλά αυξάνει το κόστος.
- Από τη στιγμή που όλοι στο δίκτυο εμπιστεύονται τον διαιτητή, αποτελεί σημείο ευπάθειας για την ασφάλεια του δικτύου.

Παρόλα αυτά, η διαιτησία έχει εφαρμογή σε αρκετά πρωτόκολλα.

2.4.5 Επιδικαζόμενα πρωτόκολλα (adjudicated protocols)

Εξαιτίας του μεγάλου κόστους πληρωμής διαιτητών, τα διαιτητευόμενα πρωτόκολλα μπορούν να διαιρεθούν σε δύο υπό-πρωτόκολλα. Το πρώτο είναι ένα μη διαιτητευόμενο υπό-πρωτόκολλο, που ακολουθείται κάθε φορά που κάποιοι θέλουν να εφαρμόσουν το πρωτόκολλο. Το δεύτερο είναι ένα διαιτητευόμενο υπό-πρωτόκολλο, που εκτελείται μόνο στην περίπτωση διαφωνίας. Το ειδικό αυτό είδος διαιτητή ονομάζεται **κριτής (adjudicator)**. Ο κριτής είναι επίσης αδιάφορος και έμπιστος. Αντίθετα, όμως, με τον διαιτητή, δεν παίρνει απευθείας μέρος σε όλα τα πρωτόκολλα. Ο κριτής καλείται μόνο για να αποφανθεί αν το

πρωτόκολλο εκτελέστηκε σωστά, και μόνο όταν αυτό είναι αναγκαίο. Τα επιδικαζόμενα πρωτόκολλα βασίζονται στην τιμιότητα των εμπλεκόμενων οντοτήτων. Αν, όμως, κάποιος υποψιάζεται απάτη, υπάρχει ένας όγκος καταγεγραμμένων δεδομένων με τα οποία μπορεί μια έμπιστη τρίτη οντότητα να ανακαλύψει την απάτη. Σε ένα καλοσχεδιασμένο τέτοιο πρωτόκολλο ο κριτής μπορεί να ανακαλύψει και την ταυτότητα του απατεώνα. Ο αναπόφευκτος εντοπισμός του δράστη λειτουργεί ως αποτρεπτικό στοιχείο.

2.4.6 Αυτοδύναμα πρωτόκολλα (self-enforcing protocols)

Τα αυτοδύναμα πρωτόκολλα είναι τα καλύτερα. Η διαδικασία του πρωτοκόλλου εγγυάται από μόνη της την νομιμότητα. Δεν χρειάζεται διαιτητής για να εφαρμοστεί το πρωτόκολλο. Ούτε κριτής για να λυθούν διαφωνίες. Το πρωτόκολλο είναι έτσι σχεδιασμένο ώστε να μην υπάρχουν διαφωνίες. Αν κάποιος προσπαθήσει να διαπράξει απάτη, οι υπόλοιποι εντοπίζουν την απάτη του και το πρωτόκολλο διακόπτεται.

Στην καλύτερη περίπτωση, όλα τα πρωτόκολλα θα ήταν αυτοδύναμα. Δυστυχώς, δεν μπορεί να σχεδιαστεί αυτοδύναμο πρωτόκολλο για κάθε περίπτωση.

2.4.7 Επιθέσεις εναντίων πρωτοκόλλων

Κρυπτογραφικές επιθέσεις μπορούν να γίνουν κατά των αλγορίθμων που χρησιμοποιούνται στα πρωτόκολλα, κατά των τεχνικών που χρησιμοποιήθηκαν για την εφαρμογή αυτών των αλγορίθμων και πρωτοκόλλων, ή κατά των ίδιων των πρωτοκόλλων. Κατά την μελέτη των πρωτοκόλλων θα θεωρήσουμε ότι οι αλγόριθμοι και οι τεχνικές που χρησιμοποιούνται είναι ασφαλείς.

Υπάρχουν διάφοροι τρόποι για να προσβληθεί ένα πρωτόκολλο. Κάποιος που δεν παίρνει μέρος στο πρωτόκολλο μπορεί να υποκλέψει μέρος ή και όλο το πρωτόκολλο. Αυτό ονομάζεται **παθητική προσβολή (passive attack)** γιατί ο επιτιθέμενος δεν επηρεάζει το πρωτόκολλο, απλά προσπαθεί να αποκτήσει πληροφορίες παρατηρώντας το πρωτόκολλο. Αυτό το είδος επίθεσης αντιστοιχεί στην προσβολή βάσει κρυπτογραφήματος. Επειδή η παθητική προσβολή είναι δύσκολο να εντοπιστεί, τα πρωτόκολλα προσπαθούν να την εμποδίσουν παρά να την εντοπίσουν.

Μία άλλη περίπτωση είναι ο επιτιθέμενος να προσπαθεί να μεταβάλει το πρωτόκολλο προς όφελός του. Θα μπορούσε να υποδύεται κάποιο άλλο πρόσωπο, να προσθέτει επιπλέον μηνύματα στο πρωτόκολλο, να διαγράφει νόμιμα

μηνύματα, να αντικαθιστά μηνύματα, να μεταδίδει ξανά παλιότερα μηνύματα, να διακόπτει μια γραμμή επικοινωνίας, ή να μεταβάλει αποθηκευμένες πληροφορίες. Όλα αυτά ανήκουν στην κατηγορία των **ενεργών προσβολών (active attack)**, επειδή απαιτούν ενεργό παρέμβαση. Η μορφή των επιθέσεων αυτών εξαρτάται από το δίκτυο.

Οι παθητικοί επιτιθέμενοι επιχειρούν να αποκτήσουν πληροφορίες για τα εμπλεκόμενα μέρη. Μαζεύουν τα μηνύματα που ανταλλάσσονται και προσπαθούν να τα αναλύσουν. Από την άλλη οι ενεργές προσβολές έχουν πιο ευρύ φάσμα στόχων. Ο επιτιθέμενος θα μπορούσε να επιθυμεί την συλλογή πληροφοριών, την μείωση της απόδοσης του συστήματος, την αλλοίωση αποθηκευμένων πληροφοριών, ή την μη εξουσιοδοτημένη πρόσβαση.

Οι ενεργές επιθέσεις είναι πιο επιβλαβείς, ιδιαίτερα σε πρωτόκολλα όπου τα διάφορα πρόσωπα δεν εμπιστεύονται το ένα το άλλο. Ο επιτιθέμενος δεν χρειάζεται να είναι ξένος προς το σύστημα. Θα μπορούσε να είναι κάποιος χρήστης του συστήματος ή ο διαχειριστής του συστήματος. Θα μπορούσαν ακόμα να υπάρχουν πολλοί συνεργαζόμενοι επιτιθέμενοι.

Είναι, επίσης, δυνατόν ο επιτιθέμενος να είναι κάποιος από τους μετέχοντες στο πρωτόκολλο. Μπορεί να ψεύδεται κατά την εφαρμογή του πρωτοκόλλου ή να μην εφαρμόζει καν το πρωτόκολλο. Αυτό το είδος επιτιθέμενου ονομάζεται **παραβάτης (cheater)**. Οι **παθητικοί παραβάτες (passive cheaters)** ακολουθούν το πρωτόκολλο, αλλά επιχειρούν να αποκτήσουν περισσότερες πληροφορίες απ' ότι θα επέτρεπε το πρωτόκολλο. Οι ενεργοί **παραβάτες (active cheaters)** διακόπτουν την εξέλιξη του πρωτοκόλλου προσπαθώντας έτσι να ε ξαπατήσουν τα άλλα μέλη.

Είναι δύσκολο να διατηρηθεί ένα πρωτόκολλο ασφαλές αν οι πλειοψηφία των χρηστών είναι ενεργοί παραβάτες, άλλα μερικές φορές είναι δυνατόν τα υπόλοιπα μέλη να αντιληφθούν την απάτη. Οπωσδήποτε, πάντως, ένα πρωτόκολλο θα πρέπει να είναι ασφαλές έναντι παθητικών παραβατών.

Όπως αναφέρει ο P. Syverson , η επιτυχία των επιθέσεων στα κρυπτογραφικά πρωτόκολλα εξαρτάται από ορισμένες βασικές υποθέσεις. Μια λίστα τέτοιων υποθέσεων παρουσιάζεται παρακάτω. Η επιλογή αυτών των υποθέσεων έγινε με βάση πραγματικά δεδομένα, όπως τα περιβάλλοντα πελάτη-εξυπηρετητή (client/server).

Υπόθεση 1η: Υπάρχει μία έμπιστη τρίτη οντότητα, καλούμενη Κέντρο Διανομής Κλειδιών (Key Distribution Center), που είναι υπεύθυνη για την δημιουργία και διανομή των κλειδιών συνόδου.

Υπόθεση 2η: Το υπολογιστικό περιβάλλον του νόμιμου χρήστη είναι ασφαλές. Δεν μας απασχολούν τα προβλήματα ασφαλείας που υπάρχουν σε ορισμένα λογισμικά, και κυρίως το Λειτουργικό Σύστημα.

Υπόθεση 3η: Είναι υπολογιστικά απίθανο κάποιος επιτιθέμενος να σπάσει το κρυπτοσύστημα με κρυπτανάλυση.

Υπόθεση 4η: Όταν επικοινωνούν δύο οντότητες, χρησιμοποιούν το κλειδί συνόδου που συμφωνήθηκε μετά τον τερματισμό της δεδομένης εφαρμογής του πρωτοκόλλου (protocol instance). Με άλλα λόγια, το κλειδί συνόδου που χρησιμοποιείται όταν είναι η Μαρία ενεργός χρήστης είναι διαφορετικό, από το κλειδί συνόδου που χρησιμοποιείται όταν ο Κώστας είναι ενεργός χρήστης.

Υπόθεση 5η: Η εφαρμογή ενός πρωτοκόλλου μπορεί να ξεκινήσει μόνο από τον ενεργό χρήστη. Αυτό έχει την βάση του στο προγραμματιστικό περιβάλλον όπου μια σύνοδος ξεκινά πάντα από τον πελάτη (client), ή αλλιώς την ενεργό οντότητα, και όχι από τον εξυπηρετητή (server), ή αλλιώς παθητική οντότητα.

Υπόθεση 6η: Κάθε οντότητα έχει ένα μηχανισμό, όπως μια μηχανή καταστάσεων (state machine), για την αποθήκευση της κατάστασης σε κάθε βήμα του πρωτοκόλλου.

Υπόθεση 7η: Οι οντότητες που παίρνουν μέρος σε ένα κρυπτογραφικό πρωτόκολλο θα μεταφράζουν αυστηρά το περιεχόμενο των μηνυμάτων που ανταλλάσσουν.

2.4.8 Ιδιότητες των κρυπτογραφικών πρωτοκόλλων

Ποιοι είναι οι στόχοι ενός **πρωτοκόλλου διανομής πιστοποιημένων κλειδιών (authenticated key distribution protocol)**; Μπορούμε να πούμε ότι, μετά την εκτέλεση ενός τέτοιου πρωτοκόλλου, οι εμπλεκόμενες οντότητες θα πρέπει να έχουν την δυνατότητα να πιστεύουν ότι επικοινωνούν μεταξύ τους και όχι με κάποιον εισβολέα, και ταυτόχρονα ότι μοιράζονται αποκλειστικά μεταξύ τους ένα μυστικό, που μπορεί να χρησιμοποιηθεί ως κλειδί συνόδου στις μελλοντικές επικοινωνίες τους. Παρακάτω αναφέρονται οι ιδιότητες ενός ορθού πρωτοκόλλου.

1. *Προφύλαξη του κλειδιού συνόδου (session key safeness)*. Θεωρούμε ότι ένα πρωτόκολλο έχει την ιδιότητα της προφύλαξης του κλειδιού συνόδου, όταν, δεδομένου ότι το πρωτόκολλο τερμάτισε φυσιολογικά, η Μαρία έχει επικοινωνήσει με ασφάλεια με τον Κώστα (χρησιμοποιώντας το κλειδί συνόδου), και κανείς τρίτος δεν γνωρίζει το κλειδί συνόδου.

2. *Ακριβής πιστοποίηση (authentication correctness)*. Θεωρούμε ότι ένα πρωτόκολλο έχει την ιδιότητα της ακριβούς πιστοποίησης, όταν οι εμπλεκόμενες οντότητες είναι μόνο οι πιστοποιημένες. Αν εντοπιστεί κάποιος εισβολέας πριν τον φυσιολογικό τερματισμό του πρωτοκόλλου, τότε το πρωτόκολλο σταματά, εμφανίζοντας προειδοποίηση. Για να τερματίσει το πρωτόκολλο φυσιολογικά, θα πρέπει να έχουν επιβεβαιωθεί οι ταυτότητες όλων των εμπλεκόμενων οντοτήτων.

3. *Ιδιότητα μη επανάληψης (non-replayable property)*. Θεωρούμε ότι ένα πρωτόκολλο έχει την ιδιότητα της μη επανάληψης, αν τα δεδομένα που μεταδίδονται σε κάθε εφαρμογή του πρωτοκόλλου δεν βοηθούν τον αντίπαλο. Δηλαδή, ο αντίπαλος δεν μπορεί ούτε να κατανοήσει αλλά ούτε και να αναμεταδώσει τα δεδομένα που υποκλέπτει, χωρίς να γίνει αντιληπτός.

4. *Μικρός πλεονασμός (low redundancy property)*. Θεωρούμε ότι ένα πρωτόκολλο έχει μικρό ή μηδενικό πλεονασμό, αν δεν περιλαμβάνει κάτι το μη απαραίτητο για να πετύχει τους στόχους του (δηλαδή την προφύλαξη του κλειδιού συνόδου, την ακριβής πιστοποίηση και την ιδιότητα μη επανάληψης). Η ιδιότητα αυτή είναι περισσότερο σχετική με την αποδοτικότητα και όχι με την ασφάλεια του πρωτοκόλλου.

2.5 Επικοινωνία με χρήση συμμετρικής κρυπτογραφίας

Το πρωτόκολλο για ασφαλή επικοινωνία μεταξύ της Μαρίας και του Κώστα έχει ως εξής:

1. Η Μαρία και ο Κώστας συμφωνούν σε ένα κρυπτοσύστημα.
2. Η Μαρία και ο Κώστας συμφωνούν σε ένα κλειδί.
3. Η Μαρία κρυπτογραφεί το μήνυμά της με τον συμφωνημένο αλγόριθμο και κλειδί.
4. Η Μαρία στέλνει το κρυπτογράφημα στον Κώστα.
5. Ο Κώστας αποκρυπτογραφεί το κρυπτογράφημα με το συμφωνημένο κλειδί και διαβάζει το μήνυμα.

   Τι μπορεί η Ήρα, που παρεμβάλλεται ανάμεσα στην Μαρία και τον Κώστα, να μάθει από το πρωτόκολλο; Αν το μόνο που καταλήγει στα χέρια της είναι το κρυπτογράφημα του βήματος 4, τότε πρέπει να το κρυπταναλύσει. Θα είναι μια παθητική προσβολή βάσει κρυπτογραφήματος. Υπάρχουν αλγόριθμοι που, απ' όσο γνωρίζουμε, είναι ανθεκτικοί σε οτιδήποτε θα μπορούσε, λογικά, να χρησιμοποιήσει η Ήρα.

   Η Ήρα το γνωρίζει αυτό, γι' αυτό θέλει να υποκλέψει και τα βήματα 1 και 2. Έτσι θα ξέρει τον αλγόριθμο και το κλειδί όπως και ο Κώστας. Υποκλέπτοντας και το κρυπτογράφημα από το βήμα 4, δεν έχει παρά να το αποκρυπτογραφήσει με το κλειδί όπως και ο Κώστας.

Όπως έχουμε πει, καλό κρυπτοσύστημα είναι εκείνο που εναποθέτει όλη του την ασφάλεια στο κλειδί και όχι στην γνώση του αλγόριθμου. Αυτός είναι ο λόγος για τον οποίο έχει τόσο μεγάλη σημασία η διαχείριση κλειδιών. Για έναν συμμετρικό αλγόριθμο, η Μαρία κι ο Κώστας μπορούν να εκτελέσουν το βήμα 1 δημόσια, αλλά το βήμα 2 πρέπει να εκτελεστεί με μυστικότητα. Το κλειδί πρέπει να παραμείνει μυστικό, πριν, κατά την διάρκεια, και μετά το πέρας του πρωτοκόλλου για όσο διάστημα θέλουμε να παραμείνει το μήνυμα κρυφό.

Ο Έκτορας θα μπορούσε να πετύχει ορισμένα ακόμα πράγματα. Θα μπορούσε να επιχειρήσει την διακοπή της επικοινωνίας κατά το βήμα 4, έτσι ώστε η Μαρία και ο Κώστας να μην μπορούν να μιλήσουν. Θα μπορούσε ακόμα να εντοπίσει και να απομακρύνει τα μηνύματα της Μαρίας, αντικαθιστώντας τα με τα δικά του. Αν γνώριζε το κλειδί (το έχει υποκλέψει κατά το στάδιο 2 ή έχει σπάσει τον κώδικα), θα μπορούσε να γράψει ένα δικό του μήνυμα και να το στείλει στον Κώστα. Ο Κώστας δεν θα είχε κανένα τρόπο να αντιληφθεί ότι το μήνυμα δεν είναι της Μαρίας. Αν, από την άλλη, δεν γνώριζε το κλειδί, το μόνο που θα μπορούσε να κάνει είναι να στείλει ένα τυχαίο μήνυμα, που όταν ο Κώστας θα αποκρυπτογραφούσε, δεν θα έβγαζε νόημα. Έτσι θα υπέθετε ότι ή η Μαρία έχει κάποιο πρόβλημα ή το δίκτυο.

Τέλος, το πρωτόκολλο αυτό υποθέτει ότι τα δύο μέρη εμπιστεύονται το ένα το άλλο.Συνοπτικά, τα συμμετρικά κρυπτοσυστήματα έχουν τα παρακάτω προβλήματα:

- Τα κλειδιά πρέπει να διανέμονται με μυστικότητα. Είναι τόσο πολύτιμα όσο και το κρυπτογραφημένο μήνυμα. Στην περίπτωση συστημάτων παγκοσμίου εμβέλειας, αυτό αποτελεί ένα αξεπέραστο πολλές φορές πρόβλημα. Συχνά, τα μυστικά κλειδιά παραδίδονται με ταχυδρομικό αποστολέα.

- Αν υποκλαπεί ένα κλειδί (κλαπεί, παραβιαστεί το κρυπτοσύστημα, κάποιος δωροδοκηθεί ή εκβιαστεί κοκ.), τότε η Ήρα θα μπορεί να διαβάσει όλα τα μηνύματα που γράφτηκαν με το κλειδί αυτό. Μπορεί επίσης να υποδυθεί κάποιο από τα μέρη.

- Αν υποθέσουμε ότι χρησιμοποιείται διαφορετικό κλειδί για κάθε ζευγάρι χρηστών σε ένα δίκτυο, ο συνολικός αριθμός κλειδιών αυξάνει ραγδαία καθώς αυξάνουν οι χρήστες. Ένα δίκτυο με n χρήστες χρειάζεται n(n-1)/2 κλειδιά. Για παράδειγμα 10 χρήστες χρειάζονται 45 κλειδιά και 100 χρήστες 4950 κλειδιά. Το πρόβλημα μπορεί να μειωθεί αν διατηρηθεί μικρός ο αριθμός των χρηστών, άλλα αυτό δεν είναι πάντα εφικτό.

2.6 Μονόδρομες συναρτήσεις (one-way functions)

Η ιδέα της **μονόδρομης συνάρτησης** (one-way function) είναι κεντρική στην κρυπτογραφία δημόσιου κλειδιού. Αν και δεν αποτελούν από μόνες τους πρωτόκολλα, οι συναρτήσεις αυτές είναι από τα θεμελιώδη στοιχεία των περισσότερων πρωτοκόλλων. Οι μονόδρομες συναρτήσεις είναι εύκολες να υπολογιστούν, άλλα σημαντικά δυσκολότερο να αντιστραφούν. Δηλαδή, δοθέντος του x είναι εύκολο να υπολογίσουμε το f(x), αλλά δοθέντος του f(x) είναι δύσκολο να υπολογίσουμε το x. Στην περίσταση αυτή, το «δύσκολο» ορίζεται κάπως έτσι: θα χρειάζονταν εκατομμύρια χρόνια για να υπολογίσουμε το x από το f(x), ακόμη κι αν χρησιμοποιούντο όλοι οι υπολογιστές του κόσμου.

Το σπάσιμο ενός πιάτου είναι καλό παράδειγμα μονόδρομης συνάρτησης. Είναι εύκολο να σπάσουμε ένα πιάτο σε χιλιάδες μικρά κομμάτια. Αντίθετα, είναι μάλλον δύσκολο να συγκολλήσουμε τα κομμάτια για να φτιάξουμε το αρχικό πιάτο.

Η ιδέα ακούγεται καλή, αλλά είναι παραπλανητική. Μιλώντας από καθαρά μαθηματική σκοπιά, δεν έχουμε αποδείξει ότι τέτοιες συναρτήσεις υπάρχουν, ούτε έχουμε ενδείξεις ότι μπορούν να κατασκευαστούν. Μόλο ταύτα, αρκετές συναρτήσεις μοιάζουν με μονόδρομες. Για παράδειγμα, για πεπερασμένο σύνολο ορισμού, το x2 είναι εύκολο να υπολογιστεί, ενώ για το x1/2 είναι σημαντικά δυσκολότερο. Παρόλα αυτά, εδώ θα θεωρήσουμε ότι μονόδρομες συναρτήσεις υπάρχουν.

Που, όμως, μας χρησιμεύουν οι μονόδρομες συναρτήσεις; Οπωσδήποτε δεν κάνουν για κρυπτογραφία. Κανείς δεν θα μπορούσε να αποκρυπτογραφήσει ένα μήνυμα κρυπτογραφημένο με μονόδρομη συνάρτηση. Δεν χρησιμεύουν ούτε και στη κρυπτογραφία δημόσιου κλειδιού. Μία, πάντως, εφαρμογή που μπορούν να έχουν είναι στην πιστοποίηση (authentication) ενός χρήστη σε ένα σύστημα (login).

Μονόδρομη συνάρτηση καταπακτής (trapdoor one-way function) ονομάζεται η μονόδρομη εκείνη συνάρτηση που μπορεί να παρακαμφθεί. Είναι εύκολο να υπολογιστεί προς τη μια κατεύθυνση, αλλά δύσκολο προς την άλλη. Αλλά υπάρχει κάποια μυστική πληροφορία y, τέτοια ώστε γνωρίζοντας τα f(x) και y να είναι εύκολο να υπολογίσεις το x.

Ένα αποσυναρμολογημένο ρολόι είναι ένα καλό παράδειγμα. Είναι πολύ δύσκολο για κάποιον να το συναρμολογήσει, εκτός κι αν έχει τις οδηγίες συναρμολόγησης.

2.6.1 Μονόδρομη συνάρτηση συμπίεσης (one-way hash function)

Η **μονόδρομη συνάρτηση** συμπίεσης (one-way hash function) έχει στα αγγλικά και άλλα ονόματα, που είναι δύσκολο (και ίσως άσκοπο) να μεταφραστούν: compression function, contraction function, message digest, fingerprint, cryptographic checksum, message integrity check (MIC), και manipulation detection code (MDC). Η λειτουργία της είναι κεντρική στη σύγχρονη κρυπτογραφία και αποτελεί ένα ακόμα θεμελιώδες στοιχείο στη δημιουργία πρωτοκόλλων.

Οι συναρτήσεις συμπίεσης (hash functions) χρησιμοποιούνται αρκετό καιρό στην κρυπτογραφία. Μια τέτοια συνάρτηση, είτε είναι μαθηματική είτε όχι, δέχεται για δεδομένα εισόδου string μεταβλητού μήκους (που ονομάζεται **αρχική εικόνα [pre-image]**) και επιστρέφει ένα string καθορισμένου μήκους (που ονομάζεται **τιμή hash [hash value]**). Μια απλή συνάρτηση συμπίεσης θα επέστρεφε το αποτέλεσμα του XOR όλων των bytes εισόδου.

Ο σκοπός εδώ είναι να φωτογραφήσουμε την αρχική εικόνα: να πάρουμε μια τιμή που θα καθορίζει αν μια υποψήφια αρχική εικόνα έχει πιθανότητες να είναι η πραγματική αρχική εικόνα. Επειδή οι συναρτήσεις συμπίεσης είναι τύπου «πολλά προς ένα», δεν τις χρησιμοποιούμε για να δείξουμε ισότητα, αλλά για να πάρουμε μια διαβεβαίωση ομοιότητας, μέσα σε λογικά πλαίσια.

Μια μονόδρομη συνάρτηση συμπίεσης είναι μια συνάρτηση συμπίεσης που λειτουργεί μόνο προς τη μια μεριά: είναι εύκολο να υπολογίσουμε την τιμή hash, αλλά δύσκολο να βρούμε μια αρχική εικόνα που να συμπιέζεται στη συγκεκριμένη τιμή. Το XOR δεν είναι μονόδρομο: είναι πανεύκολο να βρεθεί ένα string που τα bytes του να δίνουν με XOR μια συγκεκριμένη τιμή. Επιπλέον, λοιπόν, μια καλή μονόδρομη συνάρτηση συμπίεσης πρέπει να μην παρουσιάζει **συγκρούσεις (collision-free)**, να είναι, δηλαδή, δύσκολο να βρούμε δύο αρχικές εικόνες με την ίδια τιμή hash.

Ο αλγόριθμος της συνάρτησης είναι δημόσια γνωστός. Η ασφάλεια έγκειται στην μονοδρομία της. Η τιμή δεν εξαρτάται από την αρχική εικόνα με κανένα διακριτό τρόπο. Η αλλαγή ενός και μόνο bit στην αρχική εικόνα αλλάζει κατά μέσο όρο τα μισά bit της τιμής hash.

Μια μονόδρομη συνάρτηση συμπίεσης θα μπορούσε να χρησιμοποιηθεί για να πάρουμε τα **αποτυπώματα (fingerprints)** των αρχείων μας. Αν θέλει κάποιος να μας αποδείξει ότι έχει ένα συγκεκριμένο αρχείο, που και εμείς έχουμε, δεν χρειάζεται να στείλει το αρχείο, αλλά την τιμή hash του αρχείου. Αν η τιμή ταιριάζει μ' αυτή που εμείς έχουμε, τότε είναι σχεδόν σίγουρο ότι έχει το συγκεκριμένο αρχείο.

2.6.2 Κώδικες πιστοποίησης μηνυμάτων (message authentication codes)

Οι **κώδικες πιστοποίησης μηνυμάτων (message authentication codes [MACs])**, ή αλλιώς **κώδικες πιστοποίησης δεδομένων (data authentication codes [DACs])**, είναι μονόδρομες συναρτήσεις συμπίεσης με την προσθήκη κλειδιού. Η τιμή hash εξαρτάται τόσο από την αρχική εικόνα όσο κι από το κλειδί. Η ιδέα είναι η ίδια με τις μονόδρομες συναρτήσεις συμπίεσης, μόνο που την τιμή hash μπορεί να την επιβεβαιώσει μόνο κάποιος που γνωρίζει το κλειδί. Μπορούμε να κατασκευάσουμε ένα MAC χρησιμοποιώντας μια συνάρτηση hash και έναν συμμετρικό αλγόριθμο, αλλά υπάρχουν και αποκλειστικοί αλγόριθμοι MAC.

2.7 Επικοινωνία με χρήση κρυπτογραφίας δημόσιου κλειδιού

Μπορούμε να παρομοιάσουμε έναν συμμετρικό αλγόριθμο με χρηματοκιβώτιο. Το κλειδί είναι ο συνδυασμός. Όποιος τον ξέρει μπορεί να ανοίξει το χρηματοκιβώτιο, να βάλει ένα έγγραφο μέσα, και να το ξανακλείσει. Κάποιος άλλος που επίσης ξέρει τον συνδυασμό, μπορεί κι αυτός να το ανοίξει, να πάρει το έγγραφο, και να το ξανακλείσει.

Μέχρι το 1976 η κρυπτογραφία βασίζονταν μόνο σ' αυτό το μοντέλο. Την χρονιά εκείνη ο Whitfield Diffie και ο Martin Hellman άλλαξαν τον ρου της κρυπτογραφίας. Εισήγαγαν την κρυπτογραφία δημόσιου κλειδιού (public-key cryptography) (η NSA ισχυρίστηκε ότι γνώριζε την τεχνική αυτή από το 1966, αλλά δεν προσέφερε καμία απόδειξη). Χρησιμοποίησαν δύο διαφορετικά κλειδιά, το ένα δημόσιο και το άλλο ιδιωτικό.

Οποιοσδήποτε κατέχει το δημόσιο κλειδί μπορεί να κρυπτογραφήσει ένα μήνυμα, αλλά όχι να το αποκρυπτογραφήσει.

Μόνο το άτομο που έχει το ιδιωτικό κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα. Είναι σαν να μετέτρεψαν το χρηματοκιβώτιο του παραπάνω παραδείγματος σε γραμματοκιβώτιο. Η κρυπτογράφηση με το δημόσιο κλειδί είναι το ανάλογο της ρίψης γράμματος στο γραμματοκιβώτιο. Η αποκρυπτογράφηση με το ιδιωτικό κλειδί είναι το ανάλογο της συλλογής των γραμμάτων από το γραμματοκιβώτιο μόνο κάποιος με το φυσικό κλειδί του γραμματοκιβωτίου μπορεί να το κάνει εύκολα. Οποιοσδήποτε άλλος θα χρειαζόταν πυρσό οξυγονοκόλλησης.

Μαθηματικά, η διαδικασία στηρίζεται στη λειτουργία μιας μονόδρομης συνάρτησης καταπακτής. Η κρυπτογράφηση είναι η εύκολη κατεύθυνση. Έχοντας το δημόσιο κλειδί οποιοσδήποτε μπορεί να κρυπτογραφήσει ένα μήνυμα (γενικά είναι εύκολο να αποκτήσουμε το δημόσιο κλειδί, γι' αυτό και λέγεται δημόσιο). Η αποκρυπτογράφηση είναι η δύσκολη κατεύθυνση. Μόνο κάποιος που γνωρίζει την μυστική πληροφορία μπορεί να αποκρυπτογραφήσει το μήνυμα. Η μυστική πληροφορία είναι το ιδιωτικό κλειδί.

Παρακάτω καταγράφονται τα βήματα που πρέπει να ακολουθηθούν για να στείλει η Μαρία μήνυμα στον Κώστα:

1. Η Μαρία και ο Κώστας συμφωνούν σε ένα κρυπτοσύστημα.

2. Ο Κώστας στέλνει το δημόσιο κλειδί του στη Μαρία.

3. Η Μαρία κρυπτογραφεί το μήνυμά της με το δημόσιο κλειδί του Κώστα και του το στέλνει.

4. Ο Κώστας αποκρυπτογραφεί το μήνυμα της Μαρίας με το ιδιωτικό του κλειδί και το διαβάζει.

Παρατηρούμε ότι η κρυπτογραφία δημόσιου κλειδιού λύνει το πρόβλημα της διαχείρισης κλειδιών που είχαμε με τη συμμετρική κρυπτογραφία. Προηγουμένως έπρεπε με κάποιον μυστικό τρόπο να δώσει η Μαρία το κλειδί στον Κώστα. Τώρα, χωρίς καμία προηγούμενη συνεννόηση, η Μαρία μπορεί με ασφάλεια να επικοινωνήσει με τον Κώστα. Η Ήρα, που υποθέτουμε ότι ακούει όλη την επικοινωνία μεταξύ των δύο, έχει υποκλέψει το δημόσιο κλειδί του Κώστα και το κρυπτογράφημα, αλλά δεν μπορεί ούτε το ιδιωτικό κλειδί να υπολογίσει, ούτε να ανακτήσει το αρχικό μήνυμα.

Πιο συχνά συμβαίνει οι χρήστες ενός δικτύου να έχουν από πριν συμφωνήσει σε ένα **κρυπτοσύστημα δημόσιου κλειδιού**. Ο κάθε χρήστης έχει ένα ζευγάρι κλειδιών (ιδιωτικό-δημόσιο) και όλα τα δημόσια κλειδιά είναι καταχωρημένα σε μια βάση. Το πρωτόκολλο μετατρέπεται ως εξής:

1. Η Μαρία ζητά και παίρνει το δημόσιο κλειδί του Κώστα από τη βάση.

2. Η Μαρία κρυπτογραφεί το μήνυμά της με το δημόσιο κλειδί του Κώστα και του το στέλνει.

3. Ο Κώστας αποκρυπτογραφεί το μήνυμα της Μαρίας με το ιδιωτικό του κλειδί και το διαβάζει.

Στο αρχικό πρωτόκολλο ο Κώστας έπρεπε να στείλει το δημόσιο κλειδί του προτού μπορέσει να λάβει το μήνυμα. Το δεύτερο πρωτόκολλο λειτουργεί ανάλογα με το ταχυδρομικό σύστημα. Ο Κώστας δεν εμπλέκεται στην διαδικασία, παρά μόνο όταν θέλει να διαβάσει το μήνυμα.

2.8 Υβριδικά κρυπτοσυστήματα (hybrid cryptosystems)

Οι πρώτοι αλγόριθμοι δημόσιου κλειδιού εμφανίστηκαν την περίοδο που ο DES εξετάζονταν ως υποψήφιο πρότυπο. Αυτό είχε σαν αποτέλεσμα να δεχθεί η κρυπτογραφία δημόσιου κλειδιού επίθεση. Πολλοί θεώρησαν το νέο είδος ως ανταγωνιστικό του παλιού, ειδικά μετά την κριτική που άσκησαν οι Diffie και Hellman στον DES σχετικά με το μικρό μήκος κλειδιού.

Στην πραγματικότητα, οι αλγόριθμοι δημόσιου κλειδιού δεν είναι υποκατάστατο των συμμετρικών αλγορίθμων. Κι αυτό γιατί δεν χρησιμοποιούνται για κρυπτογράφηση μηνυμάτων, αλλά κλειδιών. Δύο είναι οι λόγοι:

1. Οι ασύμμετροι αλγόριθμοι είναι πιο αργοί. Οι συμμετρικοί αλγόριθμοι είναι γενικά χίλιες φορές ταχύτεροι από τους ασύμμετρους. Οι υπολογιστές γίνονται, βέβαια, ταχύτεροι, αλλά θα υπάρχει πάντα η ανάγκη για γρηγορότερη κρυπτογράφηση απ' αυτή που μπορούν οι ασύμμετροι αλγόριθμοι να προσφέρουν.

2. Τα κρυπτοσυστήματα δημόσιου κλειδιού είναι ευάλωτα σε προσβολές επιλεγμένου κειμένου. Αν θεωρήσουμε τη σχέση C=E(P), όπου P είναι ένα κείμενο επιλεγμένο από ένα σύνολο n πιθανών κειμένων, τότε ο κρυπταναλυτής μπορεί να κρυπτογραφήσει και τα n πιθανά κείμενα και να συγκρίνει το αποτέλεσμα με το C (αυτό γίνεται γιατί το κλειδί κρυπτογράφησης είναι δημόσια γνωστό). Θα επιτύχει έτσι μια τοπική ανάλυση, δηλαδή δεν θα βρει το κλειδί κρυπτογράφησης, αλλά θα βρει το αρχικό κείμενο P για το συγκεκριμένο C.

Μια προσβολή επιλεγμένου κειμένου μπορεί να είναι ιδιαίτερα αποτελεσματική εάν υπάρχει σχετικά μικρός αριθμός πιθανών κειμένων, δηλαδή αν το n είναι μικρό. Για παράδειγμα, αν το P είναι χρηματικό ποσό μικρότερο από 1.000.000, τότε χρειαζόμαστε 1.000.000 διαφορετικές κρυπτογραφήσεις. Η επίθεση αυτή είναι ικανοποιητικά αποτελεσματική ακόμα κι αν το P δεν είναι τόσο καλά ορισμένο. Και μόνο η γνώση ότι ένα κρυπτογράφημα δεν αντιστοιχεί σε κάποιο κείμενο μπορεί να βοηθήσει. Τα συμμετρικά κρυπτοσυστήματα δεν έχουν αυτό το πρόβλημα, γιατί ο αναλυτής, μη γνωρίζοντας το κλειδί, δεν μπορεί

να εφαρμόσει δοκιμαστικές κρυπτογραφήσεις. Η **πιθανολογική κρυπτογράφηση (probabilistic encryption)** λύνει αυτό το πρόβλημα, γιατί αντιστοιχεί σε ένα αρχικό κείμενο P περισσότερα του ενός κρυπτογραφήματα: C1, C2,... , Ci. Έτσι, κι αν ακόμα ο αναλυτής διαλέξει να κρυπτογραφήσει το σωστό κείμενο, θα πάρει για κρυπτογράφημα το Ck που θα είναι διαφορετικό από το Ci που έχει στα χέρια του. Θα είναι αδύνατο, λοιπόν, να καταλάβει ότι βρήκε το σωστό P.

Πρακτικά, η ασύμμετρη κρυπτογραφία χρησιμοποιείται για τη **φύλαξη και διανομή κλειδιών συνόδου (session keys)**. Τα κλειδιά συνόδου χρησιμοποιούνται με τη σειρά τους για να κρυπτογραφήσουν τα μηνύματα. Αυτό μερικές φορές καλείται **υβριδικό κρυπτοσύστημα (hybrid cryptosystem)**.

1. Ο Κώστας στέλνει στη Μαρία το δημόσιο κλειδί του.
2. Η Μαρία δημιουργεί ένα τυχαίο κλειδί συνόδου, K, το κρυπτογραφεί χρησιμοποιώντας το δημόσιο κλειδί του Κώστα, και το στέλνει σ' αυτόν.

   $E_{K\Omega}(K)$
3. Ο Κώστας αποκρυπτογραφεί το μήνυμα της Μαρίας, χρησιμοποιώντας το ιδιωτικό του κλειδί, και αποκτά το κλειδί συνόδου.

   $D_{K\Omega}(E_{K\Omega}(K)) = K$
4. Και οι δύο κρυπτογραφούν τα μηνύματά τους χρησιμοποιώντας το ίδιο κλειδί συνόδου.

Η χρήση ασύμμετρης κρυπτογραφίας λύνει ένα πολύ σημαντικό πρόβλημα. Στην συμμετρική κρυπτογραφία το κλειδί κρυπτογράφησης παραμένει αποθηκευμένο μέχρι να χρησιμοποιηθεί. Επιπλέον, καθώς είναι δύσκολο να γίνει η ανταλλαγή του κλειδιού, είναι πολύ πιθανό να χρησιμοποιηθεί σε αρκετές συνδιαλέξεις. Με το πρωτόκολλο που μόλις περιγράψαμε, το κλειδί συνόδου δημιουργείται όταν αυτό είναι απαραίτητο και καταστρέφεται με το πέρας της συνόδου. Μειώνονται έτσι δραστικά οι πιθανότητες κρυπτανάλυσης του κλειδιού.

2.9 Ψηφιακές υπογραφές

Οι χειρόγραφες υπογραφές χρησιμοποιούνται καιρό τώρα ως απόδειξη της συγγραφής ενός κειμένου, ή τουλάχιστο ως ένδειξη συμφωνίας με όσα αναφέρει το κείμενο. Οι ιδιότητες που προσφέρει η υπογραφή συνοψίζονται παρακάτω:

1. Η υπογραφή είναι γνήσια. Πείθει τον παραλήπτη ότι ο υπογράφων ενήργησε σκόπιμα.

2. Η υπογραφή είναι απαραχάρακτη. Η υπογραφή είναι απόδειξη ότι ο υπογράφων και όχι κάποιος άλλος, ηθελημένα υπέγραψε το έγγραφο.

3. Η υπογραφή δεν μπορεί να χρησιμοποιηθεί ξανά. Αποτελεί μέρος του κειμένου και δεν μπορεί κάποιος απατεώνας να την μετακινήσει.

4. Το υπογεγραμμένο κείμενο είναι αμετάβλητο.

5. Ο υπογράφων δεν μπορεί να αρνηθεί την υπογραφή του, καθώς το έγγραφο και η υπογραφή είναι φυσικές οντότητες.

Στην πραγματικότητα, καμιά από τις παραπάνω ιδιότητες δεν ισχύει απόλυτα. Οι υπογραφές μπορούν να παραχαραχθούν, μπορούν να μεταφερθούν από έγγραφο σε έγγραφο, και τα έγγραφα μπορούν να αλλοιωθούν μετά την υπογραφή τους. Είμαστε, όμως, διατεθειμένοι να παραβλέψουμε αυτούς τους κινδύνους, επειδή είναι δύσκολο να γίνουν.

Θα θέλαμε να υλοποιήσουμε την έννοια της υπογραφής και στους υπολογιστές, αλλά υπάρχουν δυσκολίες. Καταρχήν ένα αρχείο είναι πολύ απλό να αντιγραφεί. Ακόμα και αν ήταν δύσκολο να παραχαραχθεί μια υπογραφή (μια σκαναρισμένη εικόνα της υπογραφής), είναι εύκολο με διαδικασίες cut και paste να την τοποθετήσουμε σε όποιο ηλεκτρονικό έγγραφο θέλουμε. Δεύτερον, τα αρχεία των υπολογιστών είναι εύκολο να αλλοιωθούν μετά την υπογραφή, χωρίς να μπορεί η αλλοίωση αυτή να εντοπιστεί.

2.9.1 Υπογραφή εγγράφων με χρήση συμμετρικού κρυπτοσυστήματος και διαιτητή

Η Μαρία θέλει να υπογράψει ένα κείμενο και να το στείλει στον Κώστα. Μπορεί να το πετύχει με τη βοήθεια του Δημοσθένη και τη χρήση συμμετρικού κρυπτοσυστήματος.

Ο Δημοσθένης είναι ένας έμπιστος διαιτητής με μεγάλη υπολογιστική δύναμη. Μπορεί να επικοινωνήσει τόσο με την Μαρία όσο και με τον Κώστα (και γενικά με οποιονδήποτε θέλει να υπογράψει ένα ψηφιακό έγγραφο). Μοιράζεται ένα κοινό μυστικό κλειδί, ΚΑ, με τη Μαρία, και ένα κοινό μυστικό κλειδί, ΚΚ, με τον Κώστα. Τα κλειδιά αυτά έχουν συμφωνηθεί πολύ πριν την έναρξη του πρωτοκόλλου και μπορούν να χρησιμοποιηθούν πολλές φορές για πολλαπλές υπογραφές.

1. Η Μαρία κρυπτογραφεί το μήνυμά της, Μ, προς τον Κώστα με το ΚΑ και το στέλνει στον Δημοσθένη.

2. Ο Δημοσθένης αποκρυπτογραφεί το μήνυμα με το ΚΑ.

3. Ο Δημοσθένης κρυπτογραφεί το Μ (που απέκτησε από το βήμα 2) μαζί με μια δήλωση ότι το έλαβε από τη Μαρία, με το ΚΚ.

4. Ο Δημοσθένης στέλνει το καινούργιο κρυπτογράφημα στον Κώστα.

5. Ο Κώστας αποκρυπτογραφεί το μήνυμα από τον Δημοσθένη με το ΚΚ. Τώρα μπορεί να διαβάσει τόσο το μήνυμα της Μαρίας όσο και τη βεβαίωση του Δημοσθένη ότι προήλθε από αυτήν.

Ο Δημοσθένης συμπεραίνει ότι το αρχικό μήνυμα προήλθε από την Μαρία, λόγω της κρυπτογράφησής του. Από τη στιγμή που μόνο αυτός και η Μαρία μοιράζονται το κλειδί ΚΑ, μόνο η Μαρία θα μπορούσε να κρυπτογραφήσει μήνυμα με αυτό.

Ας εξετάσουμε τώρα, αν το παραπάνω σχήμα μας παρέχει τα χαρακτηριστικά που θέλουμε:

1. Η υπογραφή είναι αυθεντική. Ο Δημοσθένης είναι έμπιστος και γνωρίζει ότι το μήνυμα στάλθηκε από τη Μαρία. Η βεβαίωσή του αποτελεί απόδειξη για τον Κώστα.

2. Η υπογραφή αυτή είναι απαραχάρακτη. Μόνο η Μαρία (και ο Δημοσθένης, αλλά όλοι τον εμπιστεύονται) γνωρίζει το ΚΑ, άρα μόνο αυτή θα μπορούσε να στείλει μήνυμα κρυπτογραφημένο με το ΚΑ. Αν κάποιος προσπαθούσε να υποδυθεί την Μαρία, ο Δημοσθένης θα το καταλάβαινε στο βήμα 2 και δεν θα πιστοποιούσε την αυθεντικότητά του.

3. Η υπογραφή αυτή δεν μπορεί να χρησιμοποιηθεί ξανά. Αν ο Κώστας προσπαθούσε να χρησιμοποιήσει την βεβαίωση του Δημοσθένη σε κάποιο άλλο έγγραφο, η Μαρία θα μπορούσε να δικαιωθεί. Ένας διαιτητής (θα μπορούσε να είναι ο Δημοσθένης ή κάποιος άλλος διαιτητής) θα ζητούσε από τον Κώστα το μήνυμα και το κρυπτογραφημένο από τη Μαρία μήνυμα. έπειτα θα κρυπτογραφούσε το μήνυμα με το κλειδί της Μαρίας ΚΑ και θα έβλεπε ότι το κρυπτογράφημα δεν ταιριάζει με αυτό που του έδωσε ο Κώστας. Ο Κώστας, φυσικά, δεν θα μπορούσε ποτέ να παράσχει το κατάλληλο κρυπτογράφημα, γιατί δεν γνωρίζει το κλειδί της Μαρίας.

4. Το υπογεγραμμένο έγγραφο είναι αμετάβλητο. Αν ο Κώστας προσπαθούσε να αλλοιώσει το έγγραφο μετά την υπογραφή του, ο διαιτητής θα αποδείκνυε την απάτη όπως και στο προηγούμενο βήμα.

5. Ο υπογράφων δεν μπορεί να αρνηθεί την υπογραφή του. Η βεβαίωση του Δημοσθένη είναι η απόδειξη, γιατί όλοι εμπιστεύονται τον Δημοσθένη.

Αν ο Κώστας θέλει να δείξει στην Εύα το υπογεγραμμένο από τη Μαρία έγγραφο, πρέπει πάλι να απευθυνθεί στον Δημοσθένη.

1. Ο Κώστας κρυπτογραφεί με το μυστικό κλειδί του, ΚΚ, το έγγραφο και την βεβαίωση που έλαβε από τον Δημοσθένη, και τα στέλνει στον Δημοσθένη.

2. Ο Δημοσθένης τα αποκρυπτογραφεί με το ΚΚ.

3. Ο Δημοσθένης συμβουλεύεται την βάση δεδομένων που κρατάει και βεβαιώνει ότι το αρχικό μήνυμα προήλθε από την Μαρία.

4. Ο Δημοσθένης κρυπτογραφεί το μήνυμα και τη βεβαίωσή του,χρησιμοποιώντας το μυστικό κλειδί ΚΕ που μοιράζεται με την Εύα, και τα στέλνει στην Εύα.

5. Η Εύα αποκρυπτογραφεί την απάντηση του Δημοσθένη με το μυστικό κλειδί της, ΚΕ. Τώρα μπορεί να διαβάσει τόσο το μήνυμα, όσο και την βεβαίωση του Δημοσθένη ότι το έστειλε η Μαρία.

Τέτοια πρωτόκολλα μπορούν να λειτουργήσουν, αλλά είναι χρονοβόρα για τον Δημοσθένη. Πρέπει να λαμβάνει μέρος σε κάθε υπογραφή μηνύματος και πρέπει να διατηρεί βάση δεδομένων με όλα τα μηνύματα (αν και αυτό μπορεί να αποφευχθεί, στέλνοντας στον παραλήπτη αντίγραφο του κρυπτογραφημένου μηνύματος του αποστολέα). Επιπλέον, αποτελεί σημείο στένωσης του δικτύου, κι ας είναι ένα πρόγραμμα που τρέχει σε κάποιο γρήγορο server (εξυπηρετητή).

Ακόμη πιο προβληματικά, όμως, είναι η δημιουργία και συντήρηση ενός τέτοιου προγράμματος, που το εμπιστεύονται όλοι. Ο Δημοσθένης επιβάλλεται να είναι αλάθητος αν κάνει έστω κι ένα λάθος σε μια υπογραφή, κανείς δεν θα τον εμπιστεύεται. Πρέπει, επίσης, να είναι απόλυτα προφυλαγμένος. Αν διέρρεε η βάση με τα κλειδιά ή αν κάποιος άλλαζε τον προγραμματισμό του, όλο το σύστημα υπογραφών θα αχρηστευόταν. Μπορεί, λοιπόν, στη θεωρία το σύστημα να έχει βάση, άλλα στην πραγματικότητα δεν είναι και τόσο αποτελεσματικό.

2.9.2 Υπογραφή εγγράφων με χρήση κρυπτογραφίας δημόσιου κλειδιού

Υπάρχουν ορισμένοι αλγόριθμοι δημόσιου κλειδιού, που μπορούν να χρησιμοποιηθούν για ψηφιακές υπογραφές. Σε ορισμένους αλγόριθμους (στον RSA, για παράδειγμα) τόσο το δημόσιο όσο και το ιδιωτικό κλειδί μπορούν να χρησιμοποιηθούν για κρυπτογράφηση. Η κρυπτογράφηση ενός εγγράφου με το ιδιωτικό κλειδί παράγει μια ασφαλή ψηφιακή υπογραφή. Στις περιπτώσεις άλλων αλγορίθμων (όπως ο DSA) υπάρχει ξεχωριστός αλγόριθμος για ψηφιακές υπογραφές, ο οποίος δεν μπορεί να χρησιμοποιηθεί για κρυπτογράφηση. Η ιδέα ανακαλύφθηκε από τους Diffie και Hellman, και εξελίχθηκε περαιτέρω από άλλους.

Το βασικό πρωτόκολλο είναι απλό:

1. Η Μαρία κρυπτογραφεί το έγγραφο με το ιδιωτικό της κλειδί, υπογράφοντας έτσι το έγγραφο.

2. Η Μαρία στέλνει το υπογεγραμμένο έγγραφο στον Κώστα.

3. Ο Κώστας αποκρυπτογραφεί το έγγραφο με το δημόσιο κλειδί της Μαρίας, επιβεβαιώνοντας έτσι το γνήσιο της υπογραφής.

Το πρωτόκολλο αυτό είναι φανερά ανώτερο του προηγουμένου. Εδώ δεν χρειαζόμαστε την βοήθεια του Δημοσθένη, ούτε για να υπογράψει ούτε για να βεβαιώσει υπογραφές (χρειάζεται μόνο για να βεβαιώσει ότι το δημόσιο κλειδί που χρησιμοποιεί ο Κώστας είναι πραγματικά της Μαρίας). Οι δύο οντότητες δεν χρειάζονται βοήθεια ούτε για να διευθετήσουν παρεξηγήσεις. Αν ο Κώστας δεν μπορέσει να εκτελέσει επιτυχώς το βήμα 3, τότε γνωρίζει ότι η υπογραφή δεν είναι έγκυρη.

Και αυτό το πρωτόκολλο ικανοποιεί τα χαρακτηριστικά που ζητάμε σε μια ψηφιακή υπογραφή:

1. Η υπογραφή είναι αυθεντική: όταν ο Κώστας πιστοποιεί την υπογραφή χρησιμοποιώντας το δημόσιο κλειδί της Μαρίας, καταλαβαίνει ότι εκείνη το έχει υπογράψει.

2. Η υπογραφή είναι απαραχάρακτη: μόνο η Μαρία γνωρίζει το ιδιωτικό της κλειδί.

3. Η υπογραφή δεν μπορεί να χρησιμοποιηθεί ξανά: αποτελεί ιδιότητα του συγκεκριμένου εγγράφου και δεν μπορεί να μεταφερθεί αλλού.

4. Το έγγραφο είναι αμετάβλητο. Αν υπάρξει η οποιαδήποτε αλλοίωση, δεν θα είναι δυνατόν να πιστοποιηθεί με το δημόσιο κλειδί της Μαρίας.

5. Ο υπογράφων δεν μπορεί να αρνηθεί την πράξη του. Ο Κώστας δεν χρειάζεται την βοήθεια της Μαρίας για να βεβαιώσει την υπογραφή της.

2.9.3 Υπογραφή εγγράφων και χρονικές σφραγίδες (timestamps)

Στην πραγματικότητα, ο Κώστας μπορεί να ξεγελάσει την Μαρία. Μπορεί να χρησιμοποιήσει ξανά το υπογεγραμμένο έγγραφο. Αυτό δεν αποτελεί πρόβλημα αν το έγγραφο είναι κάποιο συμβόλαιο, αλλά αν είναι μια ψηφιακή επιταγή θα πρέπει να χρησιμοποιηθεί μόνο μία φορά. Διαφορετικά ο Κώστας (που έχει κρατήσει ένα αντίγραφο της υπογεγραμμένης ψηφιακής επιταγής) μπορεί να την παρουσιάζει κάθε τόσο στην τράπεζα και να εισπράττει το ανάλογο ποσό. Αν η Μαρία δεν ελέγχει τον λογαριασμό της, ο Κώστας μπορεί να συνεχίσει για αρκετό καιρό.

Ως εκ τούτου, οι ψηφιακές υπογραφές περιέχουν πολλές φορές και **χρονικές σφραγίδες (timestamps)**. Αυτό σημαίνει ότι στο έγγραφο περιλαμβάνονται και η μέρα και ώρα της υπογραφής, και υπογράφονται όλα μαζί. Στο παραπάνω παράδειγμα, η τράπεζα κρατάει αντίγραφο της επιταγής και όταν ο Κώστας πηγαίνει ξανά με την ίδια επιταγή, η τράπεζα ξέρει ότι την έχει ήδη εξαργυρώσει.

2.9.4 Υπογραφή εγγράφων με χρήση κρυπτογραφίας δημόσιου κλειδιού και μονόδρομων συναρτήσεων συμπίεσης

Οι ασύμμετροι αλγόριθμοι είναι, στην πράξη, ακατάλληλοι για την υπογραφή μεγάλων εγγράφων. Για τον λόγο αυτό αρκετά πρωτόκολλα ψηφιακής υπογραφής κάνουν χρήση μιας μονόδρομης συνάρτησης συμπίεσης (one-way hash function). Η Μαρία δεν υπογράφει το έγγραφο, αλλά την hash τιμή του. Στο παρακάτω πρωτόκολλο τόσο η μονόδρομη συνάρτηση συμπίεσης όσο και ο αλγόριθμος ψηφιακής υπογραφής έχουν καθοριστεί εκ των προτέρων.

1. Η Μαρία υπολογίζει την hash τιμή του εγγράφου.

2. Η Μαρία κρυπτογραφεί την hash τιμή με το ιδιωτικό της κλειδί, υπογράφοντας έτσι το έγγραφο.

3. Η Μαρία στέλνει το έγγραφο και την υπογεγραμμένη hash τιμή του στον Κώστα.

4. Ο Κώστας υπολογίζει την hash τιμή του εγγράφου που έλαβε από την Μαρία. Έπειτα αποκρυπτογραφεί την υπογεγραμμένη hash τιμή με το δημόσιο κλειδί της Μαρίας. Αν η hash τιμή που έστειλε η Μαρία ταιριάζει με την hash τιμή που ο ίδιος υπολόγισε, τότε η υπογραφή είναι έγκυρη.

Η ταχύτητα αυξάνεται κατακόρυφα και, από τη στιγμή που η πιθανότητα δύο εγγράφων να έχουν την ίδια hash τιμή είναι 2160,μπορούμε με ασφάλεια να θεωρήσουμε ότι υπογράφοντας το hash υπογράφουμε το έγγραφο. Η ιδιότητα της μονόδρομης συνάρτησης είναι απαραίτητη, γιατί διαφορετικά θα ήταν εύκολο να βρεθούν έγγραφα που θα έδιναν την ίδια hash τιμή. Έτσι υπογράφοντας ένα θα ήταν σαν να τα υπογράφαμε όλα.

Το πρωτόκολλο αυτό έχει και άλλα προτερήματα. Καταρχήν, η υπογραφή δεν είναι μέρος του εγγράφου. Δεύτερον, οι απαιτήσεις σε χωρητικότητα είναι πολύ μικρότερες για τον παραλήπτη. Ένα σύστημα αρχειοθέτησης μπορεί να χρησιμοποιήσει τον τρόπο αυτό για να επιβεβαιώνει την ύπαρξη ενός εγγράφου χωρίς να χρειάζεται να αποθηκεύει το ίδιο το περιεχόμενό του. Απλά αποθηκεύει την hash τιμή του εγγράφου. Για την ακρίβεια, δεν χρειάζεται να έχει καν γνώση των περιεχομένων του εγγράφου. Οι χρήστες καταθέτουν την hash τιμή του εγγράφου τους και η βάση προσθέτει χρονική σφραγίδα και τα υπογράφει. Το πρωτόκολλο αυτό είναι σημαντικό, επειδή η Μαρία μπορεί να πάρει τα δικαιώματα για ένα έγγραφο χωρίς να κάνει γνωστό το περιεχόμενό του απλά και μόνο καταθέτοντας την hash τιμή του.

2.10 Αλγόριθμοι και ορολογία

Υπάρχουν πολλοί αλγόριθμοι ψηφιακών υπογραφών. Όλοι τους είναι ασύμμετροι αλγόριθμοι. Μερικές φορές η διαδικασία υπογραφής ονομάζεται κρυπτογράφηση με ιδιωτικό κλειδί και η διαδικασία επιβεβαίωσης της υπογραφής αποκρυπτογράφηση με δημόσιο κλειδί. Η ορολογία αυτή είναι παραπλανητική, γιατί ισχύει μόνο για έναν αλγόριθμο, τον RSA. Άλλοι αλγόριθμοι έχουν διαφορετικούς τρόπους υλοποίησης. Για παράδειγμα, οι μονόδρομες συναρτήσεις συμπίεσης και οι χρονικές σφραγίδες προσθέτουν μερικές φορές επιπλέον βήματα στην διαδικασία υπογραφής. Πολλοί είναι και οι αλγόριθμοι που μπορούν να χρησιμοποιηθούν μόνο για υπογραφή και όχι για κρυπτογράφηση.

Γενικά, θα αναφερόμαστε στην διαδικασία υπογραφής και πιστοποίησης χωρίς αναφορά στις λεπτομέρειες του εκάστοτε αλγόριθμου. Η υπογραφή ενός μηνύματος με το ιδιωτικό κλειδί K θα δηλώνεται ως:

$S_K(M)$

και η επιβεβαίωση της υπογραφής με το αντίστοιχο δημόσιο κλειδί γράφεται ως:

$V_K(M)$

Τα bit που προστίθενται στο έγγραφο κατά την διαδικασία της υπογραφής (στο προηγούμενο παράδειγμα, η μονόδρομη hash τιμή) ονομάζονται **ψηφιακή υπογραφή (digital signature)**, ή απλά **υπογραφή (signature)**. Ολόκληρο το πρωτόκολλο κατά το οποίο ο παραλήπτης βεβαιώνεται για την ταυτότητα του αποστολέα και την ακεραιότητα του μηνύματος, ονομάζεται πιστοποίηση.

2.11 Ανταλλαγή κλειδιών

Στην ενότητα αυτή θα εξετάσουμε το πώς διανέμονται τα κλειδιά συνόδου.

2.11.1 Ανταλλαγή κλειδιών με χρήση συμμετρικής κρυπτογραφίας

Το πρωτόκολλο αυτό υποθέτει ότι η Μαρία και ο Κώστας, και οι δύο χρήστες του ιδίου δικτύου, έχουν καταχωρημένα σε μία βάση τα μυστικά τους κλειδιά. Η βάση αυτή ονομάζεται **κέντρο διανομής κλειδιών (ΚΔΚ) (Key Distribution Center [KDC])**. Τα κλειδιά αυτά πρέπει να υπάρχουν στην βάση πριν την έναρξη του πρωτοκόλλου.

Το συγκεκριμένο πρωτόκολλο αγνοεί το κατά τα άλλα πολύ σημαντικό πρόβλημα του πώς κατατίθενται τα κλειδιά στη βάση απλά είναι αποθηκευμένα εκεί και κανείς τρίτος δεν ξέρει την τιμή τους. Τον ρόλο του κέντρου τον παίζει ο Δημοσθένης. Το πρωτόκολλο έχει ως εξής:

1. Η Μαρία ζητά από τον Δημοσθένη ένα κλειδί συνόδου για να επικοινωνήσει με τον Κώστα.

2. Ο Δημοσθένης δημιουργεί ένα τυχαίο κλειδί συνόδου. Κρυπτογραφεί το κλειδί δύο φορές: μία με το μυστικό κλειδί του Κώστα και μία με το μυστικό κλειδί της Μαρίας. Στέλνει και τα δύο αντίγραφα στη Μαρία.

3. Η Μαρία αποκρυπτογραφεί το δικό της αντίγραφο με το κλειδί της.

4. Η Μαρία στέλνει στον Κώστα το δικό του αντίγραφο.

5. Ο Κώστας αποκρυπτογραφεί το δικό του αντίγραφο με το κλειδί του.

6. Και οι δύο χρησιμοποιούν αυτό το κλειδί συνόδου για να επικοινωνήσουν.

Το πρωτόκολλο αυτό επαφίεται στην απόλυτη ασφάλεια του Δημοσθένη, που το πιθανότερο είναι να είναι κάποιο πρόγραμμα παρά κάποιο άτομο. Αν ο Έκτορας διαπεράσει την ασφάλεια του Δημοσθένη, το όλο σύστημα καθίσταται ανασφαλές. Ο Έκτορας θα γνωρίζει πλέον τα μυστικά κλειδιά όλων των χρηστών και θα μπορεί να διαβάσει όλα τα μηνύματα, παλιά και καινούργια, που υποκλέπτει στο δίκτυο.

Το άλλο πρόβλημα με το σχήμα αυτό είναι ότι ο Δημοσθένης αποτελεί σημείο στένωσης των επικοινωνιών όλου του δικτύου, καθώς θα πρέπει να παίρνει μέρος σε όλες τις ανταλλαγές κλειδιών.

2.11.2 Ανταλλαγή κλειδιών με χρήση ασύμμετρης κρυπτογραφίας

Η Μαρία και ο Κώστας χρησιμοποιούν κρυπτογραφία δημόσιου κλειδιού για να συμφωνήσουν στο κλειδί συνόδου και έπειτα χρησιμοποιούν το κλειδί αυτό για να κρυπτογραφήσουν την συνομιλία τους. Σε ορισμένες εφαρμογές τα δημόσια κλειδιά και των δύο, βρίσκονται υπογεγραμμένα σε μια βάση δεδομένων. Αυτό καθιστά το πρωτόκολλο ακόμα ευκολότερο και η Μαρία μπορεί να στείλει ένα ασφαλές μήνυμα στον Κώστα ακόμη κι αν αυτός δεν την γνωρίζει.

1. Η Μαρία αποκτά το δημόσιο κλειδί του Κώστα από το κέντρο διανομής κλειδιών (ΚΔΚ).

2. Η Μαρία δημιουργεί ένα τυχαίο κλειδί συνόδου, το κρυπτογραφεί με το δημόσιο κλειδί του Κώστα και του το στέλνει.

3. Ο Κώστας αποκρυπτογραφεί το μήνυμα της Μαρίας με το ιδιωτικό του κλειδί.

4. Και οι δύο χρησιμοποιούν το ίδιο κλειδί συνόδου για να κρυπτογραφήσουν τα μηνύματά τους.

2.11.3 Επίθεση ενδιάμεσου ατόμου (man-in-the-middle attack)

Το μόνο που μπορεί η Ήρα να επιχειρήσει στο προηγούμενο πρωτόκολλο είναι να σπάσει τον αλγόριθμο. Ο Έκτορας από την άλλη, έχει περισσότερες δυνατότητες. Όχι μόνο μπορεί να ακούσει τα μηνύματα που στέλνουν οι δύο πλευρές, αλλά μπορεί και να τα αλλοιώσει, να τα διαγράψει ή να δημιουργήσει εντελώς καινούργια. Μπορεί να υποδύεται την Μαρία, όταν μιλάει στον Κώστα, και τον Κώστα όταν μιλάει στην Μαρία. Η επίθεση γίνεται ως εξής:

1. Η Μαρία στέλνει το δημόσιο κλειδί της στον Κώστα. Ο Έκτορας το υποκλέπτει και το αντικαθιστά με το δικό του δημόσιο κλειδί.
2. Ο Έκτορας στέλνει το δικό του δημόσιο κλειδί στην Μαρία. Πάλι ο Έκτορας υποκλέπτει το κλειδί και το αντικαθιστά με το δικό του δημόσιο κλειδί.
3. Όταν η Μαρία στέλνει μήνυμα στον Κώστα, κρυπτογραφημένο με το δημόσιο κλειδί του «Κώστα», ο Έκτορας το υποκλέπτει. Αφού, στην πραγματικότητα, είναι κρυπτογραφημένο με το δικό του δημόσιο κλειδί, μπορεί να το διαβάσει. Έπειτα, κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του Κώστα και το στέλνει στον Κώστα.
4. Όταν ο Κώστας στέλνει μήνυμα στην Μαρία, κρυπτογραφημένο με το δημόσιο κλειδί του «Μαρίας», ο Έκτορας το υποκλέπτει. Αφού, στην πραγματικότητα, είναι κρυπτογραφημένο με το δικό του δημόσιο κλειδί, μπορεί να το διαβάσει. Έπειτα, κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί της Μαρίας και το στέλνει στην Μαρία.

Ακόμη κι αν τα κλειδιά της Μαρίας και του Κώστα είναι αποθηκευμένα σε μια βάση, ο Έκτορας μπορεί να υποκλέψει είτε την αίτηση της Μαρίας προς τη βάση, είτε την απάντηση της βάσης, και να στείλει το δικό του δημόσιο κλειδί σαν απάντηση. Το ίδιο θα κάνει και με τον Κώστα. Αυτή η επίθεση είναι εφικτή, επειδή η Μαρία και ο Κώστας δεν έχουν κανένα τρόπο να επιβεβαιώσουν ότι μιλάνε ο ένας στον άλλο. Υποθέτοντας ότι ο Έκτορας δεν επιβαρύνει την ταχύτητα της συνομιλίας, δεν υπάρχει τρόπος να αντιληφθούν ότι κάποιος διαβάζει την αλληλογραφία τους.

2.11.4 Ανταλλαγή κλειδιών και ψηφιακές υπογραφές

Η προσθήκη ψηφιακών υπογραφών, κατά την ανταλλαγή κλειδιού συνόδου, μπορεί επίσης να εμποδίσει την επίθεση ενδιάμεσου ατόμου. Ο Δημοσθένης, που παίζει τον ρόλο του κέντρου διανομής κλειδιών (KDC), υπογράφει τα κλειδιά του Κώστα και της Μαρίας. Η υπογραφή περιλαμβάνει και ένα πιστοποιητικό ιδιοκτησίας. Το πρωτόκολλο έχει ως εξής (υποθέτουμε ότι και η Μαρία και ο Κώστας έχουν το δημόσιο κλειδί του Δημοσθένη) :

1. Η Μαρία ζητά από τον Δημοσθένη το δημόσιο κλειδί του Κώστα.
2. Ο Δημοσθένης ανακτά από τη βάση του το δημόσιο κλειδί του Κώστα, προσθέτει σ’ αυτό κάποια πληροφορία για τον Κώστα, τα υπογράφει όλα μαζί και τα στέλνει στην Μαρία.

3. Η Μαρία επιβεβαιώνει την υπογραφή του Δημοσθένη με το δημόσιο κλειδί του και πλέον γνωρίζει με σιγουριά το κλειδί του Κώστα.
4. Ο Κώστας εκτελεί τα βήματα 1-3 και αποκτά με σιγουριά το κλειδί της Μαρίας.
5. Η Μαρία δημιουργεί ένα τυχαίο κλειδί συνόδου, το υπογράφει με το ιδιωτικό κλειδί της, το κρυπτογραφεί με το δημόσιο κλειδί του Κώστα και του το στέλνει.
6. Ο Κώστας αποκρυπτογραφεί το κλειδί συνόδου με το ιδιωτικό του κλειδί.
7. Και οι δύο χρησιμοποιούν το συμφωνημένο κλειδί συνόδου για να κρυπτογραφήσουν την επικοινωνία τους.

Τα δύο μέλη γνωρίζουν ότι μιλούν μεταξύ τους, και όχι με κάποιον άλλο, από τη στιγμή που χρησιμοποιούν το ίδιο κλειδί συνόδου. Το μόνο που μπορεί να κάνει ο Έκτορας είναι να παρακολουθεί τα κρυπτογραφημένα μηνύματα και να προσπαθήσει να σπάσει τον αλγόριθμο.

Το πρωτόκολλο χρησιμοποιεί τον Δημοσθένη, ο οποίος είναι μια έμπιστη οντότητα. Μόνο αν ο Έκτορας καταφέρει και σπάσει τους μηχανισμούς ασφαλείας του Δημοσθένη, μπορεί να διαβάλει το πρωτόκολλο. Αν καταφέρει και αποκτήσει το ιδιωτικό κλειδί του Δημοσθένη, θα μπορεί να υπογράφει το δικό του δημόσιο κλειδί σαν να ήταν του Κώστα ή της Μαρίας. Όμως η απόκτηση αυτού του ιδιωτικού κλειδιού δεν είναι εύκολη υπόθεση.

2.11.5 Πιστοποίηση και ανταλλαγή κλειδιού

Τα πρωτόκολλα αυτά συνδυάζουν την πιστοποίηση των προσώπων που επικοινωνούν με την ασφαλή ανταλλαγή κλειδιού συνόδου. Τα περισσότερα υποθέτουν ότι ο Δημοσθένης μοιράζεται ένα κοινό κλειδί με κάθε έναν από τους μετέχοντες, και ότι τα κλειδιά αυτά είναι κατάλληλα διανεμημένα πριν την έναρξη του πρωτοκόλλου. Ο παρακάτω πίνακας δείχνει τα σύμβολα που χρησιμοποιούνται.

Σύμβολα που χρησιμοποιούνται στα πρωτόκολλα πιστοποίησης και ανταλλαγής κλειδιού

MA Το όνομα της Μαρίας
ΚΩ Το όνομα του Κώστα
E_M Κρυπτογράφηση με το κοινό κλειδί του Δημοσθένη με τη Μαρία
$E_{KΩ}$ Κρυπτογράφηση με το κοινό κλειδί του Δημοσθένη με τον Κώστα
E_K Κρυπτογράφηση με το κλειδί συνόδου
I Δείκτης (index)
K Τυχαίο κλειδί συνόδου
X Χρόνος ζωής
T_M, T_K Χρονικές σφραγίδες
R_M, R_K Τυχαίος αριθμός (nonce), επιλεγμένος από την Μαρία και τον Κώστα αντίστοιχα

15.9.1 Wide-mouth frog

Το πρωτόκολλο αυτό είναι μάλλον το απλούστερο συμμετρικό πρωτόκολλο διαχείρισης κλειδιών, που χρησιμοποιεί έναν έμπιστο εξυπηρετητή (server). Τόσο ο Κώστας όσο και η Μαρία μοιράζονται ένα κοινό κλειδί με τον Δημοσθένη. Τα κλειδιά αυτά χρησιμοποιούνται μόνο για διανομή κλειδιών και όχι για την κρυπτογράφηση μηνυμάτων μεταξύ των χρηστών. Με δύο, μόνο, μηνύματα η Μαρία στέλνει ένα κλειδί συνόδου στον Κώστα:

1. Η Μαρία συνενώνει μια χρονική σφραγίδα με το όνομα του Κώστα και ένα τυχαίο κλειδί συνόδου, και κρυπτογραφεί το σύνολο με το κλειδί που μοιράζεται με τον Δημοσθένη. Στέλνει το κρυπτογράφημα στον Δημοσθένη μαζί με το όνομά της.

$MA, E_M(T_M, KΩ, K)$

2. Ο Δημοσθένης αποκρυπτογραφεί το μήνυμα της Μαρίας. Έπειτα συνενώνει μια νέα χρονική σφραγίδα με το όνομα της Μαρίας και το τυχαίο κλειδί συνόδου. Κρυπτογραφεί το σύνολο με το κλειδί που μοιράζεται με τον Κώστα και το στέλνει στον Κώστα.

$E_{KΩ}(T_K, MA, K)$

Το πρωτόκολλο παίρνει ως δεδομένο κάτι πολύ σημαντικό: ότι η Μαρία έχει τη δυνατότητα και ικανότητα να δημιουργεί ασφαλή κλειδιά συνόδου. Έχουμε σημειώσει ότι η δημιουργία τυχαίων αριθμών δεν είναι εύκολη υπόθεση και μπορεί να είναι πέρα από τις δυνατότητες της Μαρίας.

2.12 Πρωτόκολλο διασύνδεσης (interlock protocol)

Το **πρωτόκολλο διασύνδεσης** ανακαλύφθηκε από τους Ron Rivest και Adi Shamir, και έχει αρκετές πιθανότητες να εμποδίσει την επίθεση ενδιάμεσου ατόμου. Παρακάτω περιγράφεται το πρωτόκολλο:

1. Η Μαρία στέλνει στον Κώστα το δημόσιο κλειδί της.
2. Ο Κώστας στέλνει στην Μαρία το δημόσιο κλειδί του.
3. Η Μαρία κρυπτογραφεί το μήνυμά της με το δημόσιο κλειδί του Κώστα και του στέλνει το μισό.
4. Ο Κώστας κρυπτογραφεί το μήνυμά του με το δημόσιο κλειδί της Μαρίας και της στέλνει το μισό.
5. Η Μαρία στέλνει το άλλο μισό του μηνύματος στον Κώστα.
6. Ο Κώστας ενώνει τα δύο μισά του μηνύματος της Μαρίας και τα αποκρυπτογραφεί με το ιδιωτικό του κλειδί. Έπειτα στέλνει το δεύτερο μισό του δικού μηνύματος στην Μαρία.
7. Η Μαρία ενώνει τα δύο μισά του μηνύματος του Κώστα και τα αποκωδικοποιεί με το ιδιωτικό της κλειδί.

Το βασικό είναι ότι το ένα μισό του μηνύματος είναι άχρηστο χωρίς το άλλο μισό. Ο Κώστας δεν μπορεί να διαβάσει το παραμικρό από το μήνυμα της Μαρίας πριν το βήμα 6· η Μαρία δεν μπορεί να διαβάσει το παραμικρό από το μήνυμα του Κώστα πριν το βήμα 7.

Αυτό μπορεί να επιτευχθεί με διάφορους τρόπους:

- Αν ο αλγόριθμος κρυπτογράφησης είναι αλγόριθμος μπλοκ, θα μπορούσε το πρώτο μισό του μηνύματος να περιέχει το πρώτο μισό από κάθε μπλοκ (δηλαδή, το κάθε δεύτερο bit).
- Η αποκρυπτογράφηση του κρυπτογραφήματος θα μπορούσε να εξαρτάται από τη τιμή ενός **διανύσματος αρχικοποίησης (initialisation vector)**, το οποίο στέλνεται με το δεύτερο μισό του μηνύματος.
- Το πρώτο μήνυμα θα μπορούσε να είναι η hash τιμή του μηνύματος και το ίδιο το μήνυμα θα μπορούσε να σταλεί κρυπτογραφημένο τη δεύτερη φορά.

Το πρωτόκολλο αυτό δημιουργεί προβλήματα στον Έκτορα. Μπορεί και πάλι να αντικαταστήσει τα κλειδιά στα βήματα 1 και 2 με το δικό του κλειδί, αλλά δεν μπορεί να αποκρυπτογραφήσει τα μηνύματα στα βήματα 3 και 4. Πρέπει να τα κρατήσει και να τα αντικαταστήσει με τα μισά δύο δικών του, τελείως άσχετων μηνυμάτων· ένα για την Μαρία και ένα για τον Κώστα. Όταν, στα βήματα 5 και 6, παίρνει το δεύτερο μισό των πραγματικών μηνυμάτων και

μαθαίνει το περιεχόμενό τους, δεν μπορεί να κάνει τίποτα για να αλλάξει το περιεχόμενο των δικών του μηνυμάτων.

Είναι πιθανό, παρόλα αυτά, να καταφέρει ο Έκτορας να συνεχίσει το κόλπο του για αρκετή ώρα, αν γνωρίζει καλά τον Κώστα και την Μαρία και μπορεί να φανταστεί μια πιθανή συζήτηση μεταξύ τους. Σίγουρα, πάντως, είναι δυσκολότερο από το να κάθεται και να ακούει παθητικά τα μηνύματά τους.

Από την άλλη, το πρωτόκολλο αυτό δεν μπορεί να χρησιμοποιηθεί παντού, γιατί ο Κώστας στέλνει το μήνυμά του παράλληλα με της Μαρίας και όχι σε απάντηση του δικού της μηνύματος.

2.12.1 Yahalom

Και σ' αυτό το πρωτόκολλο υποθέτουμε ότι η Μαρία και ο Κώστας μοιράζονται από ένα μυστικό κοινό κλειδί με τον Δημοσθένη.

1. Η Μαρία συνενώνει το όνομά της με έναν τυχαίο αριθμό και τα στέλνει στον Κώστα.

MA, R_M

2. Ο Κώστας συνενώνει το όνομα της Μαρίας και τον τυχαίο αριθμό της, με έναν δικό του τυχαίο αριθμό. Τα κρυπτογραφεί με το κλειδί που μοιράζεται με τον Δημοσθένη και του τα στέλνει μαζί με το όνομά του.

$KΩ, E_{KΩ}(MA, R_M, R_K)$

3. Ο Δημοσθένης δημιουργεί δύο μηνύματα. Το πρώτο περιλαμβάνει το όνομα του Κώστα, ένα τυχαίο κλειδί συνόδου, τον τυχαίο αριθμό της Μαρίας και τον τυχαίο αριθμό του Κώστα, και κρυπτογραφείται με το κλειδί που μοιράζεται με την Μαρία. Το δεύτερο περιλαμβάνει το όνομα της Μαρίας και το τυχαίο κλειδί συνόδου, και κρυπτογραφείται με το κλειδί που μοιράζεται με τον Κώστα. Στέλνει και τα δύο μηνύματα στην Μαρία.

$E_M(KΩ, K, R_M, R_K), E_{KΩ}(MA,K)$

4. Η Μαρία αποκωδικοποιεί το πρώτο μήνυμα, ανακτά το K, και βεβαιώνεται ότι το R_M έχει την τιμή που υπολόγισε στο βήμα 1. Έπειτα στέλνει στον Κώστα δύο μηνύματα. Το πρώτο είναι το μήνυμα που έλαβε από τον Δημοσθένη. Το δεύτερο είναι το R_K, κρυπτογραφημένο με το κλειδί συνόδου.

$E_{KΩ}(MA, K), E_K(R_K)$

5. Ο Κώστας αποκωδικοποιεί το πρώτο μήνυμα και ανακτά το *K*. Έπειτα βεβαιώνεται ότι το R_K έχει την ίδια τιμή με το βήμα 2.

Στο τέλος η Μαρία και ο Κώστας είναι πεπεισμένοι ότι μιλούν μεταξύ τους και όχι σε κάποιον τρίτο. Το καινούργιο στοιχείο εδώ είναι ότι πρώτος ο Κώστας έρχεται σε επαφή με τον Δημοσθένη, ο οποίος με τη σειρά του στέλνει μόνο μία απάντηση (στην Μαρία).

2.12.2 Κέρβερος

Στο βασικό πρωτόκολλο Κέρβερος (έκδοση 5), η Μαρία και ο Κώστας μοιράζονται ο καθένας από ένα κλειδί με τον Δημοσθένη. Το πρωτόκολλο έχει ως εξής:

1. Η Μαρία στέλνει μήνυμα στον Δημοσθένη που περιλαμβάνει την ταυτότητά της και αυτήν του Κώστα.

   ΜΑ, ΚΩ

2. Ο Δημοσθένης δημιουργεί ένα μήνυμα, που περιέχει χρονική σφραγίδα, διάρκεια ζωής, *L*, ένα τυχαίο κλειδί συνόδου και την ταυτότητα της Μαρίας. Το κρυπτογραφεί χρησιμοποιώντας το κλειδί που μοιράζεται με τον Κώστα. Έπειτα τοποθετεί σε ένα μήνυμα την χρονική σφραγίδα, την διάρκεια ζωής, το κλειδί συνόδου και την ταυτότητα του Κώστα, και το κρυπτογραφεί με το κλειδί που μοιράζεται με Μαρία. Τέλος, στέλνει και τα δύο μηνύματα στην Μαρία.

$E_M(T, L, K, K\Omega), E_{K\Omega}(T, L, K, MA)$

3. Η Μαρία δημιουργεί ένα μήνυμα που περιέχει την ταυτότητά της και την χρονική σφραγίδα που έλαβε, και το κρυπτογραφεί με το *K*. Το στέλνει στον Κώστα, μαζί με το μήνυμα του Δημοσθένη, που είναι κρυπτογραφημένο με το κλειδί του Κώστα.

   $E_K(MA, T), E_{K\Omega}(T, L, K, MA)$

4. Ο Κώστας δημιουργεί ένα μήνυμα, που περιέχει την χρονική σφραγίδα αυξημένη κατά ένα, και το κρυπτογραφεί με το *K*. Στέλνει το μήνυμα στην Μαρία.

   $E_K(T+1)$

Το πρωτόκολλο αυτό είναι εφαρμόσιμο, αλλά παίρνει ως δεδομένο ότι το ρολόι όλων των συστημάτων είναι συγχρονισμένο με του Δημοσθένη. Αυτό, όμως, είναι πρακτικά ανέφικτο. Η λύση που δίνεται είναι ο συγχρονισμός των ρολογιών (με περιθώριο κάποια λεπτά) με μια κεντρική οντότητα, και ο εντοπισμός επανάληψης μηνυμάτων μέσα στο χρονικό αυτό περιθώριο.

2.12.3 DASS

Τα πρωτόκολλα της Υπηρεσίας Ασφαλούς Κατανεμημένης Πιστοποίησης (**D**istributed **A**uthentication **S**ecurity **S**ervice), που αναπτύχθηκαν από την εταιρία DEC (Digital Equipment Corporation), προσφέρουν επίσης αμοιβαία πιστοποίηση και ανταλλαγή κλειδιού. Το DASS χρησιμοποιεί τόσο συμμετρική όσο και ασύμμετρη κρυπτογραφία. Η Μαρία και ο Κώστας έχουν ο καθένας το προσωπικό ιδιωτικό του κλειδί, ενώ ο Δημοσθένης κρατάει υπογεγραμμένα αντίγραφα των δημοσίων κλειδιών τους. Το πρωτόκολλο έχει ως εξής:

1. Η Μαρία στέλνει μήνυμα στον Δημοσθένη, που περιέχει το όνομά του Κώστα.

$K\Omega$

2. Ο Δημοσθένης στέλνει στην Μαρία το δημόσιο κλειδί του Κώστα, $K_{K\Omega}$, υπογεγραμμένο με το ιδιωτικό κλειδί του, T. Στην υπογραφή περιλαμβάνεται και το όνομα του Κώστα

$S_T(K\Omega, K_{K\Omega})$

3. Η Μαρία βεβαιώνεται για την υπογραφή του Δημοσθένη και γνωρίζει έτσι, ότι το κλειδί που έλαβε είναι του Κώστα. Δημιουργεί ένα τυχαίο κλειδί συνόδου, K, και ένα τυχαίο ζεύγος ιδιωτικού-δημόσιο κλειδιού, K_P. Με το K κρυπτογραφεί μια χρονική σφραγίδα. Έπειτα κρυπτογραφεί με το ιδιωτικό της κλειδί, K_M, ένα χρόνο ζωής κλειδιού, το όνομά της και το K_P. Τέλος, κρυπτογραφεί το K με το δημόσιο κλειδί του Κώστα και το υπογράφει με το K_P. Στέλνει όλα τα παραπάνω στον Κώστα.

$E_K(T_M)$, $S_{KM}(L, MA, KP)$, $S_{KP}(E_{KK\Omega}(K))$

4. Ο Κώστας στέλνει μήνυμα στον Δημοσθένη (που μπορεί να είναι διαφορετικός από τον προηγούμενο), που περιέχει το όνομα της Μαρίας.

MA

5. Ο Δημοσθένης στέλνει στον Κώστα το δημόσιο κλειδί της Μαρίας, κρυπτογραφημένο με το ιδιωτικό κλειδί του, T. Η υπογραφή περιέχει και το όνομα της Μαρίας.

$S_T(MA, K_M)$

6. Ο Κώστας βεβαιώνεται για την υπογραφεί του Δημοσθένη, και πλέον γνωρίζει ότι το δημόσιο κλειδί που έλαβε είναι της Μαρίας. Έπειτα βεβαιώνεται για την υπογραφή της Μαρίας (από το βήμα 3) και ανακτά το K_P. Επιβεβαιώνει την υπογραφή με το K_P (πάλι από το βήμα 3) και χρησιμοποιεί το ιδιωτικό κλειδί του για να ανακτήσει το K. Τέλος, αποκρυπτογραφεί το T_M για να βεβαιωθεί ότι το μήνυμα είναι πρόσφατο.

7. Αν απαιτείται αμοιβαία πιστοποίηση, ο Κώστας κρυπτογραφεί μια νέα χρονική χρησιμοποιώντας το *K*, και τη στέλνει στη Μαρία.

$E_K(T_{K\Omega})$

8. Η Μαρία αποκρυπτογραφεί το $T_{K\Omega}$ με το *K* και βεβαιώνεται έτσι ότι το μήνυμα είναι πρόσφατο.

Το SPX, προϊόν της DEC, είναι βασισμένο στο DASS.

2.13 Το πλαίσιο πρωτοκόλλων πιστοποίησης ISO

Η κρυπτογραφία δημόσιου κλειδιού έχει προταθεί για χρήση στα πρωτόκολλα πιστοποίησης ISO (ISO Authentication Framework), γνωστά και ως πρωτόκολλα X.509. Το πλαίσιο των πρωτοκόλλων αυτών παρέχει διαδικασίες πιστοποίησης σε δίκτυο. Αν και δεν καθορίζεται κανένας συγκεκριμένος αλγόριθμος, είτε για κρυπτογράφηση είτε για πιστοποίηση, το πρότυπο προτείνει τον RSA. Έχει ληφθεί πρόνοια, πάντως, για διάφορους αλγόριθμους και συναρτήσεις hash. Το X.509 εκδόθηκε αρχικά το 1988. Ύστερα από ανάλυση και σχολιασμούς από τη διεθνή επιστημονική κοινότητα, το πρότυπο αναθεωρήθηκε το 1993, για να διορθωθούν μερικά προβλήματα ασφάλειας.

2.13.1 Πιστοποιητικά (certificates)

Το πιο σημαντικό κομμάτι του X.509 είναι η δομή των πιστοποιητικών δημοσίων κλειδιών. Κάθε χρήστης έχει ένα χαρακτηριστικό όνομα. Μια έμπιστη **Αρχή Πιστοποίησης** (ΑΠ) (Certification Authority [CA]) αναθέτει ένα μοναδικό όνομα σε κάθε χρήστη και εκδίδει ένα υπογεγραμμένο πιστοποιητικό, που περιέχει το όνομα και το δημόσιο κλειδί του χρήστη. Το Εικόνα 15.1 περιγράφει ένα πιστοποιητικό X.509.

Το πεδίο έκδοσης καθορίζει την μορφή του πιστοποιητικού. Ο σειριακός αριθμός είναι μοναδικός για την ΑΠ (κάτι σαν αύξων αριθμός). Το επόμενο πεδίο καθορίζει τον αλγόριθμο που χρησιμοποιήθηκε για την υπογραφή του πιστοποιητικού, μαζί με οποιεσδήποτε αναγκαίες παραμέτρους. Ο εκδότης είναι το όνομα της ΑΠ. Η διάρκεια ισχύος είναι ένα ζευγάρι αριθμών· το πιστοποιητικό είναι έγκυρο για το χρονικό διάστημα ανάμεσα στις δύο τιμές. Το πεδίο ‘Χρήστης’ είναι το όνομα του χρήστη. Αμέσως μετά περιλαμβάνονται πληροφορίες για το δημόσιο κλειδί του χρήστη, που περιλαμβάνουν το όνομα του αλγόριθμου, αναγκαίες παραμέτρους και το ίδιο το δημόσιο κλειδί. Το τελευταίο πεδίο είναι η υπογραφή της Αρχής.

Αν η Μαρία θέλει να επικοινωνήσει με τον Κώστα, παίρνει πρώτα το πιστοποιητικό του από την βάση και επιβεβαιώνει την γνησιότητά του. Αν και οι δύο χρησιμοποιούν την ίδια ΑΠ, τότε η Μαρία απλά επιβεβαιώνει την υπογραφή της Αρχής.

Αν χρησιμοποιούν διαφορετικές ΑΠ, τα πράγματα είναι πιο περίπλοκα. Οι διαφορετικές ΑΠ σχηματίζουν δομή δέντρου, με κάθε μία να πιστοποιεί κάποια άλλη. Στην κορυφή βρίσκεται η πρωτεύουσα ΑΠ. Κάθε ΑΠ έχει ένα πιστοποιητικό υπογεγραμμένο από την ΑΠ πάνω από αυτήν, και πιστοποιητικά υπογεγραμμένα από τις ΑΠ κάτω από αυτήν. Η Μαρία χρησιμοποιεί τα πιστοποιητικά αυτά για να βεβαιωθεί για το πιστοποιητικό του Κώστα.

Το πιστοποιητικό της Μαρίας εκδίδεται από την ΑΠ5 ο Κώστας πιστοποιείται από την ΑΠ4. Η Μαρία γνωρίζει το κλειδί της ΑΠ5. Η ΑΠ3 έχει ένα πιστοποιητικό υπογεγραμμένο από την ΑΠ5, το οποίο βεβαιώνει την Μαρία για την εγκυρότητα της ΑΠ3. Η ΑΠ2 έχει πιστοποιητικό υπογεγραμμένο από την ΑΠ3, οπότε βεβαιώνεται και η δική της εγκυρότητα. Η ΑΠ4 έχει πιστοποιητικό υπογεγραμμένο από την ΑΠ2. Η ΑΠ4, τέλος, υπογράφει το πιστοποιητικό του Κώστα. Γενικά, διασχίζοντας προς τα πάνω το δέντρο, φτάνουμε σε ένα κοινό σημείο (στη συγκεκριμένη περίπτωση το ΑΠ2), απ’ όπου κατεβαίνοντας (από άλλο κλαδί) φτάνουμε ως το άτομο του οποίο το δημόσιο κλειδί θέλουμε..

Τα πιστοποιητικά μπορούν να αποθηκευτούν σε βάσεις διεσπαρμένες σ’ όλο το δίκτυο. Οι χρήστες μπορούν να τα στέλνουν ο ένας στον άλλο. Όταν ένα πιστοποιητικό λήγει, θα πρέπει να απομακρύνεται από οποιονδήποτε δημόσιο κατάλογο. Η ΑΠ, όμως, θα πρέπει να κρατά αντίγραφο για να λύσει πιθανές μελλοντικές διαφορές.

Τα πιστοποιητικά μπορούν επίσης να ανακληθούν, είτε επειδή το ιδιωτικό κλειδί του χρήστη έχει διαρρεύσει, είτε επειδή το κλειδί της ΑΠ έχει διαρρεύσει, είτε επειδή η ΑΠ δεν θέλει να πιστοποιεί πια τον χρήστη. Κάθε ΑΠ θα πρέπει να συντηρεί μια λίστα (διαφορετική από εκείνη των ληγμένων πιστοποιητικών), που να περιέχει όλα τα ανακληθέντα πιστοποιητικά. Κάθε φορά που η Μαρία θα λαμβάνει ένα καινούργιο πιστοποιητικό, θα μπορεί να ελέγχει τη λίστα των ανακληθέντων πιστοποιητικών μέσω του δικτύου. Το πιο πιθανό, όμως, είναι να ελέγχει μια τοπικά σωσμένη λίστα.

Υπάρχουν σαφώς δυνατότητες παραβίασης του συστήματος· το πιο ευάλωτο σημείο φαίνεται να είναι τα ανακληθέντα πιστοποιητικά.

2.13.2 Πρωτόκολλα πιστοποίησης

Η Μαρία θέλει να επικοινωνήσει με τον Κώστα. Πρώτα ανατρέχει στην βάση δεδομένων και αποκτά το **μονοπάτι πιστοποίησης** (certification path) από αυτήν μέχρι το δημόσιο κλειδί του Κώστα. Έπειτα μπορεί να ακολουθήσει ένα πρωτόκολλο πιστοποίησης μονόδρομο, αμφίδρομο ή τριών κατευθύνσεων.

Το μονόδρομο πρωτόκολλο περιέχει ένα μοναδικό μήνυμα από την Μαρία προς τον Κώστα. Εξακριβώνονται οι ταυτότητες της Μαρίας και του Κώστα, και η ακεραιότητα των δεδομένων που στέλνονται από τη Μαρία στον Κώστα. Επίσης, το πρωτόκολλο καθιστά ανέφικτες τις επιθέσεις αναμετάδοσης (replay attacks).

Το αμφίδρομο πρωτόκολλο περιλαμβάνει και μία απάντηση από τον Κώστα. Αποδεικνύει ότι αυτός που έστειλε την απάντηση ήταν ο Κώστας, και όχι κάποιος άλλος. Εξασφαλίζει, επίσης, την μυστικότητα των δύο μηνυμάτων και αποτρέπει τις επιθέσεις αναμετάδοσης.

Τόσο το μονόδρομο όσο και το αμφίδρομο πρωτόκολλο χρησιμοποιούν χρονικές σφραγίδες. Το πρωτόκολλο τριών κατευθύνσεων περιλαμβάνει και ένα τρίτο μήνυμα από την Μαρία προς τον Κώστα και καταργεί την ανάγκη για χρονικές σφραγίδες (δηλαδή για πιστοποίηση χρόνου).

Το μονόδρομο πρωτόκολλο έχει ως εξής:

1. Η Μαρία δημιουργεί έναν τυχαίο αριθμό, R_M.

2. Η Μαρία δημιουργεί ένα μήνυμα, $M = (T_M, R_M, I_K, d)$, όπου T_M είναι η χρονική σφραγίδα της Μαρίας, $I_{K\Omega}$ είναι η ταυτότητα του Κώστα και το d είναι δεδομένα. Τα δεδομένα μπορούν να κρυπτογραφηθούν με το δημόσιο κλειδί του Κώστα, K_K, για ασφάλεια.

3. Η Μαρία στέλνει το $(C_M, S_M(M))$ στον Κώστα. (C_M είναι το πιστοποιητικό της Μαρίας· S_M είναι η υπογραφή της)

4. Ο Κώστας βεβαιώνεται για την ισχύ του C_M και ανακτά το K_M (το δημόσιο κλειδί της Μαρίας). Βεβαιώνεται ότι το κλειδί δεν έχει λήξει.

5. Χρησιμοποιεί το K_M για να βεβαιωθεί για την υπογραφή της Μαρίας. Έτσι σιγουρεύεται και για την ακεραιότητα του μηνύματος.

6. Ο Κώστας ελέγχει αν το I_K είναι ακριβές.

7. Ο Κώστας ελέγχει το T_M και βεβαιώνεται ότι το μήνυμα δεν είναι παλιό.

8. Προαιρετικά, ο Κώστας μπορεί να ελέγξει αν το R_M είναι ήδη καταχωρημένο σε μια βάση που κρατά τους τυχαίους αριθμούς προηγούμενων μηνυμάτων

Το αμφίδρομο πρωτόκολλο αποτελείται από το μονόδρομο, ακολουθούμενο από ένα παρόμοιο μονόδρομο πρωτόκολλο, που εκτελεί ο Κώστας προς την Μαρία. Μετά την εκτέλεση των βημάτων 1-8 του μονόδρομου πρωτοκόλλου, το αμφίδρομο πρωτόκολλο συνεχίζει ως εξής:

9. Ο Κώστας δημιουργεί έναν άλλο τυχαίο αριθμό, R_K.

10. Ο Κώστας δημιουργεί ένα μήνυμα $M' = (T_K, R_K, I_M, R_M, d)$, όπου T_K είναι η χρονική σφραγίδα του Κώστα, I_M είναι η ταυτότητα της Μαρίας, και το d είναι δεδομένα. Τα δεδομένα μπορούν να κρυπτογραφηθούν με το δημόσιο κλειδί της Μαρίας, K_M, για ασφάλεια. Το R_M είναι ο τυχαίος αριθμός που δημιούργησε η Μαρία στο βήμα 1.

11. Ο Κώστας στέλνει το $S_K(M')$ στην Μαρία.

12. Η Μαρία χρησιμοποιεί το K_K για να βεβαιωθεί για την υπογραφή του Κώστα. Παράλληλα, σιγουρεύεται για την ακεραιότητα του μηνύματος.

13. Η Μαρία ελέγχει αν το I_M είναι ακριβές.

14. Η Μαρία ελέγχει το T_K και βεβαιώνεται ότι το μήνυμα δεν είναι παλιό.

15. Προαιρετικά, η Μαρία μπορεί να ελέγξει αν το R_K είναι ήδη καταχωρημένο σε μια βάση που κρατά τους τυχαίους αριθμούς προηγούμενων μηνυμάτων.

Το πρωτόκολλο τριών κατευθύνσεων πετυχαίνει ότι και το αμφίδρομο, αλλά χωρίς χρονικές σφραγίδες. Τα βήματα 1-15 είναι τα ίδια με το αμφίδρομο πρωτόκολλο, θεωρώντας $T_M = T_K = 0$.

16. Η Μαρία συγκρίνει το R_M που λαμβάνει στο βήμα 11, σε σχέση με το R_M που δημιούργησε στο βήμα 1.

17. Η Μαρία στέλνει το $S_M(R_K)$ στον Κώστα.

18. Ο Κώστας χρησιμοποιεί το K_M για να βεβαιωθεί για την υπογραφή της Μαρίας. Παράλληλα, σιγουρεύεται για την ακεραιότητα του μηνύματος.

19. Ο Κώστας συγκρίνει το R_K που λαμβάνει στο βήμα 17, σε σχέση με το R_K που δημιούργησε στο βήμα 9.

2.14 Κρυπτογράφηση διαύλων επικοινωνίας

Η Μαρία θέλει να στείλει με ασφάλεια ένα μήνυμα στον Κώστα, οπότε το κρυπτογραφεί. Που λαμβάνει χώρα αυτή η κρυπτογράφηση;

Θεωρητικά, η κρυπτογράφηση μπορεί να υλοποιηθεί σε οποιοδήποτε από τα επίπεδα του μοντέλου OSI (Open Systems Interconnect). Στην πράξη υλοποιείται είτε στα κατώτερα είτε στα ανώτερα επίπεδα. Αν λαμβάνει χώρα στα κατώτερα επίπεδα, ονομάζεται **κρυπτογράφηση ανά σύνδεση** (link-by-link encryption). Όλα τα δεδομένα που περνούν από μία συγκεκριμένη σύνδεση κρυπτογραφούνται. Αν λαμβάνει χώρα στα ανώτερα επίπεδα ονομάζεται **κρυπτογράφηση στα άκρα** (end-to-end encryption). Τα δεδομένα κρυπτογραφούνται κατ' επιλογή, στέλνονται στο δίκτυο και αποκρυπτογραφούνται στο άλλο άκρο. Κάθε τεχνική έχει θετικά και αρνητικά σημεία.

2.14.1 Κρυπτογράφηση ανά σύνδεση

Το πιο εύκολο είναι η κρυπτογράφηση να υλοποιηθεί στο φυσικό επίπεδο. Η διασύνδεση στο φυσικό επίπεδο χρησιμοποιεί, γενικά, γνωστά πρότυπα. Είναι, λοιπόν, εύκολο να χρησιμοποιήσουμε συσκευές κρυπτογράφησης, που συνδέονται εύκολα στην ήδη υπάρχουσα υποδομή. Οι συσκευές αυτές κρυπτογραφούν όλα τα δεδομένα που περνούν απ' αυτές, συμπεριλαμβανομένων των δεδομένων, των πληροφοριών δρομολόγησης και πληροφοριών σχετικών με το πρωτόκολλο. Μπορούν να χρησιμοποιηθούν σε οποιαδήποτε ψηφιακή σύνδεση. Από την άλλη μεριά, όμως, πρέπει κάθε φορά που τα δεδομένα περνούν από έναν κόμβο να αποκρυπτογραφούνται.

Το είδος αυτό της κρυπτογραφίας είναι πολύ αποτελεσματικό. Ο αντίπαλος δεν έχει ιδέα για την δομή της πληροφορίας στο δίαυλο. Δεν έχει ιδέα ποιος μιλάει σε ποιόν, πόσο μακριά είναι τα μηνύματα, τι ώρα της ημέρας επικοινωνούν κτλ. Αυτό ονομάζεται **ασφάλεια επικοινωνιακής ροής (traffic-flow security)**.

Η διαχείριση κλειδιών είναι επίσης εύκολη μόνο τα άκρα χρειάζεται να έχουν κοινό κλειδί και μπορούν να το αλλάξουν ανεξάρτητα από το υπόλοιπο δίκτυο.Το μεγαλύτερο πρόβλημα είναι ότι κάθε σύνδεση στο φυσικό επίπεδο, από το ένα άκρο μέχρι το άλλο, πρέπει να κρυπτογραφηθεί. Αν μείνει έστω και ένα κομμάτι της σύνδεσης μη κρυπτογραφημένο, χάνεται η ασφάλεια όλου του συστήματος. Για μεγάλα δίκτυα το κόστος της υλοποίησης ενός τέτοιου σχήματος είναι απαγορευτικό.

Επιπλέον, κάθε κόμβος στο δίκτυο πρέπει να προστατεύεται, καθώς εκεί τα δεδομένα αποκρυπτογραφούνται.

Κρυπτογράφηση ανά σύνδεση: υπέρ και κατά

Υπέρ:

Ευκολότερη λειτουργία, μια που η διαδικασία μπορεί να είναι αόρατη στον χρήστη.
Απαιτείται μόνο ένα ζεύγος κλειδιών για κάθε σύνδεση.
Παρέχει ασφάλεια επικοινωνιακής ροής, αφού οι πληροφορίες δρομολόγησης είναι κρυπτογραφημένες.
Η κρυπτογράφηση γίνεται online.

Κατά:

Τα δεδομένα είναι εκτεθειμένα σε κάθε κόμβο.
Η μετάδοση των δεδομένων είναι πιο αργή.

2.14.2 Κρυπτογράφηση στα άκρα

Μια άλλη προσέγγιση είναι η κρυπτογράφηση να λαμβάνει χώρα ανάμεσα στο επίπεδο δικτύου και στο επίπεδο μεταφοράς. Η συσκευή κρυπτογράφησης πρέπει να γνωρίζει την δομή των δεδομένων μέχρι το τρίτο επίπεδο (και ανάλογα με το πρωτόκολλο) και να κρυπτογραφεί μόνο τις μονάδες μεταφοράς δεδομένων (transport data units).

Αυτή η προσέγγιση αποφεύγει το πρόβλημα της συνεχούς κρυπτογράφησης και αποκρυπτογράφησης που υπάρχει στο φυσικό επίπεδο. Παρέχει κρυπτογράφηση στα άκρα και ως εκ τούτου τα δεδομένα παραμένουν κρυπτογραφημένα καθ’ όλη την μεταφορά τους (Εικόνα 17.2). Το βασικό πρόβλημα είναι ότι η πληροφορίες δρομολόγησης δεν είναι κρυπτογραφημένες. Ένας καλός κρυπταναλυτής-παρατηρητής μπορεί να καταλάβει αρκετά, αν γνωρίζει ποιος μιλάει σε ποιόν, ποιες ώρες της ημέρας, για πόσο διάστημα κτλ. Η κατασκευή συσκευών κρυπτογράφησης στα άκρα είναι δύσκολη, γιατί πρέπει να υπάρχουν διαφορετικές συσκευές για κάθε σύστημα που υλοποιεί τα δικά του πρωτόκολλα.

Αν η κρυπτογράφηση γίνεται σε ανώτερο επίπεδο της επικοινωνιακής αρχιτεκτονικής, όπως το επίπεδο παρουσίασης ή το επίπεδο εφαρμογής, τότε μπορεί να είναι ανεξάρτητη της επικοινωνιακής υποδομής που χρησιμοποιείται. Είναι κρυπτογράφηση στα άκρα, αλλά η υλοποίηση δεν χρειάζεται να απασχοληθεί με τη διαμόρφωση της γραμμής, τα modem κοκ. Η τεχνική αυτή είναι ένα στάδιο πιο πάνω από την off-line κρυπτογράφηση.

Η κρυπτογράφηση στα επίπεδα αυτά έχει να κάνει με το λογισμικό που χρησιμοποιεί ο χρήστης, το οποίο πρέπει να είναι βέλτιστα υλοποιημένο, ανάλογα με το υπολογιστικό σύστημα στο οποίο τρέχει. Η κρυπτογράφηση μπορεί να γίνεται απ' το λογισμικό ή από ειδικευμένες συσκευές.Το σημαντικότερο μειονέκτημα είναι ότι επιτρέπει ανάλυση της επικοινωνιακής ροής.

Κρυπτογράφηση στα άκρα: υπέρ και κατά

Υπέρ:

Υψηλότερος βαθμός ασφάλειας.

Κατά:

Απαιτείται πιο πολύπλοκο σύστημα διαχείρισης κλειδιών.

Επιτρέπει την ανάλυση της επικοινωνιακής ροής.

Η κρυπτογράφηση γίνεται off-line.

2.14.3 Συνδυάζοντας τις δύο τεχνικές

Ο συνδυασμός των δύο τεχνικών είναι η πιο ακριβή, αλλά και πιο σίγουρη μέθοδος για την ασφάλεια ενός δικτύου. Η κρυπτογράφηση ανά σύνδεση αποκρύπτει τις πληροφορίες δρομολόγησης, ενώ η κρυπτογράφηση στα άκρα διατηρεί τα δεδομένα ασφαλή και μέσα στους κόμβους του δικτύου.

2.15 Πληροφοριακή θεωρία (information theory)

Η σύγχρονη πληροφοριακή θεωρία δημοσιεύτηκε για πρώτη φορά το 1948 από τον Claude Elmwood Shannon. Παρακάτω παρουσιάζονται μερικές βασικές ιδέες.

2.15.1 Εντροπία και αβεβαιότητα

Η πληροφοριακή θεωρία ορίζει την ποσότητα της πληροφορίας σε ένα μήνυμα ως τον ελάχιστο αριθμό bit που απαιτούνται για να απεικονίσουμε όλα τα δυνατά νοήματα του μηνύματος αυτού, θεωρώντας ότι όλα τα μηνύματα είναι το ίδιο

πιθανά. Για παράδειγμα ένα πεδίο που αποθηκεύει τις μέρες της εβδομάδος δεν θα ήταν πάνω από 3 bit, γιατί η πληροφορία αυτή μπορεί να απεικονιστεί με 3 bit:

000 = Κυριακή

001 = Δευτέρα

010 = Τρίτη

011 = Τετάρτη

100 = Πέμπτη

101 = Παρασκευή

110 = Σάββατο

111 = Δεν χρησιμοποιείται

Ένα πεδίο που αποθηκεύει το φύλο περιέχει μόνο ένα bit πληροφορίας, παρόλο που μπορεί να αποθηκεύεται ως ένα string 7 byte.

Τυπικά, η ποσότητα της πληροφορίας σε ένα μήνυμα *M* μετριέται με την εντροπία του μηνύματος, που συμβολίζεται με H(*M*). Η εντροπία ενός μηνύματος που περιέχει το φύλο είναι 1 bit η εντροπία ενός μηνύματος που αναφέρει την μέρα της εβδομάδος είναι κάτι λιγότερο από 3. Γενικά, η εντροπία ενός μηνύματος είναι $\log_2 n$, όπου n είναι ο αριθμός των δυνατών εννοιών, και μετριέται σε bit. Αυτός ο ορισμός θεωρεί ότι κάθε έννοια έχει την ίδια πιθανότητα.

Η εντροπία ενός μηνύματος μετράει και την αβεβαιότητά του. Αυτή είναι ο αριθμός των bit του αρχικού κειμένου που χρειάζεται να ανακτήσουμε, όταν το κείμενο είναι κρυπτογραφημένο, για να μάθουμε ποιο είναι το αρχικό κείμενο. Για παράδειγμα, αν το «*(&AT6» είναι κομμάτι ενός κρυπτογραφήματος που σημαίνει είτε «ΑΝΔΡΑΣ» είτε «ΓΥΝΑΙΚΑ», τότε η αβεβαιότητα του μηνύματος είναι 1. Χρειάζεται να ανακτήσουμε ένα καλά διαλεγμένο bit για να μάθουμε το μήνυμα.

2.15.2 Η τάξη μιας γλώσσας

Για μια δεδομένη γλώσσα, ονομάζουμε τάξη της γλώσσας (rate of the language) το

r = H(*M*)/N

όπου N είναι το μήκος του μηνύματος. Η τάξη στα Αγγλικά παίρνει διάφορες τιμές, από 1,0 ως 1,5 bit/γράμμα, για μεγάλες τιμές του N. Γενικά, το 1,3 είναι μια αποδεκτή τιμή. Η απόλυτη τάξη (absolute rate) μιας γλώσσας είναι ο μέγιστος αριθμός bit που μπορούν να αντιστοιχούν σε ένα χαρακτήρα, θεωρώντας ότι κάθε ακολουθία χαρακτήρων είναι το ίδιο πιθανή. Αν υπάρχουν L χαρακτήρες σε μια γλώσσα, η απόλυτη τάξη είναι:

$R = \log_2 L$

Αυτή είναι η μέγιστη εντροπία των χαρακτήρων. Για τα Αγγλικά η απόλυτη τάξη είναι $\log_2 26$ ή περίπου 4,7 bit/γράμμα. Είναι φυσικό η πραγματική τάξη να είναι μικρότερη από την απόλυτη, γιατί οι γλώσσες είναι πλεονάζουσες.

Ο **πλεονασμός** (redundancy) μιας γλώσσας, *D*, ορίζεται ως:

$D = R - r$

Για τα Αγγλικά, που έχουν τάξη 1,3, ο πλεονασμός είναι 3,4 bit/γράμμα. Ένα κείμενο ASCII, που είναι απλά ένα αγγλικό κείμενο, έχει 1,3 bit πληροφορίας ανά γράμμα, δηλαδή ανά byte. Αυτό σημαίνει ότι το κάθε byte έχει 8-1,3=6,7 bit πλεονάζουσας πληροφορίας και το κάθε bit έχει 6,7/8=0,84 bit πλεονάζουσας πληροφορίας. Η εντροπία είναι 0,16 bit πληροφορίας για κάθε bit ASCII κειμένου.

17.3.3 Ασφάλεια ενός κρυπτοσυστήματος

Ο Shannon καθόρισε ένα ακριβές μαθηματικό μοντέλο για το τι σημαίνει να είναι ασφαλές ένα κρυπτοσύστημα. Ο στόχος του κρυπταναλυτή είναι να ανακτήσει το κλειδί, *K*, το αρχικό κείμενο, *P*, ή και τα δύο. Όμως, μπορεί να είναι ικανοποιημένος με την απόκτηση κάποιας πιθανολογικής πληροφορίας σχετικής με το *P*: ότι είναι ψηφιοποιημένος ήχος, κείμενο στα Ρωσικά κοκ.

Στις περισσότερες περιπτώσεις ο κρυπταναλυτής γνωρίζει εκ των προτέρων κάποια πιθανολογική πληροφορία. Καταρχήν, πιθανότατα γνωρίζει την γλώσσα (αν πρόκειται για κείμενο). Αν είναι ένα μήνυμα για τον Κώστα, τότε μάλλον θα αρχίζει με «Αγαπητέ Κώστα» κοκ. Στόχος του αναλυτή είναι να μεταβάλλει τις πιθανότητες που σχετίζονται με κάθε πιθανό κείμενο. Τελικά κάποιο κείμενο θα αναδειχτεί ως το πιθανότερο αρχικό κείμενο.

Για να παρέχει ένα κρυπτοσύστημα **τέλεια ασφάλεια** (perfect security) θα πρέπει το κρυπτογράφημα να μην φανερώνει καμία πληροφορία για το αρχικό κείμενο. Αυτό, είπε ο Shannon, μπορεί να γίνει μόνο αν ο αριθμός των πιθανών κλειδιών είναι τουλάχιστο όσο μεγάλος είναι και ο αριθμός των πιθανών μηνυμάτων. Με άλλα λόγια, θα πρέπει το κλειδί να έχει μήκος τουλάχιστο ίσο με το κείμενο, και κανένα κλειδί δεν θα πρέπει να χρησιμοποιείται ξανά. Περιέγραψε, δηλαδή, το on-time pad.

Γενικά, όμως, κάθε κρυπτογράφημα φανερώνει κάποια πληροφορία για το αρχικό κείμενο. Δουλειά ενός καλού κρυπτογραφικού αλγόριθμου είναι να ελαττώσει αυτήν την πληροφορία στο ελάχιστο· δουλειά του κρυπταναλυτή είναι να εκμεταλλευτεί την πληροφορία για να ανακτήσει το κείμενο.

Οι κρυπταναλυτές στηρίζονται στον πλεονασμό μιας γλώσσας για να μειώσουν τον αριθμό των πιθανών αρχικών κειμένων. Αυτός είναι και ο λόγος που πολλές κρυπτογραφικές εφαρμογές πρώτα συμπιέζουν το κείμενο και μετά το κρυπτογραφούν. Η συμπίεση μειώνει τον πλεονασμό της γλώσσας, και παράλληλα μειώνει το μέγεθος της εργασίας κρυπτογράφησης και αποκρυπτογράφησης.
309

Η εντροπία ενός κρυπτοσυστήματος είναι συνάρτηση του μεγέθους του συνόλου των δυνατών κλειδιών, *K*. Υπολογίζεται προσεγγιστικά από τον τύπο:

$$H(K) = \log_2 K$$

Ένα κρυπτοσύστημα με μήκος κλειδιού 64 bit έχει εντροπία 64 bit. Γενικά, όσο πιο μεγάλη η εντροπία, τόσο δυσκολότερο είναι να σπάσει το κρυπτοσύστημα.

17.3.4 Απόσταση μοναδικότητας (unicity distance)

Για ένα κρυπτογραφημένο μήνυμα μήκους *n*, ο αριθμός των διαφορετικών κλειδιών που το αποκωδικοποιούν σε κάποιο κείμενο, που να έχει νόημα στη γλώσσα στην οποία γράφτηκε, δίνεται από τον τύπο:

$$2^{H(K)-nD} - 1$$

Ο Shannon καθόρισε ως **απόσταση μοναδικότητας**, *U*, καλούμενη και σημείο μοναδικότητας, μια προσέγγιση της ποσότητας κρυπτογραφήματος, η οποία είναι τόση ώστε το άθροισμα της εντροπίας (πραγματικής πληροφορίας), που υπάρχει στο αρχικό κείμενο, και της εντροπίας του κλειδιού κρυπτογράφησης, να ισούται με τον αριθμό των bit του κρυπτογραφήματος που χρησιμοποιούμε. Έπειτα έδειξε ότι κρυπτογραφήματα με μήκος μεγαλύτερο της απόστασης αυτής, είναι σχεδόν σίγουρο ότι έχουν μία μοναδική λογική αποκρυπτογράφηση. Κρυπτογραφήματα αρκετά μικρότερα της απόστασης αυτής ενδέχεται να έχουν πολλαπλές, το ίδιο πιθανές αποκρυπτογραφήσεις. Ως εκ τούτου είναι πιο ασφαλή, καθώς ο αντίπαλος έχει δυσκολία να διαλέξει τη σωστή αποκρυπτογράφηση.

Η απόσταση μοναδικότητας υπολογίζεται, για τα περισσότερα κρυπτοσυστήματα, ως ο λόγος της εντροπίας του κρυπτοσυστήματος προς τον πλεονασμό της γλώσσας.

$$U = H(K)/D$$

Η απόσταση μοναδικότητας δεν παράγει απόλυτες προβλέψεις, αλλά δίνει πιθανολογικά αποτελέσματα. Η απόσταση μοναδικότητας υπολογίζει την ελάχιστη ποσότητα κρυπτογραφήματος για το οποίο το πιθανότερο είναι να υπάρχει ένα μοναδικό λογικό αρχικό κείμενο στο οποίο να αποκρυπτογραφείται. Γενικά, όσο μεγαλύτερη η απόσταση αυτή, τόσο καλύτερο είναι το κρυπτοσύστημα. Η κρυπτογράφηση αγγλικού κειμένου με τον DES (που έχει 56 bit κλειδί) έχει απόσταση μοναδικότητας περίπου 8,2 χαρακτήρες ή 66 bit. Ο πίνακας 17.3 δίνει την απόσταση μοναδικότητας για διάφορα κλειδιά.

Γνήσιοι τυχαίοι αριθμοί πληρούν την ιδιότητα της μη προβλεψιμότητας, αφού δεν εξαρτώνται ο ένας από τον άλλο. Χρησιμοποιούνται όμως ακόμα μάλλον σπάνια, αφού δεν είναι εύκολη η απόκτησή τους. Άλλωστε, η αναπαραγωγή τους δεν είναι δυνατή, κάτι που αποτελεί μειονέκτημα, όταν μας απασχολεί ο τρόπος διανομής των ακολουθιών τυχαίων αριθμών. Παρατηρούμε ότι η έλλειψη δυνατότητας αναπαραγωγής μιας τυχαίας ακολουθίας υποδηλώνει την επιθυμητή ιδιότητα της μη προβλεψιμότητας. Ωστόσο, για λόγους αποτελεσματικής διακίνησης των τυχαίων ακολουθιών, αποτελεί η δυνατότητα αναπαραγωγής απαίτηση της μεθόδου δημιουργίας της ακολουθίας.
Κατά κανόνα, ακολουθίες που συμπεριφέρονται όπως οι τυχαίες ακολουθίες παράγονται με τη βοήθεια αλγόριθμων, των γεννητριών (ψευδο –) τυχαίων ακολουθιών. Πολλές από αυτές τις γεννήτριες βασίζονται σε κρυπτογραφικά συστήματα, συμμετρικά και ασύμμετρα. Αυτές οι γεννήτριες θεωρούνται κατάλληλες για κρυπτογραφικές εφαρμογές εφόσον θεωρούνται και τα αντίστοιχα κρυπτογραφικά συστήματα ως ασφαλή.

Πίνακας 17.3
Αποστάσεις μοναδικότητας κειμένων ASCII κρυπτογραφημένα

με διάφορα μήκη κλειδιών Μήκος κλειδιού (σε bit)	Απόσταση μοναδικότητα χαρακτήρες)
40	5,9
56	8,2
64	9,4
80	11,8
128	18,8
256	37,6

3.1 Data Encryption Standard (DES)

3.1.1 Ιστορία του DES

Το Πρότυπο Κρυπτογράφησης Δεδομένων (Data Encryption Standard [DES]), αλλιώς γνωστός ως Αλγόριθμος Κρυπτογράφησης Δεδομένων (Data Encryption Algorithm [DEA]) για την ANSI και DEA-1 για τον ISO, είναι παγκόσμιο πρότυπο εδώ και 23 χρόνια. Αν και δείχνει σημάδια γήρατος, έχει αντέξει ιδιαίτερα καλά απέναντι σε χρόνια κρυπτανάλυσης, και παρέχει ασφάλεια ακόμα και σήμερα απέναντι σε όλους εκτός από τους πιο δυνατούς αντιπάλους.

Το 1972 η Εθνική Υπηρεσία Προτύπων των ΗΠΑ (National Bureau of Standards [NBS]), που τώρα είναι γνωστή ως Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology [NIST]), έθεσε σε εφαρμογή ένα πρόγραμμα για την προστασία των δεδομένων σε υπολογιστές και επικοινωνίες.

Στις 15 Μαίου, 1973, η NBS εξέδωσε μια δημόσια αίτηση για προτάσεις αλγορίθμων κρυπτογράφησης. Η ανταπόκριση του κοινού έδειξε ότι υπήρχε σημαντικό ενδιαφέρον στα κρυπτογραφικά πρότυπα, αλλά έλειπε η πείρα στον τομέα αυτό.

Η NBS εξέδωσε μια δεύτερη αίτηση στις 27 Αυγούστου, 1974. Τελικά έλαβαν μια ελπιδοφόρα πρόταση από την IBM. Η IBM είχε δουλέψει πάνω σε έναν αλγόριθμο, ονόματι Lucifer, από το 1970. Ο αλγόριθμος, αν και περίπλοκος, ήταν καλά δομημένος.

Η NBS ζήτησε την βοήθεια της NSA για να αποφανθεί για την ασφάλεια που προσέφερε ο αλγόριθμος και την καταλληλότητά του για ομοσπονδιακό πρότυπο. Τελικά η NBS κατέληξε με την IBM στους όρους της συμφωνίας και έλαβε την μη αποκλειστική άδεια να παράγει και να πουλά μηχανήματα που χρησιμοποιούσαν τον αλγόριθμο, χωρίς να πληρώνει δικαιώματα στην IBM.

Στις 17 Μαρτίου, 1975, η NBS δημοσίευσε τόσο τις λεπτομέρειες του αλγορίθμου, όσο και την δήλωση της IBM για παραίτηση από τα δικαιώματα του αλγορίθμου. Κατόπιν, την 1 Αυγούστου, 1975, η NBS ζήτησε σχόλια και κριτικές για τον αλγόριθμο από εταιρίες και το ευρύ κοινό.

Πολλοί ήταν σκεπτικοί για την ανάμιξη της NSA. Φοβόταν μήπως η NSA είχε τροποποιήσει τον αλγόριθμο και εγκαταστήσει μια καταπακτή. Παράπονα υπήρχαν και για την μείωση του κλειδιού από 128 bit σε 56 bit.

Το 1976 έγιναν δύο συνέδρια, διοργανωμένα από την NBS, για να εκτιμηθεί το προτεινόμενο πρότυπο. Παρά την κριτική, η NBS καθιέρωσε τον αλγόριθμο ως πρότυπο στις 23 Νοεμβρίου, 1976. Η επίσημη περιγραφή του προτύπου, FIPS PUB 46, «Data Encryption Standard» δημοσιεύτηκε στις 15 Ιανουαρίου, 1975, και μπήκε σε ισχύ έξι μήνες αργότερα. Η NBS δημοσίευσε και άλλα σχετικά πρότυπα: FIPS PUB 81 «Τρόποι χρήσης του DES», FIPS PUB 74 «Οδηγίες για την εφαρμογή και χρήση του DES» κ.α.

Τα πρότυπα αυτά ήταν πρωτόγνωρα. Ποτέ στο παρελθόν δεν είχε γίνει γνωστός κάποιος αλγόριθμος εξετασμένος από την NSA. Αυτό ήταν μάλλον το αποτέλεσμα σύγχυσης. Η NSA πίστεψε ότι ο DES είναι υλοποιήσιμος μόνο σε hardware. Το πρότυπο καθόριζε υλοποίηση σε hardware, αλλά η NBS

δημοσίευσε αρκετές πληροφορίες ώστε να είναι δυνατόν να γραφεί και σε πρόγραμμα. Ανεπίσημα, η NSA χαρακτήρισε τον DES ως ένα από τα μεγαλύτερα λάθη της. Αν γνώριζε ότι οι λεπτομέρειες θα γίνονταν γνωστές και ότι ο κόσμος θα μπορούσε να γράψει λογισμικό που να τον χρησιμοποιεί, δεν θα είχαν ποτέ συμφωνήσει. Ο DES ισχυροποίησε το πεδίο της κρυπτανάλυσης περισσότερο από οτιδήποτε άλλο. Οι επιστήμονες είχαν τώρα στα χέρια τους έναν αλγόριθμο, που η NSA θεωρούσε ασφαλή. Δεν ήταν τυχαίο, ότι το επόμενο κυβερνητικό πρότυπο αλγόριθμου διαβαθμίστηκε.

Το πρότυπο καθόριζε ότι κάθε 5 χρόνια θα εξεταζόταν εκ νέου η καταλληλότητά του. Το 1983 το πρότυπο εγκρίθηκε ξανά, χωρίς καμία αντίδραση. Το 1987 η NSA πρότεινε την αντικατάστασή του από το πρόγραμμα CCEP (Commercial COMSEC Endorsement Program), θεωρώντας ότι ήταν πλέον πολύ πιθανό ότι σύντομα κάποιος θα έσπαγε τον DES. Σ’ αυτό υπήρξε αντίδραση, με την λογική ότι πολλές εταιρίες (κυρίως χρηματιστηριακές) χρησιμοποιούσαν ήδη τον αλγόριθμο και αλλαγή του προτύπου θα την άφηνε απροστάτευτες. Τελικά το πρότυπο εγκρίθηκε ξανά. Το 1992 ακόμα δεν υπήρχε αντικαταστάτης για τον DES. Το NIST (πρώην NBS) ζήτησε ξανά νέα έγκριση του προτύπου, με προϋπόθεση αυτή τη φορά, όμως, να γίνουν στο διάστημα των επόμενων πέντε χρόνων σαφής προετοιμασίες για την αλλαγή του προτύπου.

Για να ανταποκριθεί στη συνεχώς αυξανόμενη απαίτηση για αντικατάσταση του DES, το NIST ανακοίνωσε τον Ιανουάριο του 1997 το πρόγραμμα AES (Advanced Encryption Standard). Οι αλγόριθμοι έπρεπε να είναι τύπου μπλοκ, με μέγεθος μπλοκ 128 bit και μεγέθη κλειδιού 128, 192 και 256 bit. Οι υποψηφιότητες θα κρίνονταν με βάση την ασφάλειά, την ταχύτητα, την ευελιξία και την απλότητά τους. Οι προτάσεις έπρεπε να κατατεθούν μέχρι τον Ιούνιο του 1998, και τον Αύγουστο του 1998 δεκαπέντε υποψήφιοι παρουσίασαν τους αλγορίθμους τους στο 1ο Συνέδριο Υποψήφιων AES. Οι αλγόριθμοι είναι οι παρακάτω:

• CAST-256. Ανήκει στην οικογένεια των αλγορίθμων CAST, που σχεδιάστηκαν από τον Carlisle Adams. Απ’ όσο γνωρίζουμε, κανένας αλγόριθμός του δεν έχει σπάσει.

• LOKI-97. Όπως οι LOKI-89 και LOKI-91, έτσι κι αυτός αναλύθηκε με διαφορική επίθεση.

• Frog. Προτάθηκε από την TechApro International. Η παρουσίαση του έγινε από τον Διανέλο Γεωργούδη. Ο αλγόριθμος αναλύθηκε πριν καν το πρώτο συνέδριο.

• MARS. Η IBM ήταν αυτή που έφτιαξε τον DES και ο Mars είναι η πρότασή της για το νέο πρότυπο.

• Magenta. Ο αλγόριθμος αναλύθηκε κατά τη διάρκεια του πρώτου συνεδρίου.

• RC6. Η υποψηφιότητα αυτή από τον Ron Rivest και συναδέλφους του από την RSA Data Security Inc.

• Decorrelated Fast Cipher (DFC). Η υποψηφιότητα αυτή προέρχεται από το CNRS - Centre National pour la Recherche Scientifique - Ecole Normale Superieure και σχεδιάστηκε από τον Serge Vaudenay.

• Serpent. Ο αλγόριθμος είναι σχεδιασμένος από τον Eli Biham και τον Lars Knudsen, δύο από τους καλύτερους κρυπταναλυτές.

• E2. Ο αλγόριθμος αυτός σχεδιάστηκε από την NTT (Nippon Telegraph and Telecom).

• Rijndael. Είναι βασισμένος στον αλγόριθμο Square και φαίνεται να είναι δυνατός αλγόριθμος. Σχεδιάστηκε από τους Vincent Rijmen και Joan Daemen.

• DEAL. Αποτελεί παραλλαγή του τριπλού DES. Σχεδιάστηκε από τον Lars Knudsen.

• Hasty Pudding Cipher (HPC). Σχεδιάστηκε από τον Rich Schroeppel.

• Crypton. Κι αυτός ο αλγόριθμος είναι παραλλαγή του Square. Σχεδιάστηκε από την Future Systems Inc. και παρουσιάστηκε από τον Chae Hoon Lim.

• Twofish. Ο αλγόριθμος σχεδιάστηκε από τους Bruce Schneier, John Kelsey, Chris Hall και Niels Ferguson της Counterpane Systems, τον Doug Whiting της Hi/Fn Inc. και τον David Wagner του Πανεπιστημίου της Καλιφόρνια στο Berkley. Αποτελεί παραλλαγή του Blowfish.

• SAFER+. Ανήκει στην οικογένεια των αλγορίθμων SAFER. Προτάθηκε από την Cylink Corporation και σχεδιάστηκε εν μέρει από τον James Massey.

Το NIST διοργάνωσε ένα δεύτερο συνέδριο στις 22 Μαρτίου, 1999, στην Ρώμη. Στο συνέδριο κατατέθηκαν διάφορες εργασίες (συνολικά 28) που αποτελούσαν έρευνα πάνω στους υποψήφιους αλγόριθμους.

Στις 9 Αυγούστου, 1999, το NIST ανακοίνωσε τους πέντε φιναλίστες. Αυτοί ήταν οι :

• MARS

• RC6

• Rijndael

• Serpent

• Twofish

Οι τελικοί αυτοί υποψήφιοι πέρασαν έναν τελευταίο γύρο εξέτασης και στις 13-14 Απριλίου 2000, το NIST διοργάνωσε το τρίτο και τελικό συνέδριο, στο οποίο παρουσιάστηκαν τεχνικές αναλύσεις πάνω στους αλγόριθμους και συζητήθηκαν απόψεις σχετικά με το ποιος ή ποιοι θα πρέπει να είναι οι νικητές. Το NIST ζήτησε την τεχνική βοήθεια της NSA για την διεξαγωγή ενός βασικού συγκριτικού τεστ των αλγορίθμων, με κριτήριο την απόδοσή τους σε hardware. Στις 15 Μαίου 2000 η NSA παρέδωσε στο NIST την τελική της έκθεση αξιολόγησης: «Εξομοίωση της Απόδοσης σε hardware των Αλγορίθμων 2ου γύρου του AES (Hardware Performance Simluations of Round 2 Advanced Encryption Standard Algorithms)». Τελικά, στις 2 Οκτωβρίου 2000 το NIST επέλεξε τον Rijndael ως προτεινόμενο AES.

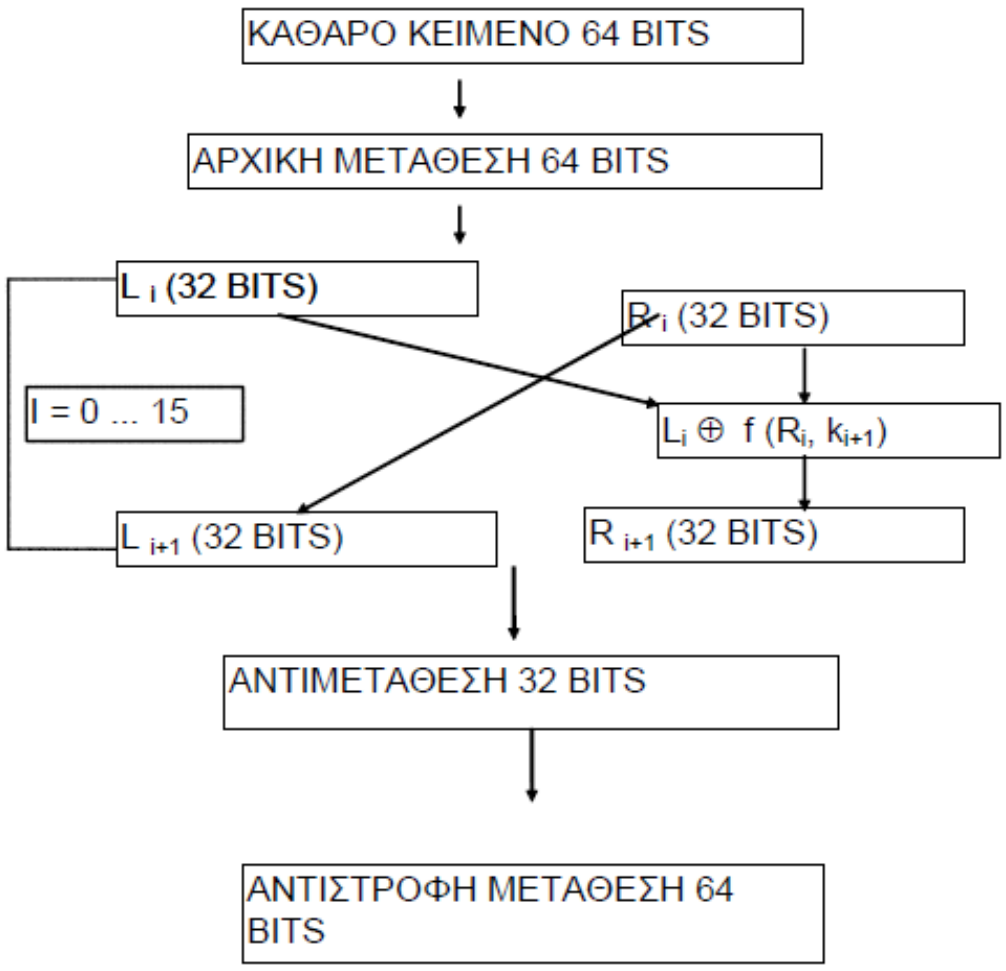
3.2 Περιγραφή του DES

Ο DES είναι ένας αλγόριθμος μπλοκ· κρυπτογραφεί τα δεδομένα σε μπλοκ των 64 bit. Κάθε μπλοκ 64 bit αρχικού κειμένου δίνει ένα μπλοκ 64 bit κρυπτογραφήματος. Ο DES είναι συμμετρικός αλγόριθμος· ο ίδιος αλγόριθμος και το ίδιο κλειδί χρησιμοποιούνται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση.

Το κλειδί έχει μήκος 56 bit. Στην πραγματικότητα είναι 64 bit, αλλά κάθε όγδοο bit χρησιμοποιείται για έλεγχο ισοτιμίας (parity check) και αγνοείται. Το bit ισοτιμίας είναι το χαμηλής τάξης bit κάθε byte.

Στη βάση του ο DES εφαρμόζει έναν συνδυασμό των δύο βασικότερων τεχνικών στην κρυπτογραφία, την σύγχυση και την διάχυση (confusion και diffusion). Τη σύγχυση την πετυχαίνει με αντικατάσταση και τη διάχυση με μετάθεση (substitution και permutation). Και οι δύο τεχνικές εφαρμόζονται στο κείμενο, με τρόπο εξαρτώμενο από το κλειδί. Αυτό είναι γνωστό σαν **γύρος (round)**. Ο DES αποτελείται από 16 γύρους (Εικόνα 17.4).

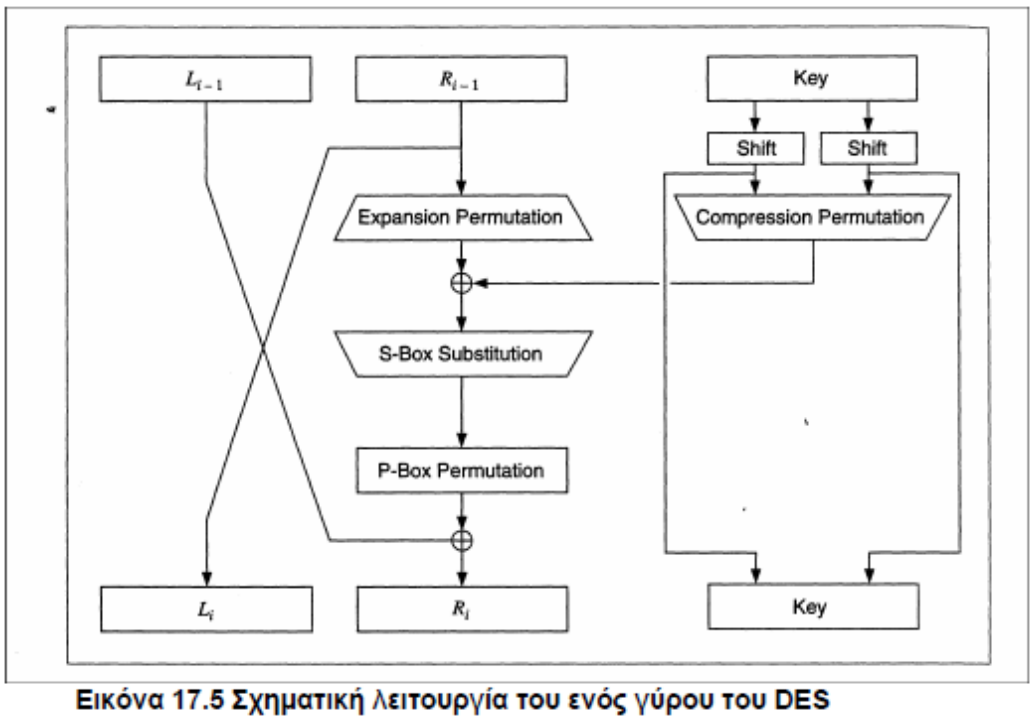
Ο αλγόριθμος χρησιμοποιεί βασικές αριθμητικές και λογικές πράξεις.



Εικόνα 17.4 Σχηματική λειτουργία του DES

3.2.1 Περίγραμμα του αλγορίθμου

Ο DES εφαρμόζεται σε μπλοκ 64 bit αρχικού κειμένου. Μετά από μια αρχική μετάθεση, το μπλοκ διαιρείται στο αριστερό μισό και στο δεξιό μισό, καθένα μήκους 32 bit. Έπειτα ακολουθούν 16 όμοιοι γύροι, που εφαρμόζουν την λεγόμενη Συνάρτηση f. Σ' αυτήν τα δεδομένα συνδυάζονται με το κλειδί. Μετά τον 16ο γύρο τα δύο μισά ενώνονται και μια τελική μετάθεση (η ανάστροφη της αρχικής) τελειώνει τον αλγόριθμο.



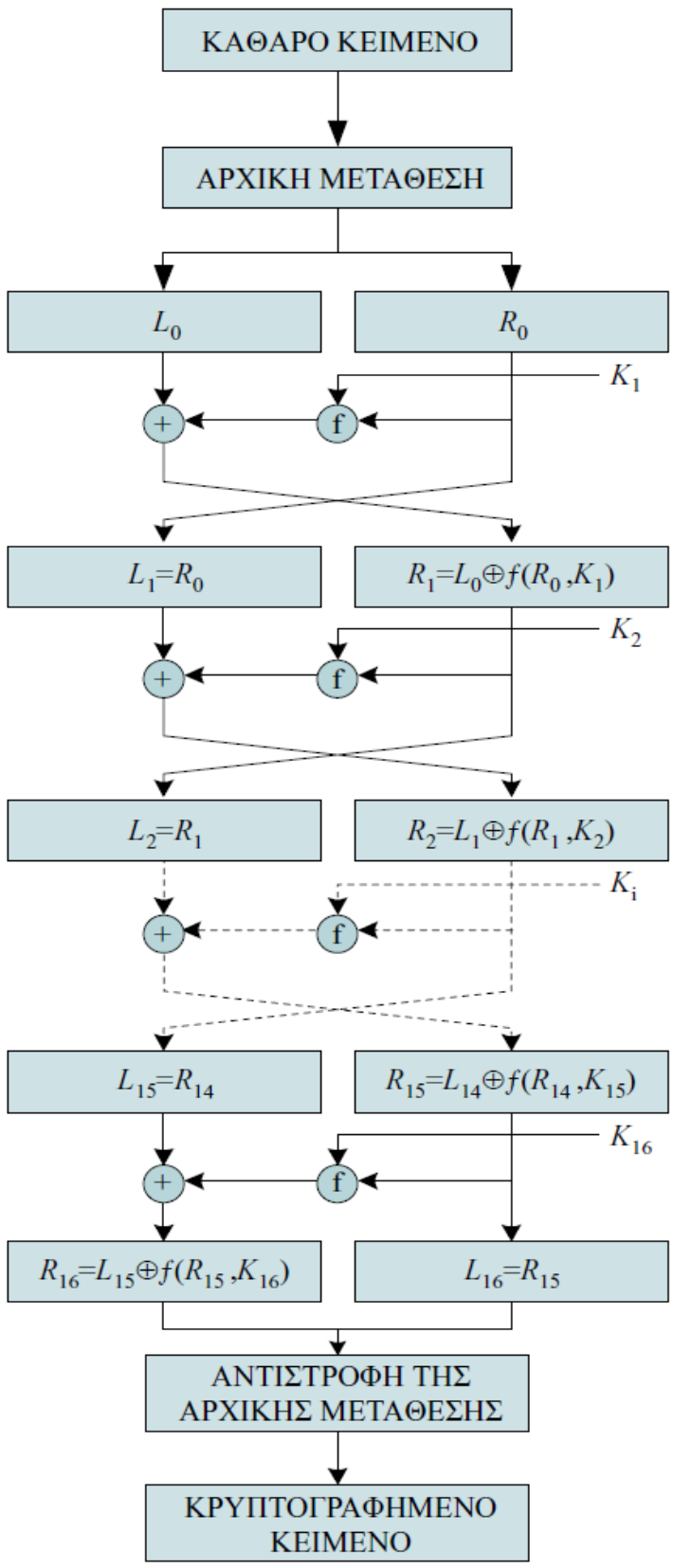
Εικόνα 17.5 Σχηματική λειτουργία του ενός γύρου του DES

Σε κάθε γύρο (Εικόνα 17.5) τα bit του κλειδιού κυλίονται κυκλικά προς τα αριστερά, και έπειτα επιλέγονται 48 bit από τα 56 αρχικά bit του κλειδιού. Το δεξί μισό των δεδομένων επεκτείνεται σε 48 bits μέσω μιας **μετάθεσης διαστολής** (expansion permutation), συνδυάζονται με τα 48 bit ενός κυλισμένου και μετατεθειμένου κλειδιού με τη χρήση ενός XOR, περνούν μέσα από 8 **κουτιά αντικατάστασης** (S-boxes) παράγοντας 32 νέα bit, και τέλος μετατίθενται ξανά. Αυτές οι τέσσερις λειτουργίες αποτελούν την Συνάρτηση *f*. Η έξοδος της Συνάρτησης *f* συνδυάζεται με το αριστερό μισό των δεδομένων με τη χρήση XOR. Το αποτέλεσμα αυτής της πράξης γίνεται το νέο δεξί μισό· το παλιό δεξί μισό γίνεται το νέο αριστερό μισό. Οι πράξεις αυτές επαναλαμβάνονται 16 φορές, αποτελώντας τους 16 γύρους του DES.

Αν L_i και R_i είναι το αριστερό και δεξί μισό του γύρου *i*, K_i είναι το 48-bit κλειδί του γύρου *i*, και *f* είναι η συνάρτηση που περιγράψαμε πιο πάνω, τότε ο κάθε γύρος συμβολίζεται ως εξής:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$



Σχήμα 4.1

Γενικό διάγραμμα του αλγόριθμου DES

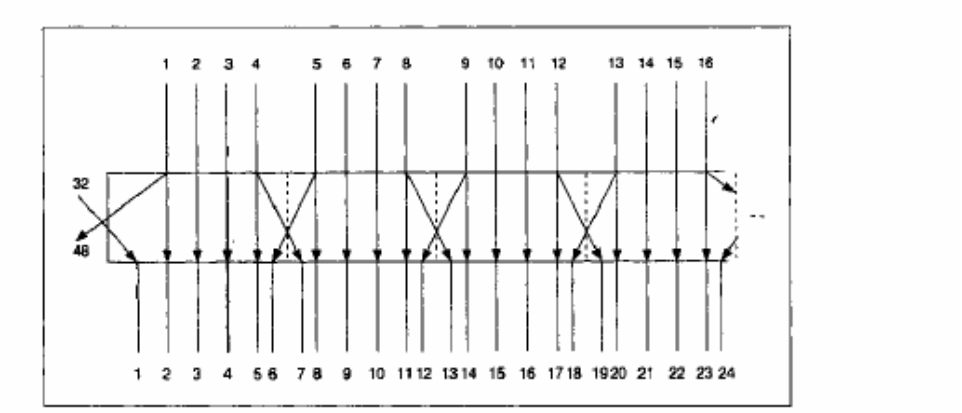
3.2.2 Η αρχική μετάθεση

Η αρχική μετάθεση λαμβάνει χώρα πριν τον πρώτο γύρο. Μεταθέτει το αρχικό μπλοκ 64 bit όπως περιγράφεται στον πίνακα 17.4. Ο πίνακας αυτός, όπως και όλοι οι πίνακες του κεφαλαίου, θα πρέπει να διαβαστεί απ' τα αριστερά προς τα δεξιά, από πάνω προς τα κάτω. Για παράδειγμα, η αρχική μετάθεση μετακινεί το 58^{o} bit του αρχικού κειμένου στη θέση 1, το 50^{o} στη θέση 2, το 42^{o} στη θέση 3 κοκ.

Η αρχική μετάθεση και η αντίστοιχη τελική μετάθεση δεν προσθέτουν στην ασφάλεια του DES. Απ' όσο μπορεί να ξέρει κανείς, ο κύριος σκοπός τους είναι να καταστήσουν ευκολότερη την τροφοδότηση ενός DES chip με καθαρό κείμενο και με κρυπτογράφημα. Επειδή η μετάθεση αυτή κάνει πιο δύσκολη την εφαρμογή σε software, χωρίς να προσθέτει σε ασφάλεια, πολλοί κατασκευαστές λογισμικού την παραλείπουν. Ο νέος αλγόριθμος, αν και δεν είναι λιγότερο ασφαλής από τον DES, δεν θα πρέπει να ονομάζεται DES.

Πίνακας 17.4

Αρχική μετάθεση															
50,	42,	34,	26,	18,	10,	2,	60,	52,	44,	36,	28,	20,	12,	4,	58,
62,	54,	46,	38,	30,	22,	14,	6,	64,	56,	48,	40,	32,	24,	16,	8,
57,	49,	41,	33,	25,	17,	9,	1,	59,	51,	43,	35,	27,	19,	11,	3,
61,	53,	45,	37,	29,	21,	13,	5,	63,	55,	47,	39,	31,	23,	15,	7



Εικόνα 17.6 Μετάθεση διαστολής

Πίνακας 17.5
Μετάθεση κλειδιού

57,	49,	41,	33,	25,	17,	9,	1,	58,	50,	42,	34,	26,	18,
10,	2,	59,	51,	43,	35,	27,	19,	11,	3,	60,	52,	44,	36,
63,	55,	47,	39,	31,	23,	15,	7,	62,	54,	46,	38,	30,	22,
14,	6,	61,	53,	45,	37,	29,	21,	13,	5,	28,	20,	12,	4

Πίνακας 17.6
Πλήθος bit του κλειδιού που κυλίονται ανά γύρο

Γύρος	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Πλήθος	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Πίνακας 17.7
Μετάθεση συμπίεσης

14,	17,	11,	24,	1,	5,	3,	28,	15,	6,	21,	10,
23,	19,	12,	4,	26,	8,	16,	7,	27,	20,	13,	2,
41,	52,	31,	37,	47,	55,	30,	40,	51,	45,	33,	48,
44,	49,	39,	56,	34,	53,	46,	42,	50,	36,	29,	32

Αυτό ονομάζεται φαινόμενο **χιονοστιβάδας (avalanche effect)**. Ο DES σχεδιάστηκε έτσι ώστε να φτάνει γρήγορα στην κατάσταση όπου το κάθε bit του κρυπτογραφήματος να εξαρτάται από κάθε bit του αρχικού κειμένου και από κάθε bit του κλειδιού. Το Εικόνα 17.6 δείχνει την διαδικασία της μετάθεσης διαστολής. Μερικές φορές καλείται και κουτί διαστολής (E-box). Για κάθε μπλοκ 4 bit, το πρώτο και τέταρτο bit αντιπροσωπεύουν το καθένα από δύο bit του μπλοκ εξόδου, ενώ το δεύτερο και τρίτο bit αντιπροσωπεύουν το καθένα από ένα bit του μπλοκ

εξόδου. Ο πίνακας 17.8 δείχνει ποιες θέσεις εξόδου αντιστοιχούν σε ποιες θέσεις εισόδου. Για παράδειγμα η θέση 3 του μπλοκ εισόδου μεταφέρεται στην θέση 4 του μπλοκ εξόδου και η θέση 21 μεταφέρεται στις θέσεις 30 και 32.

Αν και το μπλοκ εξόδου είναι μεγαλύτερο από το μπλοκ εισόδου, κάθε μπλοκ εισόδου παράγει ένα ιδιαίτερο μπλοκ εξόδου.

3.2.3 Τα κουτιά αντικατάστασης (S-boxes)

Αφού το συμπιεσμένο κλειδί γίνει XOR με το διασταλμένο μπλοκ, το 48-μπιτο αποτέλεσμα περνάει από μια διαδικασία αντικατάστασης. Οι αντικαταστάσεις υλοποιούνται από οκτώ κουτιά αντικατάστασης (substitution boxes ή αλλιώς S-boxes). Κάθε κουτί αντικατάστασης έχει είσοδο των 6 bit και έξοδο των 4 bit. (Η συνολική μνήμη που απαιτείται για τα οκτώ κουτιά είναι 256 bytes.) Τα 48 bit που προέρχονται από το XOR διαιρούνται σε οκτώ κομμάτια των 6 bit. Κάθε κουτί αντικατάστασης επεξεργάζεται ένα μοναδικό κομμάτι: το πρώτο κουτί επεξεργάζεται το πρώτο κομμάτι, το δεύτερο κουτί το δεύτερο κομμάτι κοκ. Αυτό φαίνεται στο Εικόνα 17.7.

Κάθε κουτί αντικατάστασης είναι ένας πίνακας με 4 γραμμές και 16 στήλες. Κάθε στοιχείο του πίνακα είναι ένας 4-μπιτος αριθμός. Τα 6 bit εισόδου καθορίζουν τον αριθμό της γραμμής και της στήλης που βρίσκεται ο αριθμός που θα αποτελέσει την τιμή εξόδου.

Πίνακας 17.8
Μετάθεση διαστολής

32,	1,	2,	3,	4,	5,	4,	5,	6,	7,	8,	9,
8,	9,	10,	11,	12,	13,	12,	13,	14,	15,	16,	17,
16,	17,	18,	19,	20,	21,	20,	21,	22,	23,	24,	25,
24,	25,	26,	27,	28,	29,	28,	29,	30,	31,	32,	1

Ο τρόπος που υπολογίζεται ο αριθμός της στήλης και της γραμμής είναι ο εξής:

Ονομάζουμε τα 6 bit εισόδου ως b_1, b_2, b_3, b_4, b_5 και b_6. Τα bit b_1 και b_6 συνδυάζονται για να σχηματίσουν έναν αριθμό 2 bit, από το 0 ως το 3, που αντιστοιχεί στον αριθμό της γραμμής. Τα bit από το b_2 ως το b_5 συνδυάζονται για να σχηματίσουν έναν αριθμό 4 bit, από 0 ως 15, που αντιστοιχεί στον αριθμό της στήλης.

Για παράδειγμα, υποθέτουμε ότι τα 6 bit εισόδου στο έκτο κουτί αντικατάστασης (δηλαδή τα bit 31 ως 36 της συνάρτησης XOR) έχουν την τιμή 110011. Το πρώτο και το τελευταίο συνδυάζονται δίνοντας τον αριθμό $11_2 = 3_{10}$, δηλαδή η γραμμή του αριθμού εξόδου είναι η 3. Τα τέσσερα μεσαία bit συνδυάζονται δίνοντας τον αριθμό $1001_2 = 9_{10}$, δηλαδή ο αριθμός εξόδου βρίσκεται στην στήλη 9. Η τιμή στη θέση (3,9) του έκτου κουτιού αντικατάστασης είναι $14_{10} = 1110_2$. Η τιμή 110011, λοιπόν, αντικαθίσταται από την τιμή 1110 (στο έκτο S-box).

Η λειτουργία των κουτιών αντικατάστασης αποτελεί το κεντρικό κομμάτι του DES. Οι άλλες διαδικασίες είναι γραμμικές και αναλύονται εύκολα. Τα S-boxes είναι μη γραμμικά και είναι αυτά που, περισσότερο απ' οτιδήποτε άλλο, δίνουν στον DES την ασφάλειά του.

Το αποτέλεσμα αυτής της φάσης είναι οκτώ μπλοκ των 4 bit, που ενώνονται σε ένα μπλοκ των 32 bit.

S-box 1:

14,	4,	13,	1,	2,	15,	11,	8,	3,	10,	6,	12,	5,	9,	0,	7,
0,	15,	7,	4,	14,	2,	13,	1,	10,	6,	12,	11,	9,	5,	3,	8,
4,	1,	14,	8,	13,	6,	2,	11,	15,	12,	9,	7,	3,	10,	5,	0,
15,	12,	8,	2,	4,	9,	1,	7,	5,	11,	3,	14,	10,	0,	6,	13,

S-box 2:

15,	1,	8,	14,	6,	11,	3,	4,	9,	7,	2,	13,	12,	0,	5,	10,
3,	13,	4,	7,	15,	2,	8,	14,	12,	0,	1,	10,	6,	9,	11,	5,
0,	14,	7,	11,	10,	4,	13,	1,	5,	8,	12,	6,	9,	3,	2,	15,
13,	8,	10,	1,	3,	15,	4,	2,	11,	6,	7,	12,	0,	5,	14,	9,

S-box 3:

10,	0,	9,	14,	6,	3,	15,	5,	1,	13,	12,	7,	11,	4,	2,	8,
13,	7,	0,	9,	3,	4,	6,	10,	2,	8,	5,	14,	12,	11,	15,	1,
13,	6,	4,	9,	8,	15,	3,	0,	11,	1,	2,	12,	5,	10,	14,	7,
1,	10,	13,	0,	6,	9,	8,	7,	4,	15,	14,	3,	11,	5,	2,	12,

S-box 4:

7,	13,	14,	3,	0,	6,	9,	10,	1,	2,	8,	5,	11,	12,	4,	15,
13,	8,	11,	5,	6,	15,	0,	3,	4,	7,	2,	12,	1,	10,	14,	9,
10,	6,	9,	0,	12,	11,	7,	13,	15,	1,	3,	14,	5,	2,	8,	4,
3,	15,	0,	6,	10,	1,	13,	8,	9,	4,	5,	11,	12,	7,	2,	14,

S-box 5:

2,	12,	4,	1,	7,	10,	11,	6,	8,	5,	3,	15,	13,	0,	14,	9,
14,	11,	2,	12,	4,	7,	13,	1,	5,	0,	15,	10,	3,	9,	8,	6,
4,	2,	1,	11,	10,	13,	7,	8,	15,	9,	12,	5,	6,	3,	0,	14,
11,	8,	12,	7,	1,	14,	2,	13,	6,	15,	0,	9,	10,	4,	5,	3,

S-box 6:

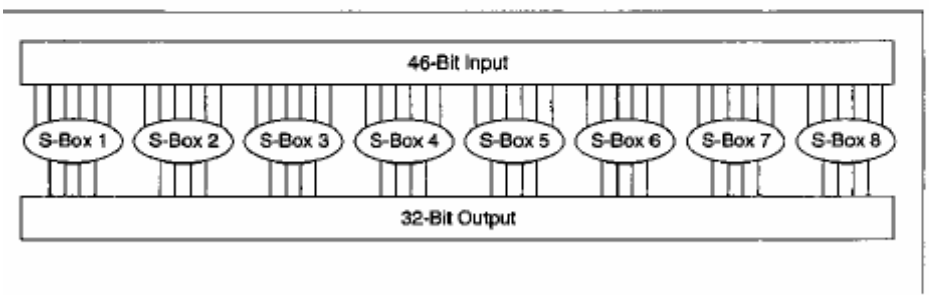
12,	1,	10,	15,	9,	2,	6,	8,	0,	13,	3,	4,	14,	7,	5,	11,
10,	15,	4,	2,	7,	12,	9,	5,	6,	1,	13,	14,	0,	11,	3,	8,
9,	14,	15,	5,	2,	8,	12,	3,	7,	0,	4,	10,	1,	13,	11,	6,
4,	3,	2,	12,	9,	5,	15,	10,	11,	14,	1,	7,	6,	0,	8,	13,

S-box 7:

4,	11,	2,	14,	15,	0,	8,	13,	3,	12,	9,	7,	5,	10,	6,	1,
13,	0,	11,	7,	4,	9,	1,	10,	14,	3,	5,	12,	2,	15,	8,	6,
1,	4,	11,	13,	12,	3,	7,	14,	10,	15,	6,	8,	0,	5,	9,	2,
6,	11,	13,	8,	1,	4,	10,	7,	9,	5,	0,	15,	14,	2,	3,	12,

S-box 8:

13,	2,	8,	4,	6,	15,	11,	1,	10,	9,	3,	14,	5,	0,	12,	7,
1,	15,	13,	8,	10,	3,	7,	4,	12,	5,	6,	11,	0,	14,	9,	2,
7,	11,	4,	1,	9,	12,	14,	2,	0,	6,	10,	13,	15,	3,	5,	8,
2,	1,	14,	7,	4,	10,	8,	13,	15,	12,	9,	0,	3,	5,	6,	11



Εικόνα 17.7 S-Boxes και η λειτουργία τους

3.2.4 Το κουτί μετάθεσης (P-box)

Η έξοδος των 32 bit από τα S-boxes μετατίθεται σύμφωνα με ένα **κουτί μετάθεσης** (permutation box ή P-box). Κατά την μετάθεση αυτή αντιστοιχίζεται κάθε bit εισόδου σε μια θέση εξόδου. Κανένα bit δεν χρησιμοποιείται δύο φορές και κανένα δεν παραλείπεται. Ο πίνακας 17.9 δείχνει την θέση που παίρνει στην έξοδο το κάθε bit εισόδου. Για παράδειγμα, το bit 21 πηγαίνει στη θέση 4 και το bit 4 στη θέση 31.

Στο τέλος η έξοδος του P-box γίνεται XOR με το αριστερό μισό του αρχικού 64-μπιτου μπλοκ. Το δεξί και αριστερό μισό αντιμετατίθενται και αρχίζει καινούργιος γύρος.

3.2.5 Η τελική μετάθεση

Η τελική μετάθεση είναι το ανάστροφο της αρχικής και περιγράφεται στον πίνακα 17.10. Αξίζει να σημειώσουμε ότι το δεξί και αριστερό μισό που παράγονται από τον $16^{ο}$ γύρο, δεν αντιμετατίθενται πριν υποστούν την τελική μετάθεση. Αυτό συμβαίνει για να είναι η διαδικασία αντιστρέψιμη και να χρησιμοποιείται ο ίδιος αλγόριθμος για κρυπτογράφηση και αποκρυπτογράφηση.

3.3 Αποκρυπτογράφηση του DES

Όλες οι πράξεις και διαδικασίες που εκτελεί ο DES έχουν προσεχτικά επιλεχτεί ώστε να είναι αναστρέψιμες. Μπορεί, λοιπόν, να χρησιμοποιηθεί η ίδια συνάρτηση για κρυπτογράφηση και αποκρυπτογράφηση. Η μόνη διαφορά είναι ότι τα κλειδιά πρέπει να χρησιμοποιηθούν με αντίθετη σειρά. Δηλαδή αν τα υπο-κλειδιά κρυπτογράφησης για κάθε γύρο ήταν τα K_1, K_2, K_3, ..., K_{16}, τότε τα υπο-κλειδιά αποκρυπτογράφησης είναι τα K_{16}, K_{15}, K_{14}, ..., K_1. Ο αλγόριθμος που δημιουργεί τα υπο-κλειδιά είναι επίσης κυκλικός. Η κύλιση του κλειδιού είναι προς τα δεξιά και ο αριθμός των θέσεων κύλισης είναι 0, 1, 2, 2, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 2, 1.

Πίνακας 17.9
Μετάθεση του P-box

16,	7,	20,	21,	29,	12,	28,	17,	1,	15,	23,	26,	5,	18,	31,	10,
2,	8,	24,	14,	32,	27,	3,	9,	19,	13,	30,	6,	22,	11,	4,	25

Πίνακας 17.10
Τελική μετάθεση

40,	8,	48,	16,	56,	24,	64,	32,	39,	7,	47,	15,	55,	23,	63,	31,
38,	6,	46,	14,	54,	22,	62,	30,	37,	5,	45,	13,	53,	21,	61,	29,
36,	4,	44,	12,	52,	20,	60,	28,	35,	3,	43,	11,	51,	19,	59,	27,
34,	2,	42,	10,	50,	18,	58,	26,	33,	1,	41,	9,	49,	17,	57,	25

3.4 Τρόποι λειτουργίας του DES (modes)

Ο **τρόπος λειτουργίας** (mode) ενός αλγορίθμου καθορίζει πώς τα μπλοκ του αρχικού κειμένου κρυπτογραφούνται σε μπλοκ κρυπτογραφήματος, και αντίστροφα.Ένας κρυπτογραφικός τρόπος λειτουργίας συνήθως συνδυάζει τον βασικό αλγόριθμο, κάποια μορφή ανακύκλωσης (feedback) και μερικές απλές λειτουργίες. Οι λειτουργίες είναι απλές, γιατί δεν έχουν στόχο την ενίσχυση της ασφάλειας. Ακόμη πιο σημαντικό είναι ο τρόπος λειτουργίας να μην αναιρεί την ασφάλεια που προσφέρει ο αλγόριθμος.

Υπάρχουν και άλλα που πρέπει να ληφθούν υπ' όψιν κατά τον σχεδιασμό ενός τρόπου λειτουργίας: θα πρέπει να αποκρύπτονται τυχόν αναγνωρίσιμα χαρακτηριστικά του κειμένου, θα πρέπει να καθίστανται τυχαία τα δεδομένα εισόδου του αλγορίθμου, θα πρέπει να καθίσταται δύσκολη η μεταβολή του αρχικού κειμένου με εισαγωγή λαθών στο κρυπτογράφημα, και θα πρέπει να καθίσταται δυνατή η κρυπτογράφηση περισσότερων του ενός μηνυμάτων με το ίδιο κλειδί.

Η αποδοτικότητα είναι ένα ακόμα μέλημα. Ο τρόπος λειτουργίας δεν θα πρέπει να μειώνει σημαντικά την απόδοση του αλγορίθμου. Σε μερικές περιπτώσεις είναι σημαντικό το κρυπτογράφημα να έχει ίδιο μέγεθος με το αρχικό κείμενο.

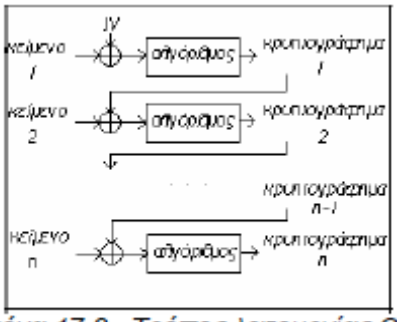
Ένα τρίτο μέλημα είναι η ανοχή σε λάθη. Σε μερικές εφαρμογές είναι σημαντικό να μπορεί η διαδικασία αποκρυπτογράφησης να αντιμετωπίζει τυχόν λάθη στα bit του κρυπτογραφήματος (ciphertext stream), που

μπορεί να περιλαμβάνουν bit με αλλαγμένη τιμή, bit που έχουν προστεθεί ή bit που έχουν χαθεί.

Οι τρόποι λειτουργίας του DES (οι τρόποι αυτοί δεν σχετίζονται μόνο με τον DES, αλλά έχουν εφαρμογή και σε άλλους αλγόριθμους) είναι:

• **ECB** (electronic code book). Είναι η πιο απλή μορφή λειτουργίας, κατά την οποία κάθε μπλοκ κειμένου κρυπτογραφείται δίνοντας ένα μπλοκ κρυπτογραφήματος. Ο τρόπος αυτός έχει το μειονέκτημα ότι ένα κείμενο δίνει πάντα το ίδιο κρυπτογράφημα, αν χρησιμοποιηθεί το ίδιο κλειδί. Αυτό μπορεί να το εκμεταλλευτεί ο αναλυτής.

• **CBC** (cipher block chaining). Ο τρόπος αυτός αντιμετωπίζει την αδυναμία του ECB. Κάθε μπλοκ του αρχικού κειμένου συνδυάζεται με το προηγούμενο μπλοκ κρυπτογραφήματος, με χρήση του XOR. Το αποτέλεσμα του XOR κρυπτογραφείται και μας δίνει το επόμενο κρυπτογράφημα. Αυτό φαίνεται στο Εικόνα 17.8. Επειδή δεν υπάρχει προηγούμενο κρυπτογράφημα για να συνδυαστεί με το πρώτο μπλοκ κειμένου, χρησιμοποιείται μια σταθερά αρχικοποίησης (initialisation vector [IV]) για το πρώτο μπλοκ. Το IV είναι συνήθως τυχαία δεδομένα. Ο αλγόριθμος αποκρυπτογράφησης πρέπει να χρησιμοποιήσει το ίδιο IV. Η αποκρυπτογράφηση είναι το ανάστροφο της κρυπτογράφησης. Από τον τρόπο που χρησιμοποιείται, βλέπουμε ότι το IV είναι ένα είδος κλειδιού. Ο παραλήπτης πρέπει να λάβει και το IV, μαζί με το κρυπτογράφημα, για να μπορέσει να το αποκρυπτογραφήσει.



Εικόνα 17.8 Τρόπος λειτουργίας CBC

- **CFB** (cipher feedback). Ο τρόπος αυτός λειτουργίας επιτρέπει σε έναν αλγόριθμο μπλοκ να λειτουργήσει σαν αλγόριθμος συρμού. Χρησιμοποιεί και αυτός σταθερά αρχικοποίησης (IV), όπως και ο CBC, αλλά η διαδικασία του είναι πιο περίπλοκη. Το βασικό είναι ότι ένας αλγόριθμος μπλοκ σε CFB λειτουργία μπορεί να κρυπτογραφήσει κομμάτια δεδομένων που είναι μικρότερα από το μέγεθος του μπλοκ. Για την ακρίβεια, ο CFB μπορεί να χρησιμοποιηθεί για κρυπτογράφηση οποιουδήποτε μεγέθους δεδομένων, από ένα bit ως και το μέγεθος του μπλοκ. Συνήθως χρησιμοποιείται για να κρυπτογραφήσει ή αποκρυπτογραφήσει ένα byte, οπότε καλείται CFB8.

  Ένα byte καθαρού κειμένου, *P*, μετατρέπεται σε byte κρυπτογραφήματος, *C*, με την παρακάτω διαδικασία:

  1. Κρυπτογραφείται, με τη χρήση του αλγορίθμου μπλοκ, ένα buffer (κομμάτι δεδομένων) ίσο με το μέγεθος του μπλοκ που υποστηρίζει ο αλγόριθμος. Το buffer αρχικά περιέχει το IV.
  2. Ο επιθυμητός αριθμός των αριστερότερων bit του κρυπτογραφημένου buffer γίνονται XOR με το καθαρό κείμενο. Το αποτέλεσμα είναι το κρυπτογράφημα. Το υπόλοιπο του κρυπτογραφημένου buffer αγνοείται. Στο CFB8, το αριστερότερο byte του κρυπτογραφημένου buffer γίνεται XOR με το byte καθαρού κειμένου, δίνοντας ένα byte κρυπτογραφήματος.
  3. Το αρχικό buffer κυλίεται δεξιά κατά τον επιθυμητό αριθμό bit. Στο CFB8, το buffer μετακινείται κατά ένα byte. Το κρυπτογράφημα χρησιμοποιείται για να γεμίσει τον άδειο χώρο στην δεξιά μεριά του buffer. Καθώς η

διαδικασία αυτή συνεχίζεται, το buffer θα γεμίσει τελικά με κρυπτογράφημα.

Η αποκρυπτογράφηση ακολουθεί την ίδια διαδικασία, εκτός από το βήμα 2.

1. Το buffer κρυπτογραφείται χρησιμοποιώντας τον αλγόριθμο μπλοκ. Αν και *αποκρυπτογραφούμε* ένα byte κρυπτογραφήματος, παρόλα αυτά χρησιμοποιούμε τον αλγόριθμο για να *κρυπτογραφήσουμε* το buffer.
2. Τα αριστερότερα bit του buffer γίνονται XOR με το κρυπτογράφημα, δίνοντας το αρχικό κείμενο. Ξανά, το υπόλοιπο του buffer αγνοείται.
3. Το αρχικό buffer κυλίεται αριστερά και γεμίζει με κρυπτογράφημα. Το buffer θα χρησιμοποιηθεί ξανά στην επόμενη αποκρυπτογράφηση.

Η λειτουργία CFB δεν είναι ιδιαίτερα αποδοτική. Κάθε φορά που ένα κομμάτι κειμένου κρυπτογραφείται, κρυπτογραφείται ένα ολόκληρο μπλοκ από τον αλγόριθμο. Το ίδιο συμβαίνει και κατά την αποκρυπτογράφηση. Για έναν αλγόριθμο 64 bit το CFB θα είναι οκτώ φορές πιο αργό από το ECB ή το CBC. Το CFB μπορεί να χρησιμοποιηθεί από οποιονδήποτε αλγόριθμο μπλοκ, αλλά και από ασύμμετρους αλγόριθμους, οι οποίοι όμως σ' αυτήν την περίπτωση συμπεριφέρονται σαν συμμετρικοί (πρέπει να χρησιμοποιείται το ίδιο κλειδί τόσο κατά την κρυπτογράφηση όσο και κατά την αποκρυπτογράφηση).

- **OFB** (output feedback). Δουλεύει ακριβώς όπως το CFB, μόνο που στο βήμα 2 το κύλισμα δεν είναι απλό, αλλά κυκλικό. Θεωρητικά μπορεί να χρησιμοποιηθεί για κάθε μέγεθος bit, μικρότερο ή ίσο με το μέγεθος του μπλοκ του αλγορίθμου. Αλλά το OFB παρουσιάζει αδυναμίες όταν το

μέγεθος των bit είναι μικρότερο από το μέγεθος του μπλοκ του κώδικα. Καλό είναι να χρησιμοποιούμε το OFB μόνο με μέγεθος bit ίσο με το μπλοκ.

Υπάρχουν και άλλοι τρόποι λειτουργίας, όπως ο PCBC.
Το FIPS PUB 81 καθορίζει τέσσερις τρόπους λειτουργίας για τον DES: ECB, CBC, OFB.

3.5 Ασφάλεια του DES

3.5.1. Αδύναμα κλειδιά

Εξαιτίας του τρόπου που το αρχικό κλειδί τροποποιείται για να πάρουμε ένα υπο-κλειδί σε κάθε γύρο, υπάρχουν ορισμένα **αδύναμα κλειδιά** (weak keys). Έχουμε πει ότι το αρχικό κλειδί χωρίζεται σε δύο μισά, και κάθε μισό κυλίεται κυκλικά ανεξάρτητα από το άλλο. Αν όλα τα bit σε κάθε μισό είναι είτε 0 είτε 1, τότε για κάθε γύρο του αλγορίθμου χρησιμοποιείται το ίδιο κλειδί. Αυτό μπορεί να συμβεί και αν το ένα μισό είναι μόνο 1 και το άλλο μόνο 0.

Επιπλέον, μερικά ζευγάρια κλειδιών κρυπτογραφούν ένα κείμενο δίνοντας το ίδιο κρυπτογράφημα. Με άλλα λόγια, το ένα κλειδί του ζευγαριού μπορεί να αποκρυπτογραφήσει μηνύματα, που κρυπτογραφήθηκαν με το άλλο κλειδί. Αυτό οφείλεται στον τρόπο με τον οποίο δημιουργούνται στον DES τα υπο-κλειδιά. Τα συγκεκριμένα κλειδιά, αντί να δώσουν 16 διαφορετικά υπο-κλειδιά, δίνουν μόνο δύο. Καθένα από τα δύο αυτά υπο-κλειδιά χρησιμοποιείται οκτώ φορές στον αλγόριθμο. Αυτά τα κλειδιά ονομάζονται **ημι-αδύναμα** (semi-weak).

Μερικά κλειδιά δίνουν μόνο τέσσερα υπο-κλειδιά, που καθένα χρησιμοποιείται τέσσερις φορές στον αλγόριθμο. Τα κλειδιά αυτά ονομάζονται **πιθανά αδύναμα** κλειδιά (possibly weak keys). Είναι σημαντικό εδώ να πούμε, ότι οι παραπάνω περιπτώσεις αδύναμων κλειδιών δίνουν ένα σύνολο 64 κλειδιών, μέγεθος απειροελάχιστο μπροστά στα 72.057.594.037.927.936 δυνατά κλειδιά. Αν διαλέξουμε τυχαία ένα κλειδί, η πιθανότητα να είναι αδύναμο είναι ασήμαντη.

3.5.2 Συμπληρωματικά κλειδιά

Έχουμε ένα κλειδί και παίρνουμε το συμπληρωματικό του με βάση τα bit (αντικαταστήσουμε όλα τα 0 με 1 και όλα τα 1 με 0). Αν κρυπτογραφήσουμε ένα κείμενο με το κλειδί, τότε κρυπτογραφώντας το

συμπληρωματικό του κειμένου με το συμπληρωματικό κλειδί, μας δίνει το συμπληρωματικό κρυπτογράφημα.

Έχουμε, δηλαδή, την παρακάτω σχέση (το x' είναι το συμπληρωματικό του x):

$E_K(P) = C$

$E_{K'}(P') = C'$

Αυτή η **συμπληρωματική ιδιότητα** (complementation property) είναι απόρροια του ότι τα υπο-κλειδιά γίνονται XOR με το δεξί μισό μετά την μετάθεση διαστολής, σε κάθε γύρο.

Αυτό σημαίνει ότι μια επίθεση επιλεγμένου κειμένου στον DES χρειάζεται να δοκιμάσει μόνο τα μισά κλειδιά: 2^{55} αντί για 2^{56}. Ο Eli Biham και ο Adi Shamir έδειξαν ότι υπάρχει μια επίθεση γνωστού κειμένου με την ίδια πολυπλοκότητα (2^{55}), που χρειάζεται τουλάχιστον 2^{33} γνωστά κείμενα.

Είναι σχετικό το κατά πόσο μπορεί αυτό να θεωρηθεί αδυναμία. Τα περισσότερα μηνύματα δεν έχουν συμπληρωματικά μπλοκ κειμένου (ειδικά αν το αρχικό κείμενο είναι τυχαίο, οι πιθανότητες είναι ιδιαίτερα μικρές), και οι χρήστες μπορούν να προσέχουν να μην χρησιμοποιούν συμπληρωματικά κλειδιά.

3.5.3 Μήκος κλειδιού

Η αρχική πρόταση της IBM προς την NSA μιλούσε για κλειδί 112 bit. Όταν ο DES έγινε πρότυπο, κλειδί είχε μειωθεί στα 56 bit. Πολλοί επιχειρηματολόγησαν υπέρ ενός μεγαλύτερου κλειδιού. Τα επιχειρήματά τους επικεντρώνονται στην δυνατότητα μιας δυναμικής επίθεσης.

Το 1976 και 1977, οι Diffie και Hellman υποστήριξαν ότι ένας παράλληλος υπολογιστής, ειδικά κατασκευασμένος για το σπάσιμο του DES, θα μπορούσε να βρει το κλειδί σε μία μέρα, και θα κόστιζε 20 εκατομμύρια δολάρια. Το 1981, ο Diffie ανέβασε τις εκτιμήσεις του χρόνου σπασίματος σε δύο ημέρες και του κόστους σε 50 εκατομμύρια δολάρια. Οι Diffie και Hellman θεώρησαν ότι το πόσο αυτό ήταν απαγορευτικό για όλους εκτός από υπηρεσίες όπως η NSA, αλλά είπαν ότι μετά το 1990 ο DES δεν θα παρείχε καμιά ασφάλεια.

Ο Hellman κατέθεσε ακόμα ένα επιχείρημα κατά του μικρού μεγέθους κλειδιού: ήταν δυνατό να επιταχυνθεί η δυναμική επίθεση, αν

αφιερώνονταν μεγαλύτερη ποσότητα μνήμης. Κατέδειξε την δυνατότητα του υπολογισμού και αποθήκευσης 2^{56} δυνατών αποτελεσμάτων κρυπτογράφησης ενός συγκεκριμένου μπλοκ κειμένου με όλα τα δυνατά κλειδιά. Έπειτα, για να βρούμε ένα κλειδί, το μόνο που θα χρειαζόταν θα ήταν να τοποθετήσουμε (με κάποιον τρόπο) το συγκεκριμένο μπλοκ στην διαδικασία κρυπτογράφησης, να πάρουμε το κρυπτογράφημα και να κοιτάζαμε σε ποιο κλειδί αντιστοιχεί.

Απόψεις για την ύπαρξη ή όχι μιας μηχανής δυναμικής επίθεσης για τον DES, καταχωνιασμένης στα υπόγεια κάποιας μυστικής υπηρεσίας, συνέχισαν για καιρό. Εν τω μεταξύ τα DES chip ολοένα και αύξαναν την ταχύτητά τους, πλησιάζοντας τις απαιτήσεις της μηχανής των Diffie και Hellman. Το 1984 υπήρχαν chip που έκαναν 256.000 κρυπτογραφήσεις το δευτερόλεπτο. Το 1987 έφτασαν τις 512.000 κρυπτογραφήσεις το δευτερόλεπτο, και γίνονταν μελέτες για την υλοποίηση chip με τις διπλάσιες δυνατότητες. Το 1993 ο Michael Wiener σχεδίασε μια μηχανή κόστους 1 εκατομμυρίου δολαρίων, που μπορούσε να βρει ένα DES κλειδί με δυναμική επίθεση σε περίπου 3,5 ώρες.

Όμως τα σημαντικά νέα ήρθαν στις 17 Ιουλίου, 1998, όταν το Electronic Frontier Foundation (EFF) ανακοίνωσε την κατασκευή ενός μηχανήματος δυναμικής επίθεσης για τον DES. Το μηχάνημα κοστίζει 220.000 δολάρια και μπορεί να σπάσει τον αλγόριθμο σε, περίπου, 4,5 μέρες .

Το σημαντικό δεν είναι ότι ο DES είναι μη ασφαλής, ούτε ότι μια τέτοια μηχανή μπορεί να κατασκευαστεί, ούτε ότι το κλειδί είναι πολύ μικρό. Όπως είδαμε και παραπάνω, όλα αυτά είχαν επισημανθεί από καιρό.

Το σημαντικό είναι ότι η αμερικάνικη κυβέρνηση αρνιόταν κατηγορηματικά την δυνατότητα κατασκευής μιας τέτοιας μηχανής. Μόλις στις 8 Ιουλίου, 1998, ο Robert Litt, βασικός βοηθός Γενικού Εισαγγελέα στο Υπουργείο Δικαιοσύνης, αρνήθηκε ότι το FBI μπορούσε να σπάσει τον DES.

Το γεγονός ότι η αμερικάνικη κυβέρνηση μπορούσε να σπάσει τον DES δηλώνεται και από το γεγονός της απλής κατασκευής της μηχανής. Η μηχανή δεν χρησιμοποιεί ούτε επαναστατικά ηλεκτρονικά κυκλώματα, ούτε μαθηματική κρυπτογραφία. Χρησιμοποιεί παλιά, γνωστά chip και καθόλου κρυπτογραφία. Το ενδιαφέρον είναι ότι η μηχανή αναβαθμίζεται εύκολα. Ξοδεύοντας άλλα 220.000 δολάρια μπορεί κανείς να αποκτήσει την διπλάσια ισχύ.

Η μηχανή αυτή έσπασε τον DES αλλά θα μπορούσε να χρησιμοποιηθεί για οποιονδήποτε άλλο αλγόριθμο, αφού η επίθεση στηρίζεται στο μήκος του κλειδιού και όχι στον σχεδιασμό του αλγορίθμου. Επιπλέον, αν χρησιμοποιηθεί πιο ακριβή τεχνολογία, όπως τα FPGA, η επίθεση μπορεί να έχει ισχύ σε ακόμη μεγαλύτερο αριθμό αλγορίθμων. Η μόνη άμυνα είναι να χρησιμοποιηθεί μεγαλύτερο κλειδί.

3.6 Διαφορική και γραμμική κρυπτανάλυση (differential and linear cryptanalysis)

3.6.1 Διαφορική κρυπτανάλυση

Το 1990 δύο Ισραηλινοί μαθηματικοί, ο Eli Biham και ο Adi Shamir, εισήγαγαν την έννοια της **διαφορικής κρυπτανάλυσης** (differential cryptanalysis). Με χρήση της μεθόδου βρήκαν μια επίθεση επιλεγμένου κειμένου κατά του DES, που ήταν πιο αποτελεσματική από μια δυναμική επίθεση.

Η διαφορική κρυπτανάλυση ψάχνει για ζευγάρια κρυπτογραφημάτων, που τα αρχικά τους κείμενα έχουν συγκεκριμένες διαφορές. Αναλύει την εξέλιξη των διαφορών αυτών, καθώς τα αρχικά κείμενα προχωρούν από γύρο σε γύρο του DES κρυπτογραφημένα με το ίδιο κλειδί.

Πιο απλά, διαλέγουμε δύο κείμενα με κάποια γνωστή διαφορά (τα κείμενα μπορούν να διαλεχτούν στην τύχη, χωρίς ο κρυπταναλυτής να γνωρίζει την τιμή τους, αρκεί να έχουν κάποια δεδομένη διαφορά). Για τον DES η ‘διαφορά’ καθορίζεται από την πράξη του XOR (σε άλλους αλγόριθμους καθορίζεται διαφορετικά).

Έπειτα, ανάλογα με τις διαφορές στα παραγόμενα κρυπτογραφήματα, αποδίδουμε διαφορετικές πιθανότητες σε διαφορετικά κλειδιά. Καθώς αναλύουμε όλο και μεγαλύτερη ποσότητα κρυπτογραφήματος, κάποιο κλειδί θα αναδειχτεί ως το πιο πιθανό. Αυτό είναι και το σωστό.

Στο Εικόνα 17.9 φαίνεται η επαναλαμβανόμενη συνάρτηση f του DES. Θεωρούμε δύο κείμενα X και X', που έχουν μια διαφορά ΔX. Τα αποτελέσματα της συνάρτησης, Y και Y', είναι γνωστά, οπότε γνωστή είναι και η διαφορά τους ΔY. Τόσο η μετάθεση διαστολής, όσο και το P-

box μας είναι γνωστά, οπότε γνωρίζουμε και τα ΔA και ΔC. Τα B και B' δεν είναι γνωστά, αλλά μας είναι γνωστό το ΔB, που είναι ίσο με το ΔA.

Αυτό συμβαίνει γιατί $\Delta A = \Delta(A \oplus K_i)$. Για ένα δεδομένο Δ$A$ δεν είναι το ίδιο πιθανές όλες οι τιμές του ΔC. Ο συνδυασμός των ΔA και ΔC υποδεικνύει κάποιες τιμές για τα bit των $A \oplus K_i$ και $A' \oplus K_i$. Από τη στιγμή που τα A και A' είναι γνωστά, μπορούμε να συλλέξουμε πληροφορίες για το K_i.

Αν μπορέσουμε να καθορίσουμε το K_{16}, τότε έχουμε 48 bit του κλειδιού (αν προσέξουμε θα δούμε ότι τα κυκλικά κυλίσματα του κλειδιού σε κάθε γύρο είναι φτιαγμένα έτσι ώστε στον 16^{o} γύρο το κλειδί να επανέρχεται στην αρχική του τιμή). Τα υπόλοιπα 8 bit, που τα αποκρύπτει η μετάθεση συμπίεσης, μπορούμε να τα βρούμε με δυναμική επίθεση.

Η καλύτερη επίθεση κατά του πλήρους DES 16 γύρων απαιτεί 2^{47} επιλεγμένα κείμενα. Η επίθεση αυτή μπορεί να μετατραπεί και σε επίθεση γνωστού κειμένου, αλλά απαιτεί 2^{55} γνωστά κείμενα και 2^{37} εφαρμογές του αλγορίθμου.

Πάντως η επίθεση είναι κατά το μεγαλύτερο μέρος θεωρητική. Οι μεγάλες απαιτήσεις σε χρόνο και δεδομένα καθιστούν την διαφορική επίθεση απρόσιτη στους περισσότερους. Για να αποκτήσει κανείς τα απαιτούμενα δεδομένα για την επίθεση θα πρέπει να κρυπτογραφεί μια ψηφιακή σύνδεση των 1,5 Mbps για τρία χρόνια.

Δεύτερον, η επίθεση είναι κατά κύριο λόγο επίθεση επιλεγμένου κειμένου. Μπορεί να μετατραπεί σε επίθεση γνωστού κειμένου, αλλά τότε γίνεται ελαφρώς πιο αργή από

την δυναμική επίθεση. Κατά γενική ομολογία, λοιπόν, ο DES, αν υλοποιηθεί σωστά, είναι ανθεκτικός στην διαφορική κρυπτανάλυση.

Πώς συμβαίνει και ο DES είναι ανθεκτικός σ' αυτό το είδος κρυπτανάλυσης; Η απάντηση είναι ότι οι κατασκευαστές του γνώριζαν την επίθεση αυτή, περίπου 15 χρόνια πριν γίνει ευρέως γνωστή.

3.6.2 Κρυπτανάλυση συσχετιζόμενων κλειδιών

Η κρυπτανάλυση **συσχετιζόμενων κλειδιών (related-key cryptanalysis)** είναι παρόμοια με την διαφορική κρυπτανάλυση, αλλά εξετάζει τη διαφορά μεταξύ κλειδιών. Η επίθεση είναι διαφορετική απ' όσες έχουμε δει ως τώρα: ο κρυπταναλυτής επιλέγει μια διαφορά ανάμεσα σε ένα ζευγάρι κλειδιών, αλλά δεν γνωρίζει τα ίδια τα κλειδιά. Δεδομένα κρυπτογραφούνται και με τα δύο κλειδιά. Στην περίπτωση γνωστού κειμένου, ο αναλυτής γνωρίζει το αρχικό κείμενο και τα κρυπτογραφήματα που προήλθαν από τα δύο κλειδιά. Στην περίπτωση επιλεγμένου κειμένου ο αναλυτής μπορεί να διαλέξει το κείμενο που κρυπτογραφείται με τα δύο κλειδιά.

Ο DES για να αποφύγει αυτήν την περίπτωση κυλίει το κλειδί όπως είχαμε δει στον πίνακα 17.6. Η επίθεση αυτή δεν είναι καθόλου πρακτική, αλλά είναι ενδιαφέρουσα για τρεις λόγους. Πρώτον, ήταν η πρώτη κρυπταναλυτική επίθεση κατά του αλγόριθμου δημιουργίας υπο-κλειδιών του DES. Δεύτερον, η επίθεση δεν επηρεάζεται από αριθμό των γύρων του αλγορίθμου• μπορεί να είναι 16 ή 1000. Και τρίτον, ο DES είναι απόλυτα ανθεκτικός σ' αυτήν την επίθεση.

3.6.3 Γραμμική κρυπτανάλυση

Η **γραμμική κρυπτανάλυση** (linear cryptanalysis) ανακαλύφθηκε από τον Mitsuru Matsui. Η επίθεση αυτή χρησιμοποιεί γραμμικές προσεγγίσεις για να περιγράψει την δράση του αλγορίθμου μπλοκ (στην περίπτωσή μας, του DES).

Αυτό σημαίνει ότι αν γίνουν XOR μεταξύ τους ορισμένα bit του αρχικού κειμένου, γίνουν XOR μεταξύ τους μερικά bit κρυπτογραφήματος, και μετά γίνουν XOR τα αποτελέσματα, θα πάρουμε ένα bit, που είναι το XOR ορισμένων από τα bit του κλειδιού. Αυτό είναι μια γραμμική προσέγγιση και ισχύει με μια πιθανότητα p. Αν το $p \neq 0,5$ τότε αυτή η απόκλιση (bias) $(0,5 - p)$ μπορεί να χρησιμοποιηθεί υπέρ του κρυπταναλυτή. Χρησιμοποιούμε κείμενα με τα αντίστοιχα κρυπτογραφήματά τους για να μαντέψουμε τα bit του κλειδιού. Όσο περισσότερα δεδομένα έχουμε, τόσο πιο αξιόπιστη είναι η εικασία. Όσο μεγαλύτερη είναι η απόκλιση, τόσο μεγαλύτερο είναι και το ποσοστό επιτυχίας με την ίδια ποσότητα δεδομένων.

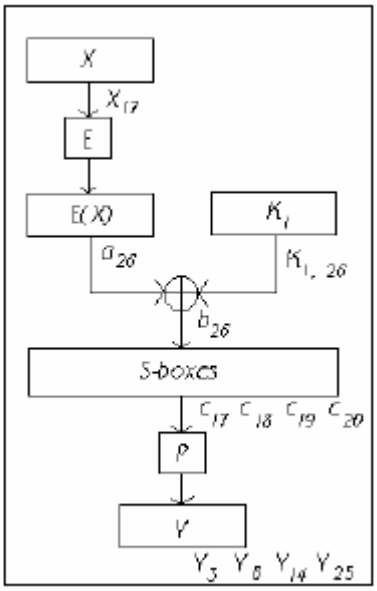
Για να βρούμε καλές γραμμικές προσεγγίσεις για τον DES, βρίσκουμε καλές γραμμικές προσεγγίσεις για ένα γύρο του DES και τις ενώνουμε σε σειρά. Τα S-boxes έχουν 6 bit εισόδου και 4 bit εξόδου. Τα bit εισόδου μπορούν να συνδυαστούν με χρήση XOR κατά 63 τρόπους $(2^6 - 1)$, και τα bit εξόδου κατά 15 τρόπους. Για κάθε S-box μπορούμε να υπολογίσουμε την πιθανότητα, ένας συνδυασμός XOR των bit εισόδου να είναι ίσος με κάποιον συνδυασμό XOR των bit εξόδου, για κάποια τυχαία είσοδο στο S-box. Αν υπάρχει συνδυασμός με αρκετά μεγάλη απόκλιση, τότε η γραμμική κρυπτανάλυση μπορεί να πετύχει.
Το S-box με την μεγαλύτερη απόκλιση είναι το πέμπτο. Για την ακρίβεια, το δεύτερο bit εισόδου είναι ίσο με το XOR και των τεσσάρων bit εξόδου για μόνο 12 τιμές εισόδου στο S-box. Αυτό μεταφράζεται σε μια πιθανότητα 3/16 ή μια απόκλιση 5/16.

Η Εικόνα 17.10 δείχνει πώς χρησιμοποιούμε τις γραμμικές προσεγγίσεις για μια επίθεση κατά του DES. Το bit εισόδου στο S-box 5 είναι το b26 (μετρώντας από αριστερά προς τα δεξιά, από το 1 ως το 64). Τα τέσσερα bit εξόδου από το S-box είναι τα c17, c18, c19, c20. Από το b26 μπορούμε να πάμε αντίστροφα προς τα πάνω. Το a26 γίνεται XOR

με το Ki,26 και μας δίνει το b26. Και το bit X17 περνάει από την μετάθεση διαστολής και δίνει το a26. Μετά το S-box τα 4 bit εξόδου περνούν από το P-box και μετατρέπονται στα τελικά 4 bit εξόδου της επαναλαμβανόμενης συνάρτησης: Y3, Y8, Y14, Y25. Αυτό σημαίνει ότι με πιθανότητα (1/2 - 5/16) ισχύει το

$$X17 \oplus Y3 \oplus Y8 \oplus Y14 \oplus Y25 = Ki,26$$

Γραμμικές προσεγγίσεις για διαφορετικούς γύρους μπορούν να ενωθούν με τρόπο ανάλογο της διαφορικής κρυπτανάλυσης. Η βασική επίθεση είναι να χρησιμοποιήσουμε τις καλύτερες γραμμικές προσεγγίσεις για τον πλήρη DES 16 γύρων. Απαιτεί 247 γνωστά κείμενα και ανακτά 1 bit κλειδιού. Αυτό δεν είναι και πολύ χρήσιμο.



Εικόνα 17.10 Μια γραμμική προσέγγιση ενός γύρου του DES

Παρόλα αυτά υπάρχουν βελτιώσεις. Μια βελτιωμένη έκδοση της επίθεσης έσπασε τον DES σε 50 μέρες χρησιμοποιώντας 12 HP9000/735 σταθμούς εργασίας.

Η γραμμική κρυπτανάλυση βασίζεται κατά το μέγιστο στην κατασκευή των S-boxes. Ο DES δεν έχει S-boxes επιλεγμένα για να αποκρούσουν αυτήν την επίθεση. Η γραμμική κρυπτανάλυση είναι νεότερη από την διαφορική και μπορεί να υπάρχουν σημαντικές βελτιώσεις στα επόμενα χρόνια.

3.7 Παραγοντοποίηση (factoring)

Παραγοντοποίηση ενός αριθμού σημαίνει να βρει κανείς τους πρώτους παράγοντές του. Το πρόβλημα της παραγοντοποίησης είναι ένα από τα αρχαιότερα προβλήματα στην θεωρία αριθμών. Η δυσκολία ισχύει και στις μέρες μας, αλλά έχει γίνει κάποια πρόοδος στην επιστήμη.

Στις μέρες μας ο καλύτερος αλγόριθμος παραγοντοποίησης είναι ο

Αλγόριθμος του κόσκινου πεδίου αριθμών (number field sieve [NFS]). **Το κόσκινο πεδίου γενικών αριθμών (general number field sieve)** είναι ο γρηγορότερος αλγόριθμος για αριθμούς άνω των 110 ψηφίων. Δεν ήταν πρακτικός όταν δημοσιεύτηκε, αλλά ορισμένες βελτιώσεις τον έκαναν αποτελεσματικό.

Άλλοι αλγόριθμοι παραγοντοποίησης έχουν παραγκωνιστεί από τον NFS:

Τετραγωνικό κόσκινο (quadratic sieve). Αυτός είναι ο ταχύτερος αλγόριθμος για αριθμούς μικρότερους από 110 δεκαδικά ψηφία.

Μέθοδος ελλειπτικής καμπύλης (elliptic curve method [ECM]). Η μέθοδος αυτή έχει χρησιμοποιηθεί για να παραγοντοποιήσουμε αριθμούς μέχρι 43 ψηφία.

Αλγόριθμος Monte Carlo του Pollard.

Αλγόριθμος διαδοχικών κλασμάτων (continued fraction algorithm).

Αλγόριθμος δοκιμαστικής διαίρεσης (trial division). Αυτός είναι ο αρχαιότερος αλγόριθμος παραγοντοποίησης και δοκιμάζει κάθε πρώτο αριθμό που είναι μικρότερος ή ίσος με την τετραγωνική ρίζα του υποψήφιου αριθμού.

Σήμερα ο μεγαλύτερος ‘δύσκολος’ αριθμός που έχει παραγοντοποιηθεί είναι γύρω στα 450 bit. Με το χαρακτηρισμό ‘δύσκολος’ εννοούμε ότι δεν έχει μικρούς παράγοντες και δεν είναι ειδικής μορφής που θα καθιστούσε εύκολη την παραγοντοποίησή του.

Πρόσφατα ο Adi Shamir παρουσίασε στο συνέδριο Eurocrypt ’99 ένα σχέδιο για ένα ειδικό μηχάνημα, που μπορεί να επιταχύνει τα πρώτα στάδια της διαδικασίας παραγοντοποίησης ενός αριθμού. Συγκεκριμένα το μηχάνημα επιταχύνει τη διαδικασία του κοσκινίσματος. Η κατασκευή του μηχανήματος βασίζεται στην οπτική ηλεκτρονική.

3.8 Δίκτυα Feistel

Οι περισσότεροι αλγόριθμοι μπλοκ είναι **δίκτυα Feistel** (Feistel networks). Η ιδέα εμφανίστηκε στις αρχές της δεκαετίας του ’70. Η λογική είναι η εξής: Παίρνουμε ένα μπλοκ μήκους *n* και το διαιρούμε σε δύο μισά μήκους *n/2*, *L* και *R*. Φυσικά το *n* πρέπει να είναι άρτιος αριθμός. Έπειτα ορίζουμε έναν επαναλαμβανόμενο αλγόριθμο μπλοκ, όπου το αποτέλεσμα του γύρου *i* εξαρτάται από το αποτέλεσμα του προηγούμενου γύρου:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

K_i είναι το υπο-κλειδί που χρησιμοποιείται κατά τον γύρο *i* και *f* είναι μια οποιαδήποτε επαναλαμβανόμενη συνάρτηση (round function).

Η ιδέα αυτή εφαρμόζεται στον DES, αλλά και σε άλλους αλγόριθμους (Lucifer, FEAL, Khufu, Khafre, LOKI, GOST, CAST, Blowfish κα.) Έχει τόσο μεγάλη απήχηση, επειδή είναι αντιστρέψιμη συνάρτηση. Επειδή χρησιμοποιείται το XOR για να συνδυάσει το αριστερό μισό με το αποτέλεσμα της συνάρτησης *f*, ισχύει οπωσδήποτε ότι

$$L_{i-1} \oplus f(R_{i-1}, K_i) \oplus f(R_{i-1}, K_i) = L_{i-1}$$

Ένας αλγόριθμος που χρησιμοποιεί αυτή τη διάταξη είναι εγγυημένο ότι είναι αντιστρεπτός, αν η είσοδος της συνάρτησης *f* για κάθε γύρο μπορεί να δημιουργηθεί ξανά. Δεν έχει σημασία τι είναι η συνάρτηση *f*· δεν χρειάζεται να είναι αντιστρέψιμη. Μπορούμε να σχεδιάσουμε την *f* να είναι όσο πολύπλοκη θέλουμε, και δεν χρειάζεται να υλοποιήσουμε δύο διαφορετικούς αλγόριθμους για κρυπτογράφηση και αποκρυπτογράφηση.

3.9 RSA

3.9.1 Ιστορικό

Η ιδέα της κρυπτογραφίας δημοσίου κλειδιού βρέθηκε από τους Whitfield Diffie και Martin Hellman, και ανεξάρτητα από τον Ralph Merkle. Η συνεισφορά τους στην κρυπτογραφία ήταν η λογική ότι τα κλειδιά μπορούσαν να υπάρχουν ανά ζεύγη, ένα για κρυπτογράφηση και ένα για αποκρυπτογράφηση, χωρίς να είναι στα όρια του δυνατού να υπολογίσουμε το ένα κλειδί από το άλλο. Πρώτοι οι Diffie και Hellman παρουσίασαν την ιδέα το 1976 στην National Computer Conference. Μερικούς μήνες

μετά δημοσιεύτηκε η εργασία-σταθμός τους «New Directions in Cryptography» (Νέες Κατευθύνσεις στην Κρυπτογραφία)

Από τότε εμφανίστηκαν πολλοί αλγόριθμοι δημοσίου κλειδιού. Πολλοί δεν προσφέρουν ασφάλεια. Κι απ' αυτούς που θεωρούνται ασφαλείς, πολλοί δεν είναι πρακτικά χρήσιμοι. Μόνο μερικοί αλγόριθμοι είναι ασφαλείς και πρακτικοί. Απ' αυτούς τους ασφαλείς και πρακτικούς τους αλγορίθμους, μερικοί είναι κατάλληλοι μόνο για διανομή κλειδιών, άλλοι για κρυπτογράφηση (οπότε και για διανομή κλειδιών) και άλλοι μόνο για ψηφιακές υπογραφές. Μόνο τρεις αλγόριθμοι είναι κατάλληλοι τόσο για κρυπτογράφηση όσο και για υπογραφές: ο RSA, ο ElGamal και

ο Rabin. Και οι τρεις είναι αργοί. Τα υβριδικά κρυπτοσυστήματα επιταχύνουν τη διαδικασία.

3.10 Περιγραφή

Απ' όλους τους αλγόριθμους δημοσίου κλειδιού που έχουν προταθεί, ο RSA είναι ο πιο κατανοητός και εύκολος να υλοποιηθεί. Γι' αυτό ίσως είναι και ο δημοφιλέστερος. Το όνομά του το παίρνει από τα αρχικά των ονομάτων των τριών εφευρετών του, του Ron Rivest, του Adi Shamir και του Leonard Adleman. Έχει αντέξει σε χρόνια κρυπτανάλυσης.

Ο RSA στηρίζει την ασφάλειά του στη δυσκολία παραγοντοποίησης μεγάλων αριθμών. Το δημόσιο και ιδιωτικό κλειδί παίρνουν τις τιμές τους από ένα ζευγάρι μεγάλων πρώτων αριθμών (100 με 200 ψηφία, ή και περισσότερα). Η ανάκτηση του αρχικού κειμένου με χρήση του δημόσιου κλειδιού και του κρυπτογραφήματος θεωρείται ότι είναι ανάλογη της παραγοντοποίησης του γινομένου δύο πρώτων αριθμών.

Για να δημιουργήσουμε τα δύο κλειδιά, διαλέγουμε δύο μεγάλους πρώτους αριθμούς, p και q. Για μέγιστη ασφάλεια, διαλέγουμε τα p και q να είναι ίδιου μήκους. Υπολογίζουμε το γινόμενο:

$$n = pq$$

Έπειτα διαλέγουμε στην τύχη το κλειδί κρυπτογράφησης, e, να είναι τέτοιο ώστε το e και το $(p-1)(q-1)$ να είναι πρώτοι μεταξύ τους αριθμοί. Τελικά, χρησιμοποιούμε τον επεκταμένο αλγόριθμο του Ευκλείδη για να υπολογίσουμε το κλειδί αποκρυπτογράφησης, που δίνεται από τη σχέση

$$ed \equiv 1 \bmod (p-1)(q-1)$$

Με άλλα λόγια:

$$d = e^{-1} \bmod ((p-1)(q-1))$$

Παρατηρούμε ότι τα d και e είναι κι αυτά μεταξύ τους πρώτοι αριθμοί. Οι αριθμοί e και n είναι το δημόσιο κλειδί και το d είναι το ιδιωτικό. Οι δύο πρώτοι αριθμοί p και q δεν μας χρειάζονται πλέον· θα πρέπει να διαγραφούν και ποτέ να μην φανερωθούν.

Για να κρυπτογραφήσουμε ένα μήνυμα m, πρώτα το διαιρούμε σε αριθμητικά μπλοκ μικρότερα του n (για δυαδικά {binary} δεδομένα διαλέγουμε την μεγαλύτερη δύναμη του 2, που να είναι μικρότερη του n).

Δηλαδή, αν τα p και q είναι πρώτοι αριθμοί 100 ψηφίων, τότε το n θα έχει μόλις κάτω από 200 ψηφία.

(Αν χρειάζεται να κρυπτογραφήσουμε ένα καθορισμένο αριθμό μπλοκ, μπορούμε να προσθέσουμε μερικά μηδενικά στα αριστερά για να εξασφαλίσουμε ότι θα είναι πάντα μικρότερα από n.) Το κρυπτογραφημένο μήνυμα, c, θα αποτελείται από μπλοκ παρόμοιου μήκους, c_i. Η σχέση της κρυπτογράφησης είναι απλά

$c_i = m_i^e \bmod n$

Για να αποκρυπτογραφήσουμε το μήνυμα, παίρνουμε το κάθε κρυπτογραφημένο μπλοκ c_i και υπολογίζουμε το

$m_i = c_i^d \bmod n$

Από τη στιγμή που $c_i^d = (m_i^e)^d = m_i^{ed} = m_i^{k(p-1)(q-1)+1} = m_i m_i^{k(p-1)(q-1)} = m_i * 1 = m_i$ (όλα είναι mod n) ο αλγόριθμος ανακτά το μήνυμα.

Κρυπτογράφηση του RSA

Δημόσιο κλειδί

n: γινόμενο δύο πρώτων, p και q (τα p και q πρέπει να παραμείνουν μυστικά)

e: πρώτος σε σχέση με το $(p-1)(q-1)$

Ιδιωτικό κλειδί

d: $e^{-1} \bmod ((p-1)(q-1))$

Κρυπτογράφηση

$c = m^e \bmod n$

Αποκρυπτογράφηση

$m = c^d \bmod n$

3.10.1 Ασφάλεια του RSA

Η ασφάλεια του RSA βασίζεται πλήρως στο πρόβλημα παραγοντοποίησης μεγάλων αριθμών. Για την ακρίβεια, *εικάζεται* ότι η ασφάλεια του RSA βασίζεται στο πρόβλημα παραγοντοποίησης μεγάλων αριθμών. Δεν έχει αποδειχθεί μαθηματικά ότι χρειάζεται να παραγοντοποιήσουμε το n για να υπολογίσουμε το m από τα c και e. Δεν

είναι απίθανο να ανακαλυφθεί ένας τελείως νέος τρόπος κρυπτανάλυσης του RSA. Όμως, αν ο τρόπος αυτός επιτρέπει τον υπολογισμό του *d*, τότε θα μπορούσε να χρησιμοποιηθεί και σαν νέα μέθοδος παραγοντοποίησης μεγάλων αριθμών. Δηλαδή, κατά πάσα πιθανότητα, η κρυπτανάλυση του RSA εξαρτάται από το πρόβλημα παραγοντοποίησης μεγάλων αριθμών.

Είναι επίσης δυνατό να επιτεθούμε στον RSA μαντεύοντας την τιμή $(p-1)(q-1)$. Αυτή η επίθεση έχει τον ίδιο βαθμό δυσκολίας με την παραγοντοποίηση του *n*. Ο αναλυτής θα μπορούσε επίσης να δοκιμάσει όλα τα δυνατά κλειδιά *d*. Αυτό είναι ακόμα πιο δύσκολο κι από την παραγοντοποίηση του *n*.

Η παραγοντοποίηση του *n* είναι η πιο προφανής μέθοδος επίθεσης. Ο αντίπαλος θα έχει το δημόσιο κλειδί, *e*, και το modulus, *n*. Για να βρει το κλειδί αποκρυπτογράφησης, *d*, θα πρέπει να παραγοντοποιήσει το *n*. Από καιρού εις καιρόν εμφανίζονται ισχυρισμοί για εύκολους τρόπους σπασίματος του RSA. Κανένας απ' αυτούς δεν ισχύει.

Υπάρχει και μια άλλη ανησυχία. Οι πιο κοινοί αλγόριθμοι υπολογισμού των *p* και *q* είναι πιθανολογικοί, υπάρχει δηλαδή η πιθανότητα να δώσουν κάποιο σύνθετο αριθμό. Όμως οι πιθανότητες να συμβεί κάτι τέτοιο είναι ελάχιστες. Ακόμα κι αν συμβεί, όμως, το πιθανότερο είναι να το καταλάβουμε, γιατί δεν θα γίνεται σωστή κρυπτογράφηση και αποκρυπτογράφηση. Υπάρχουν μόνο μερικοί αριθμοί, οι αριθμοί Carmichael, που κάποιοι αλγόριθμοι υπολογισμού πρώτων αριθμών δεν θα τους εντοπίσουν. Οι αριθμοί αυτοί είναι ανασφαλείς, αλλά και πάλι η πιθανότητα εμφάνισής τους είναι ελάχιστη.

3.10.2 Προσβολή επιλεγμένου κειμένου εναντίον του RSA

Μερικές επιθέσεις κατευθύνονται ενάντια στην υλοποίηση του RSA. Δεν είναι επιθέσεις ενάντια στον αλγόριθμο αλλά ενάντια στο πρωτόκολλο.

1η εκδοχή: Η Ήρα υποκλέπτει τις επικοινωνίες της Μαρίας, και καταφέρνει να συγκεντρώσει ένα κρυπτογράφημα, *c*, κρυπτογραφημένο με το δημόσιο κλειδί της. Η Ήρα θέλει να διαβάσει το μήνυμα. Μαθηματικά μιλώντας, θέλει το *m*, όπου $m = c^d$

Για να ανακτήσει το *m*, πρώτα διαλέγει έναν τυχαίο αριθμό, *r*, τέτοιο ώστε να είναι μικρότερος του *n*. Παίρνει το δημόσιο κλειδί της Μαρίας, *e*. Έπειτα υπολογίζει τα

$x = r^e \bmod n$

$y = xc \bmod n$

$t = r^{-1} \bmod n$

Αν $x=r^e \bmod n$, τότε $r=x^d \bmod n$.

Έπειτα η Ήρα βρίσκει τον τρόπο να υπογράψει η Μαρία το *y* με το ιδιωτικό κλειδί της, αποκρυπτογραφώντας μ' αυτόν τον τρόπο το *y* (η Μαρία πρέπει να υπογράψει το μήνυμα και όχι την hash τιμή του μηνύματος). Η Μαρία στέλνει στην Ήρα το $u = y^d \bmod n$

Τώρα η Ήρα υπολογίζει το παρακάτω $tu \bmod n = r^{-1} y^d \bmod n =$
$r^{-1} x^d c^d \bmod n = c^d \bmod n = m$
Έτσι η Ήρα αποκτά το *m*.

2η εκδοχή: Ο Δημοσθένης είναι ένα πρόγραμμα που εκτελεί χρέη συμβολαιογράφου. Αν η Μαρία θέλει να επικυρώσει ένα έγγραφο, το στέλνει στον Δημοσθένη. Ο Δημοσθένης το υπογράφει χρησιμοποιώντας τον RSA και το στέλνει πίσω. (Ο Δημοσθένης δεν κρυπτογραφεί την hash τιμή του εγγράφου, αλλά όλο το έγγραφο.)

Ο Έκτορας θέλει να καταφέρει να υπογράψει ο Δημοσθένης ένα έγγραφο που κανονικά δεν θα υπέγραφε. Έστω ότι το μήνυμα αυτό είναι το *m'*.

Αρχικά, ο Έκτορας διαλέγει μια τυχαία τιμή *x* και υπολογίζει το $y=x^e \bmod n$. Μπορεί εύκολα να αποκτήσει το *e*· είναι το δημόσιο κλειδί του Δημοσθένη και πρέπει να είναι προσιτό σε όλους για να μπορούν να επιβεβαιώνονται οι υπογραφές του. Έπειτα ο Έκτορας υπολογίζει το $m=ym' \bmod n$, και στέλνει το *m* στον Δημοσθένη για να το υπογράψει. Ο

Δημοσθένης επιστρέφει το $m'^{d} \bmod n$. Τέλος, ο Έκτορας υπολογίζει το $(m^{d} \bmod n)x^{-1} \bmod n$, που ισούται με $n'^{d} \bmod n$ και είναι η υπογραφή για το *m'*.

Υπάρχουν διάφοροι τρόποι με τους οποίους μπορεί ο Έκτορας να πετύχει τα ίδια. Όλοι βασίζονται στην ιδιότητα

$(xm)^{d} \bmod n = x^{d} m^{d} \bmod n$

3η εκδοχή: Η Ήρα θέλει να υπογράψει η Μαρία το m_3. Δημιουργεί δύο μηνύματα, m_1 και m_2, τέτοια ώστε $m_3 \equiv m_1 m_2 \pmod n$

Αν μπορέσει η Ήρα να καταφέρει να υπογράψει η Μαρία τα m_1 και m_2, μπορεί να υπολογίσει το m_3:

$m_3^{d} = (m_1^{d} \bmod n)(m_2^{d} \bmod n)$

Καταλαβαίνουμε, λοιπόν, ότι θα πρέπει να χρησιμοποιούμε συναρτήσεις hash κατά την υπογραφή.

3.10.3 Επίθεση κοινού modulus στον RSA

Μια πιθανή υλοποίηση του RSA θα μπορούσε να δίνει σε όλους το ίδιο *n*, αλλά διαφορετικούς εκθέτες *e* και *d*. Το σχήμα αυτό δεν λειτουργεί σωστά. Το πιο προφανές πρόβλημα είναι ότι αν ποτέ κρυπτογραφηθεί το ίδιο μήνυμα με δύο διαφορετικούς εκθέτες (που έχουν το ίδιο *n*), και αυτοί οι εκθέτες είναι πρώτοι μεταξύ τους (που γενικά είναι), τότε το κείμενο μπορεί να ανακτηθεί χωρίς τη γνώση οποιουδήποτε από τα δύο κλειδιά αποκρυπτογράφησης.

3.10.4 Επίθεση μικρού εκθέτη κρυπτογράφησης εναντίον του RSA

Η κρυπτογράφηση (και η επιβεβαίωση υπογραφής) με τον RSA γίνεται γρηγορότερη όταν χρησιμοποιούμε μικρό εκθέτη κρυπτογράφησης, *e*, αλλά είναι και επικίνδυνο. Αν κρυπτογραφήσουμε *e(e+1)/2* γραμμικώς εξαρτημένα μηνύματα με διαφορετικά κλειδιά, που να έχουν το ίδιο *e*, υπάρχει δυνατή επίθεση εναντίον του συστήματος. Αν υπάρχουν λιγότερα μηνύματα, ή αν τα μηνύματα είναι γραμμικώς ανεξάρτητα, δεν υπάρχει κίνδυνος. Αν τα μηνύματα είναι ίδια, τότε χρειάζονται μόνο *e* μηνύματα για την επίθεση. Η πιο εύκολη λύση είναι

να επικολλούνται τα μηνύματα με τυχαίες τιμές. Αυτό διασφαλίζει και την ανισότητα $m^e \bmod n \neq m^e$. Οι περισσότερες εφαρμογές του RSA το κάνουν αυτό (PGP, PEM κα.)

3.10.5 Επίθεση μικρού εκθέτη αποκρυπτογράφησης εναντίον του RSA

Μια άλλη επίθεση ανακτά το *d*, όταν το *d* είναι μικρότερο ή ίσο από το ένα τέταρτο του *n* και το *e* είναι μικρότερο του *n*. Αυτό συμβαίνει σπάνια όταν οι εκθέτες επιλέγονται τυχαία, και δεν μπορεί να συμβεί αν το *e* έχει μικρή τιμή.

3.10.6 Βασικοί περιορισμοί

Η Judith Moore αναφέρει κάποιους περιορισμούς στη χρήση του RSA:

- Γνώση ενός ζεύγους εκθετών κρυπτογράφησης-αποκρυπτογράφησης για ένα συγκεκριμένο modulus επιτρέπει στον αντίπαλο να παραγοντοποιήσει το modulus.

- Γνώση ενός ζεύγους εκθετών κρυπτογράφησης-αποκρυπτογράφησης για ένα συγκεκριμένο modulus επιτρέπει στον αντίπαλο να υπολογίσει κι άλλα ζεύγη, χωρίς να χρειάζεται να παραγοντοποιήσει το *n*.
- Δεν θα πρέπει να χρησιμοποιούνται κοινά modulus σε πρωτόκολλο που χρησιμοποιεί τον RSA.

- Τα μηνύματα θα πρέπει να επικολλούνται με τυχαίες τιμές, ώστε να αποφεύγονται επιθέσεις σε μικρούς εκθέτες κρυπτογράφησης.

- Ο εκθέτης αποκρυπτογράφησης πρέπει να είναι μεγάλος.

3.11 MD5

3.11.1 Γενικά

Ο MD5 είναι ένας μονόδρομος αλγόριθμος συμπίεσης (one-way hash function). Μια συνάρτηση hash, *H(M)*, δρα πάνω σε ένα οποιουδήποτε μήκους αρχικό κείμενο, *M*, και επιστρέφει μια τιμή καθορισμένου μήκους, *h*.

h = H(M), όπου το *h* έχει μήκος *m*

Επιπλέον, για να είναι μία συνάρτηση μονόδρομη πρέπει να έχει τα παρακάτω χαρακτηριστικά:

• Δεδομένου του *M*, είναι εύκολο να υπολογίσουμε το *h*.

• Δεδομένου του *h*, είναι δύσκολο να υπολογίσουμε το *M*, έτσι ώστε *h = H(M)*.

• Δεδομένου του *M*, είναι δύσκολο να βρούμε ένα άλλο μήνυμα, *M'*, τέτοιο ώστε *H(M) = H(M')*.

Δηλαδή, σκοπός μιας μονόδρομης συνάρτησης συμπίεσης είναι να δώσει ένα μοναδικό 'αποτύπωμα' του αρχικού κειμένου.

Σε μερικές εφαρμογές τίθεται και μία επιπλέον απαίτηση, που καλείται **αποφυγή συγκρούσεων** (collision resistance).

• Είναι δύσκολο να βρεθούν δύο τυχαία μηνύματα, *M* και *M'*, τέτοια ώστε *H(M) = H(M')*.

Το επόμενο πρωτόκολλο, που περιγράφηκε πρώτη φορά από τον Gideon Yuval, δείχνει πώς η Μαρία θα μπορούσε να εξαπατήσει τον Κώστα, χρησιμοποιώντας την επίθεση γενεθλίων.

1. Η Μαρία ετοιμάζει δύο εκδοχές ενός συμβολαίου: μία ευνοϊκή για τον Κώστα και μία αρνητική γι' αυτόν.

2. Η Μαρία κάνει μερικές ανεπαίσθητες αλλαγές σε κάθε κείμενο και υπολογίζει την τιμή hash για το κάθε ένα. (Οι αλλαγές αυτές θα μπορούσαν να είναι η αντικατάσταση του <SPACE> με <SPACE><BACKSPACE><SPACE>, η τοποθέτηση μερικών κενών

πριν την αλλαγή γραμμής κοκ.) Κάνοντας τέτοιες αλλαγές η Μαρία μπορεί εύκολα να δημιουργήσει 2^{32} διαφορετικά συμβόλαια.

3. Η Μαρία συγκρίνει τις τιμές hash κάθε αλλαγής σε κάθε έγγραφο, ψάχνοντας για ένα ζευγάρι όμοιων τιμών. (Αν ο αλγόριθμος hash παράγει τιμές των 64 bit, τότε συνήθως υπάρχει ένα ζευγάρι ανάμεσα στις 2^{32} εκδοχές του κάθε κειμένου.)

4. Η Μαρία και ο Κώστας υπογράφουν την έκδοση του συμβολαίου που είναι ευνοϊκή γι' αυτόν, χρησιμοποιώντας πρωτόκολλο όπου υπογράφεται μόνο η τιμή hash.

5. Κάποια στιγμή στο μέλλον η Μαρία αντικαθιστά το συμβόλαιο που υπέγραψε ο Κώστας με το συμβόλαιο που δεν υπέγραψε. Τώρα μπορεί να πείσει τον δικαστή ότι ο Κώστας υπέγραψε το καταδικαστικό γι' αυτόν συμβόλαιο.

Πρέπει, λοιπόν, να χρησιμοποιούμε μονόδρομες συναρτήσεις hash που δίνουν hash τιμές ικανοποιητικού μήκους. Σήμερα τα 128 bit είναι ακόμα ασφαλή, αλλά δεν υπάρχει λόγος να μην χρησιμοποιήσουμε τιμές των 160 bit.

3.11.2 Περιγραφή του MD5

Μετά από κάποια αρχική διεργασία, ο MD5 επεξεργάζεται το αρχικό κείμενο σε μπλοκ των 512 bit, χωρισμένα σε 16 32-μπιτα υπο-μπλοκ. Η έξοδος του αλγορίθμου είναι ένα σετ τεσσάρων 32-μπιτων μπλοκ, που ενώνονται σχηματίζοντας μία 128-μπιτη τιμή hash.

Αρχικά, το μήνυμα συμπληρώνεται κατάλληλα ώστε το μήκος του να είναι μόλις 64 bit μικρότερο από το πλησιέστερο προς τα πάνω πολλαπλάσιο του 512. Το συμπλήρωμα αυτό είναι ένας άσσος, που προστίθεται στο τέλος του κειμένου, ακολουθούμενος από όσα μηδενικά χρειάζονται. Έπειτα ένας αριθμός 64 bit, που ισούται με το μέγεθος του μηνύματος (πριν προστεθεί το συμπλήρωμα), προσαρτάται στο επαυξημένο μήνυμα. Αυτά τα δύο βήματα έχουν σκοπό να μετατρέψουν το μήκος του μηνύματος σε πολλαπλάσιο των 512 bit (που είναι απαραίτητο για την εκτέλεση του αλγορίθμου), και παράλληλα εγγυώνται ότι διαφορετικά μηνύματα δεν πρόκειται να έχουν την ίδια μορφή μετά την προσθήκη του συμπληρώματος.

Κατόπιν, τέσσερις 32-μπιτες μεταβλητές αρχικοποιούνται:

A = 0x01234567
B = 0x89abcdef
C = 0xfedcba98
D = 0x76543210

Αυτές καλούνται **συνδετικές μεταβλητές** (chaining variables).

Από ‘δω και πέρα αρχίζει ο κύριος βρόχος του αλγορίθμου. Ο βρόχος εκτελείται τόσες φορές, όσα είναι τα μπλοκ 512 bit στο κείμενο.

Οι τέσσερις μεταβλητές αντιγράφονται σε διαφορετικές μεταβλητές: το *a* ισούται με *A*, το *b* ισούται με *B*, το *c* ισούται με *C* και το *d* ισούται με *D*.

Ο κύριος βρόχος έχει τέσσερις γύρους (ο MD4 είχε μόνο 3), όλοι τους παρόμοιοι. Κάθε γύρος χρησιμοποιεί μια διαφορετική διαδικασία 16 φορές. Κάθε διαδικασία εκτελεί μια μη γραμμική συνάρτηση ανάμεσα σε τρεις από τις μεταβλητές *a*, *b*, *c*, *d*. Έπειτα προσθέτει το αποτέλεσμα στην τέταρτη μεταβλητή, μαζί με ένα υπο-μπλοκ του κειμένου και μια σταθερά. Έπειτα κυλίει κυκλικά το αποτέλεσμα προς τα δεξιά, κατά ένα μεταβλητό αριθμό bit και προσθέτει το αποτέλεσμα σε ένα από τα *a*, *b*, *c*, *d*. Τέλος, το αποτέλεσμα της πρόσθεσης αντικαθιστά ένα από τα *a*, *b*, *c*, *d*.

Υπάρχουν τέσσερις μη γραμμικές συναρτήσεις, κάθε μία χρησιμοποιούμενη σε μια διαδικασία (διαφορετική για κάθε γύρο).

$$F(X, Y, Z) = (X \wedge Y) \vee ((\neg X) \wedge Z)$$

$$G(X, Y, Z) = (X \wedge Z) \vee (Y \wedge (\neg Z))$$

$$H(X, Y, Z) = X \oplus Y \oplus Z$$

$I(X, Y, Z) = Y \oplus (X \vee (\neg Z))$

(το $\oplus$ είναι XOR, το $\wedge$ είναι AND, το $\vee$ είναι OR, και το $\neg$ είναι NOT.)

Αυτές οι συναρτήσεις είναι σχεδιασμένες ώστε, αν τα bit που αντιστοιχούν στα X, Y, Z είναι ανεξάρτητα μεταξύ τους, τότε και κάθε bit του αποτελέσματος να είναι ανεξάρτητο. Η συνάρτηση F είναι η συνθήκη: Αν X τότε Y διαφορετικά Z, εκφρασμένη σε bit. Η συνάρτηση H είναι ο τελεστής ισοτιμίας για bit.

Αν το Mj αντιπροσωπεύει το j υπο-μπλοκ του μηνύματος (από 0 ως 15), και το <<<s αντιπροσωπεύει ένα αριστερό κυκλικό κύλισμα κατά s bit, τότε οι τέσσερις διαδικασίες είναι οι παρακάτω:

FF(a,b,c,d,Mj,s,ti) σημαίνει a = b + ((a + F(b,c,d) + Mj + ti) <<< s)

GG(a,b,c,d,Mj,s,ti) σημαίνει a = b + ((a + G(b,c,d) + Mj + ti) <<< s)

HH(a,b,c,d,Mj,s,ti) σημαίνει a = b + ((a + H(b,c,d) + Mj + ti) <<< s)

II(a,b,c,d,Mj,s,ti) σημαίνει a = b + ((a + I(b,c,d) + Mj + ti) <<< s)

Οι σταθερές ti επιλέγονται ως εξής:

Κατά το βήμα i, το ti είναι το ακέραιο μέρος του 232*abs(sin(i)), όπου το i είναι σε ακτίνια.

Μετά απ' όλα αυτά, τα a, b, c, d προστίθενται στα A, B, C, D αντίστοιχα, και ο αλγόριθμος συνεχίζει με το επόμενο μπλοκ δεδομένων. Το τελικό αποτέλεσμα είναι η συνένωση των A, B, C, D.

Κεφάλαιο 4ο

Η Ανάγκη Προστασίας Των Δικτύων & Αρχιτεκτονική Ασφάλειας Internet

Ασφάλεια δικτύων και ασφαλείς συναλλαγές

4.1 Η Σημασία των Δικτύων

Εισαγωγικές Παρατηρήσεις

Η χρήση των δικτύων από επιχειρήσεις συνεχίζει να αυξάνεται και επενδύσεις σε τεχνολογίες ηλεκτρονικού εμπορίου και ηλεκτρονικού χρήματος υλοποιούνται καθημερινά και με ταχύτατα αυξανόμενους ρυθμούς. Η δημόσια διοίκηση συνεχίζει να επεκτείνει τόσο το πεδίο εφαρμογής όσο και το μέγεθος των δικτυακών της συνδέσεων. Επιπλέον, οι τεχνολογίες πληροφοριών και επικοινωνιών εμφανίζονται απαρέγκλιτα σε οποιοδήποτε σχέδιο βελτίωσης της αποτελεσματικότητας της λειτουργίας της δημόσιας διοίκησης.

4.1.1 Η Κοινωνία της Πληροφορίας

Το Συμβούλιο της Ευρώπης, στη συνεδρίασή του το Δεκέμβριο του 1993 στις Βρυξέλλες, αποφάσισε να αναθέσει σε μια επιτροπή υψηλού επιπέδου, με πρόεδρο τον Martin Bangemann, επίτροπο της Ευρωπαϊκής Επιτροπής, το έργο της σύνταξης μιας έκθεσης με θέμα *«Ευρώπη και η Παγκόσμια Κοινωνία της Πληροφορίας. Συστάσεις προς το Συμβούλιο της Ευρώπης»*. Η έκθεση χρησιμοποιήθηκε ως βάση της συζήτησης στη Σύνοδο της Κέρκυρας (24–25 Ιουνίου 1994). Στην έκθεση, γνωστή πια ως «Έκθεση Bangemann», αναφέρονται τα εξής: *«Σ' ολόκληρο τον κόσμο, οι τεχνολογίες πληροφοριών και επικοινωνιών προκαλούν μια νέα βιομηχανική επανάσταση, ήδη εξίσου σημαντική και εκτεταμένη όσο –τουλάχιστον– και οι προηγούμενες. Είναι μια επανάσταση βασισμένη στην*

πληροφορία, που αντιπροσωπεύει αυτή καθαυτή την ανθρώπινη γνώση. Η τεχνολογική πρόοδος μας επιτρέπει τώρα να επεξεργαζόμαστε, να αποθηκεύουμε, να ανακτούμε και να μεταδίδουμε πληροφορία σε οποιαδήποτε μορφή θέλουμε: προφορική, γραπτή ή οπτική, χωρίς περιορισμούς απόστασης, χρόνου και όγκου. Η επανάσταση αυτή προσθέτει τεράστιες νέες δυνατότητες στην ανθρώπινη νοημοσύνη και μεταβάλλει τον τρόπο που ζούμε και που εργαζόμαστε».

Από τότε, ο όρος «Κοινωνία της Πληροφορίας» μπήκε για τα καλά στο καθημερινό λεξιλόγιο εκατομμυρίων Ευρωπαίων. Αλλά τι ακριβώς είναι η Κοινωνία της Πληροφορίας; Στην ουσία αποτελείται από τρία επάλληλα και πολύ στενά συνδεμένα στρώματα τεχνολογίας:

- ένα βασικό δίκτυο επικοινωνιών,
- ένα σύνολο υπηρεσιών γενικής φύσης (π.χ. ηλεκτρονικό ταχυδρομείο, αλληλεπιδραστικό video κτλ.)
- εφαρμογές, που μπορούν να κυμαίνονται από πραγματοποίηση ***τραπεζικών εργασιών από απόσταση (telebanking)*** μέχρι ***ιδεατή ιατρική (virtual medicine)***.

4.1.2 Το Ηλεκτρονικο Εμπόριο

Από τη σκοπιά των επιχειρήσεων, το δίκτυο χωρίζεται σε τρεις επιχειρηματικές περιοχές: το εσωτερικό δίκτυο (intranet), το εξωτερικό δίκτυο (extranet) και το διαδίκτυο (internet).
Αυτά διακρίνονται ως εξής:

- Στο περιβάλλον του εσωτερικού δικτύου όλοι οι χρήστες βρίσκονται κάτω από τον έλεγχο ενός και μοναδικού οργανισμού. Οι κόμβοι ανήκουν σε υπαλλήλους ή υπεργολάβους, που όλοι τους έχουν ελεγχόμενες συμβατικές σχέσεις με το τελικό σύστημα (host).

- Στο περιβάλλον του εξωτερικού δικτύου οι χρήστες επεκτείνονται και περιλαμβάνουν τους πελάτες, τους προμηθευτές και τους συνεταίρους, με τους οποίους ο ιδιοκτήτης του τελικού συστήματος έχει συμβατική σχέση.

- Στο περιβάλλον του διαδικτύου οι χρήστες μπορούν να είναι εκτός του οργανισμού και να περιλαμβάνουν πιθανούς πελάτες, πιθανούς προμηθευτές, πιθανούς συνεταίρους και ανταγωνιστές, με τους οποίους δεν υφίσταται καμιά συμβατική σχέση.

Οι ορισμοί αυτοί δε σχετίζονται με τη γεωγραφική θέση των χρηστών και τα όρια ανάμεσα στις περιοχές είναι μάλλον ασαφή και ταυτόχρονα πολύπλοκα.

Οι προοπτικές για το ορατό μέλλον είναι να αυξηθεί ακόμη περισσότερο η επιχειρηματική χρήση των δικτύων. Η συνολική αξία των συναλλαγών που θα πραγματοποιούνται ηλεκτρονικά το έτος 2000 στις ΗΠΑ προβλέπεται να είναι ανάμεσα στα 130.000.000.000 και στα 200.000.000.000 δολάρια, με μέση ετήσια αξία ανά πελάτη 600–800 δολάρια, μέση αξία ανά συναλλαγή 25–35 δολάρια, ενώ προβλέπεται ότι το 60%–70% των συνολικά προσφερόμενων αγαθών θα είναι διαθέσιμα προς πώληση στο δίκτυο.

Όσα όμως επιχειρηματικά οφέλη φαίνεται να παρέχει η χρήση των δικτύων αναιρούνται, αν η χρήση αυτή δεν είναι ασφαλής. Είναι φανερό ότι ένας πωλητής που ταξιδεύει θα πρέπει να μπορεί να στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου στη βάση του χωρίς να παραβιαστεί η **εμπιστευτικότητα** του μηνύματος.

Πώς μπορεί να ξέρει ο χρήστης που συνδέεται με τη σελίδα μιας επιχείρησης στον παγκόσμιο ιστό ότι πράγματι η σελίδα ανήκει στην εταιρεία; Αν κάποια σελίδα είναι σφραγισμένη, πώς μπορεί να ξέρει ο χρήστης ότι η σφραγίδα είναι αυθεντική και όχι αντίγραφο σφραγίδας από άλλη σελίδα; Με άλλα λόγια, η διαφύλαξη της **ακεραιότητας** της πληροφορίας είναι επίσης σημαντική.

Για να γίνει αντιληπτή η οικονομική σημασία της διατήρησης της **διαθεσιμότητας** της πληροφορίας, αρκεί να αναφέρουμε ότι ένα τρις δολάρια διακινούνται μέσω τραπεζών ηλεκτρονικά κάθε χρόνο.

Αυτό σημαίνει ότι για κάθε μέρα που το δίκτυο δεν είναι διαθέσιμο η απώλεια σε τόκους υπολογίζεται σε 30 εκατομμύρια δολάρια. Η θέση αυτή επιβεβαιώνεται και από τα αποτελέσματα μιας έρευνας που έγινε στις ΗΠΑ σχετικά με τα προβλήματα στην ανάπτυξη του διαδικτύου, όπως τα αντιλαμβάνονται οι επιχειρήσεις.

4.2 Πρωτόκολλα ασφάλειας επιπέδου μεταφοράς

Όπως και με τα πρωτόκολλα επιπέδου Internet, η ιδέα προτυποποίησης ενός πρωτοκόλλου ασφάλειας για το επίπεδο μεταφοράς δεν είναι καινούρια. Πριν ακόμη την εμφάνιση της ομάδας εργασίας TLS (Transport Layer Security) της IETF, είχαν προταθεί τα εξής πρωτόκολλα:

• Το πρωτόκολλο ***Security Protocol 4 (SP4)*** είναι πρωτόκολλο επιπέδου μεταφοράς, που αναπτύχθηκε από την NSA και το NIST ως τμήμα της ομάδας πρωτοκόλλων SDNS.

• Το πρωτόκολλο *Transport Layer Security Protocol (TLSP)* αναπτύχθηκε και προτυποποιήθηκε από τον ISO.

• Οι Matt Blaze και Steven Bellovin της AT&T Bell Labs ανέπτυξαν ένα πακέτο λογισμικού με το όνομα ***Encrypted Session Manager (ESM)***, που σε πολλά του σημεία μοιάζει με το Secure Shell (SSH), το οποίο θα συζητήσουμε αμέσως μετά.

4.2.1 ΤΟ ΠΡΩΤΟΚΟΛΛΟ Secure Shell

Το ***Secure Shell (SSH)*** είναι ένα σχετικά απλό πρόγραμμα, που μπορεί να χρησιμοποιηθεί για να συνδεθεί κανείς ασφαλώς σε απομακρυσμένη μηχανή, να εκτελέσει εντολές στη μηχανή αυτή και να μετακινήσει αρχεία από μια μηχανή σε άλλη. Το SSH παρέχει ισχυρή αυθεντικοποίηση και ασφαλείς επικοινωνίες μέσω ανασφαλών καναλιών. Η πρόθεση κατασκευής του ήταν να μπορεί να αντικαταστήσει τα εργαλεία rlogin, rsh, rdist, rcp. Επίσης μπορεί, σε πολλές περιπτώσεις, να αντικαταστήσει το telnet.

Το SSH παρέχει υποστήριξη για αυθεντικοποίηση μηχανής αλλά και αυθεντικοποίηση χρήστη, μαζί με συμπίεση δεδομένων, και προστασία ακεραιότητας και εμπιστευτικότητας δεδομένων. Ένα μειονέκτημά του είναι το γεγονός ότι χρησιμοποιεί προκαθορισμένα δημόσια κλειδιά που δε διανέμονται αυτόματα, αντί για ένα σχήμα διαχείρισης κλειδιών βασισμένο σε πιστοποιητικά.

Το πρωτόκολλο αρχίζει με τον πελάτη να στέλνει μια αίτηση αυθεντικοποίησης στον εξυπηρετητή. Ο εξυπηρετητής, με τη σειρά του, στέλνει πίσω στον πελάτη το δημόσιο κλειδί του κεντρικού συστήματος, που είναι συνήθως κλειδί RSA μήκους 1024 bits, και ένα δημόσιο κλειδί εξυπηρετητή, που είναι συνήθως κλειδί RSA μήκους 768 bits και αλλάζει κάθε ώρα. Ο σκοπός του κλειδιού κεντρικού συστήματος είναι να συσχετίσει τη σύνδεση με το επιθυμητό κεντρικό σύστημα εξυπηρετητή, ενώ οσκοπός του κλειδιού εξυπηρετητή είναι να κάνει αδύνατη την αποκρυπτογράφηση καταγραμμένης κίνησης, ακόμη και αν σπάσει το κλειδί κεντρικού συστήματος. Επομένως, το κλειδί εξυπηρετητή δεν πρέπει ποτέ να σώζεται στο δίσκο.
Ο πελάτης τώρα συγκρίνει το κλειδί κεντρικού συστήματος που έλαβε με εκείνα τα κλειδιά που είχαν διανεμηθεί και καθοριστεί εκ των προτέρων και που βρίσκονται αποθηκευμένα σε κάποια βάση δεδομένων του.

Φυσιολογικά, ο πελάτης αποδέχεται το κλειδί ενός άγνωστου κεντρικού συστήματος και το αποθηκεύει στη βάση του για μελλοντική χρήση. Αυτό κάνει τη χρήση του SSH πρακτική στα περισσότερα περιβάλλοντα. Ωστόσο, σε περιβάλλοντα υψηλής ασφάλειας, είναι δυνατόν να διαμορφώσουμε τον πελάτη SSH έτσι ώστε να αρνείται πρόσβαση σε οποιοδήποτε κεντρικό σύστημα του οποίου το κλειδί δεν υπάρχει ήδη στη βάση κλειδιών του. Αν ο πελάτης αποδεχτεί το κλειδί του κεντρικού συστήματος, δημιουργεί ένα κλειδί μήκους 256 bits, το οποίο χρησιμοποιείται ως το κλειδί της συνόδου.

Επιπλέον, ο πελάτης επιλέγει έναν αλγόριθμο κρυπτογράφησης απ' αυτούς που υποστηρίζει ο εξυπηρετητής, συνήθως Blowfish, DES ή 3DES τριπλού κλειδιού σε λειτουργία Chain Block Cipher (CBC). Ο πελάτης συμπληρώνει το κλειδί συνόδου με τυχαία bytes, το κρυπτογραφεί διπλά, με τα δημόσια κλειδιά του κεντρικού συστήματος και του εξυπηρετητή, και στέλνει το αποτέλεσμα στον εξυπηρετητή.

Ο εξυπηρετητής το αποκρυπτογραφεί και παραλαμβάνει το κλειδί συνόδου. Και τα δύο μέρη μπορούν τώρα να χρησιμοποιήσουν το κλειδί συνόδου και να κρυπτογραφήσουν διαφανώς τη σύνδεση. Ο εξυπηρετητής στέλνει μια κρυπτογραφημένη επιβεβαίωση του γεγονότος αυτού στον πελάτη. Η λήψη της επιβεβαίωσης αυτής σημαίνει για τον πελάτη ότι ο εξυπηρετητής ανέκτησε επιτυχώς το κλειδί συνόδου, και ότι πρέπει, κατά συνέπεια, να κρατήσει τα ιδιωτικά κλειδιά του. Από τη στιγμή αυτή, ο πελάτης εμπιστεύεται τον εξυπηρετητή ως αυθεντικό και θεωρεί ότι η προστασία ακεραιότητας και η κρυπτογράφηση επιπέδου μεταφοράς λειτουργούν καλώς. Σε μερικές περιπτώσεις είναι δυνατόν να χρειάζεται και αυθεντικοποίηση χρήστη.

Η αντίστοιχη ανταλλαγή ξεκινάει από τον πελάτη, που στέλνει μια αίτηση αυθεντικοποίησης στον εξυπηρετητή. Η αίτηση περιλαμβάνει το όνομα χρήστη που θέλει να συνδεθεί. Ανάλογα με τη μέθοδο αυθεντικοποίησης, ο διάλογος μεταξύ πελάτη και εξυπηρετητή μπορεί να διαφέρει. Υπάρχουν δύο τέτοιες μέθοδοι:

• Στην περίπτωση της ***αυθεντικοποίησης με συνθηματικό***, το συνθηματικό του χρήστη μεταφέρεται μέσω του καναλιού επικοινωνίας που είναι διαφανώς κρυπτογραφημένο με SSH.

• Στην περίπτωση της ***αυθεντικοποίησης RSA***, ο εξυπηρετητής προκαλεί τον πελάτη με έναν τυχαίο αριθμό, ο οποίος είναι κρυπτογραφημένος με το δημόσιο κλειδί του χρήστη. Στην περίπτωση αυτή, ο εξυπηρετητής πρέπει επίσης να έχει πρόσβαση σε μια βάση προκαθορισμένων και χειροκίνητα διανεμηθέντων δημόσιων κλειδιών των εγγεγραμμένων χρηστών. Ο πελάτης μπορεί να αποκρυπτογραφήσει την πρόκληση μόνο αν γνωρίζει το ιδιωτικό κλειδί του χρήστη. Επομένως, ζητάει μια συνθηματική φράση που απαιτείται προκειμένου να ξεκλειδωθεί προσωρινά το ιδιωτικό κλειδί του χρήστη. Για να αυθεντικοποιηθεί στον εξυπηρετητή, ο πελάτης πρέπει να απαντήσει με τη σωστή τιμή σύνοψης MD5 της αποκρυπτογραφημένης πρόκλησης και κάποια επιπλέον δεδομένα που συσχετίζουν το αποτέλεσμα με την τρέχουσα σύνοδο.

Και στις δύο περιπτώσεις ο εξυπηρετητής πρέπει να απαντήσει με ένα μήνυμα επιτυχούς ή αποτυχημένης αυθεντικοποίησης. Αν δεν απαιτείται αυθεντικοποίηση πελάτη, ή αν ο πελάτης μπόρεσε επιτυχώς να αυθεντικοποιηθεί στον εξυπηρετητή, μπορεί τώρα να ζητήσει την παροχή μιας υπηρεσίας. Ειδικότερα, μπορεί να συνδεθεί ασφαλώς με ένα απομακρυσμένο σύστημα (slogin), να εκτελέσει εντολές (ssh), να μεταφέρει αρχεία (scp) κλπ. Τα κλειδιά συνόδου μπορούν επίσης να επανανταλλαγούν δυναμικά. Επίσης, υπάρχουν και διάφορα εργαλεία που ο πελάτης και ο εξυπηρετητής μπορούν να χρησιμοποιήσουν για τη διαχείριση του SSH και των σχετικών αρχείων.

Η ομάδα εργασίας Secure Shell (SECSH) της IETF, το Σεπτέμβριο του 1996, πρότεινε – σε Internet Draft— τη διαίρεση του πρωτοκόλλου SSH, όπως το περιγράψαμε εδώ, σε ένα πρωτόκολλο επιπέδου μεταφοράς SSH (SSH transport layer protocol) και σε ένα πρωτόκολλο αυθεντικοποίησης SSH (SSH authentication protocol), που λειτουργεί πάνω από το SSH transport layer protocol.

4.2.2 ΤΟ ΠΡΟΤΟΚΟΛΛΟ SSL/TLS

Το πρωτόκολλο TCP παρέχει μια αξιόπιστη ροή bytes μεταξύ δύο κόμβων. Το πρωτόκολλο αυτό είναι προσανατολισμένο σε σύνδεση και έχει κατάσταση, ανιχνεύει απώλειες πακέτων και λήψη πακέτων εκτός σειράς και απορρίπτει επαναλαμβανόμενα δεδομένα. Το πρωτόκολλο, επίσης, εκτελεί αυθεντικοποίηση οντότητας βασισμένη σε διευθύνσεις, όταν εγκαθιστά σύνοδο μεταξύ δύο κόμβων. Το TCP δεν υποστηρίζει ισχυρή κρυπτογραφική αυθεντικοποίηση οντοτήτων, ακεραιότητα δεδομένων και εμπιστευτικότητα. Οι υπηρεσίες αυτές εισάχθηκαν στο ***πρωτόκολλο Secure Socket Layer (SSL)***, που αναπτύχθηκε από την Netscape, κυρίως για να προστατεύσει την κίνηση στον παγκόσμιο ιστό. Η προδιαγραφή ***Transport Layer Security (TLS)*** της IETF είναι σχεδόν ταυτόσημη με την έκδοση 3 του SSL και γι’ αυτό το πρωτόκολλο είναι τώρα γνωστό ως SSL/TLS.

Μέσα στη σειρά πρωτοκόλλων Internet, το SSL βρίσκεται μεταξύ του επιπέδου εφαρμογής και του TCP. Επομένως, το SSL μπορεί να βασίζεται στις ιδιότητες που εγγυάται το TCP και, για παράδειγμα, δε χρειάζεται να ασχοληθεί με την αξιόπιστη παράδοση των δεδομένων.

Όπως και το TCP, το SSL έχει κατάσταση και είναι προσανατολισμένο σε σύνδεση. Η κατάσταση συνόδου SSL περιέχει πληροφορίες που

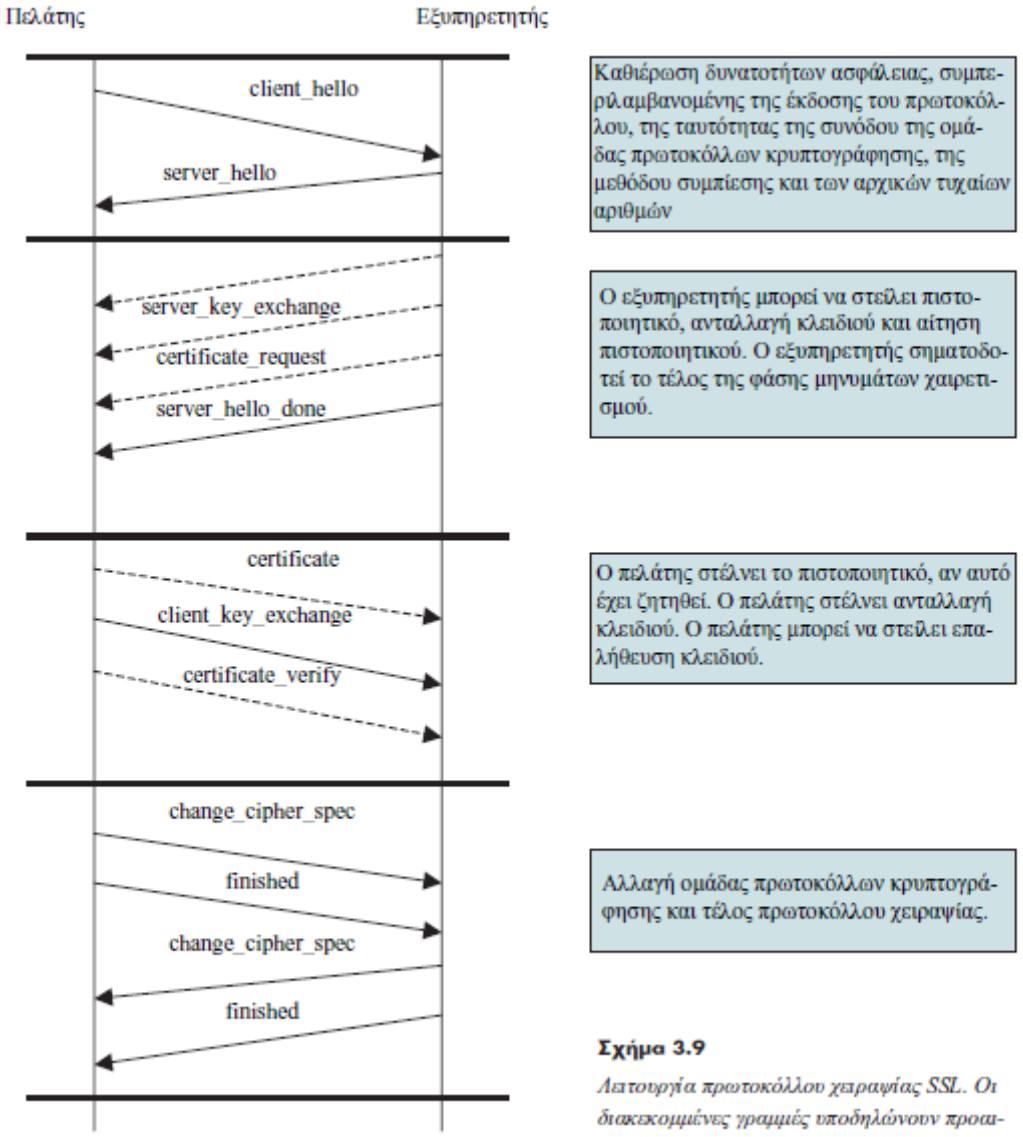
απαιτούνται για την εκτέλεση κρυπτογραφικών αλγόριθμων, όπως ταυτότητα συνόδου, καθορισμός κρυπτογραφικού συστήματος, κοινά μυστικά κλειδιά, πιστοποιητικά, τυχαίες τιμές που χρησιμοποιούν πρωτόκολλα, όπως το πρωτόκολλο Diffie–Hellman, κ.λπ. Για να εξυπηρετήσει την επιβάρυνση που προκαλείται από τη διαχείριση κλειδιών, μια σύνοδος SSL μπορεί να περιέχει πολλαπλές συνδέσεις. Το χαρακτηριστικό παράδειγμα είναι μια σύνοδος HTTP μεταξύ ενός πελάτη και ενός εξυπηρετητή, όπου δημιουργείται μια καινούργια σύνδεση για τη μεταφορά ενός σύνθετου εγγράφου. Μόνο ένα υποσύνολο της πληροφορίας κατάστασης χρειάζεται να αλλάξει για κάθε σύνδεση.

Το πρωτόκολλο SSL υποδιαιρείται σε δύο υπο–πρωτόκολλα:
• Το *πρωτόκολλο εγγραφής SSL* και
• Το *πρωτόκολλο χειραψίας SSL*.

Το πρωτόκολλο εγγραφής SSL δέχεται blocks δεδομένων από ένα πρωτόκολλο ανώτερου επιπέδου, τα τεμαχίζει σε μη κρυπτογραφημένες εγγραφές SSL και μετά εφαρμόζει τον κρυπτογραφικό μετασχηματισμό που καθορίζεται από την παράμετρο
cipher spec στην τρέχουσα κατάσταση συνόδου. Βασικά, το πρωτόκολλο αυτό παρέχει μια υπηρεσία παρόμοια με αυτή του IPsec, η δε ομοιότητα ανάμεσα στη σύναψη ασφάλειας του IPsec και την κατάσταση SSL δεν είναι καθόλου τυχαία.

Το πρωτόκολλο χειραψίας SSL είναι το βασικό πρωτόκολλο που βρίσκεται πάνω από το πρωτόκολλο εγγραφής SSL. Μηνύματα χειραψίας SSL παρέχονται στο πρωτόκολλο εγγραφής SSL, όπου εσωκλείονται μέσα σε μία ή περισσότερες εγγραφές SSL, οι οποίες υφίστανται επεξεργασία και μεταδίδονται όπως καθορίζει η μέθοδος
συμπίεσης και οι προδιαγραφές κρυπτογράφησης των τρεχουσών καταστάσεων συνόδου και σύνδεσης. Ο σκοπός του πρωτοκόλλου χειραψίας SSL είναι να μπορέσουν ο πελάτης και ο εξυπηρετητής να

συμφωνήσουν για τα πρωτόκολλα που θα χρησιμοποιήσουν στην επικοινωνία τους, να επιλέξουν τη μέθοδο συμπίεσης και τις προδιαγραφές κρυπτογράφησης, πιθανόν να αυθεντικοποιηθούν αμοιβαία, και να δημιουργήσουν ένα βασικό μυστικό, από το οποίο είναι δυνατόν να παραχθούν τα διάφορα κλειδιά συνόδων για κρυπτογράφηση και ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ μηνυμάτων.



Σχήμα 3.9

Λειτουργία πρωτοκόλλου χειραψίας SSL. Οι διακεκομμένες γραμμές υποδηλώνουν προαιρετικά μηνύματα

Το ηλεκτρονικό εμπόριο γενικά, και ειδικότερα μέσω του Internet, εξαρτάται από τη διαθεσιμότητα και την ευρεία διάδοση συστημάτων ηλεκτρονικών πληρωμών.

Τα συστήματα αυτά μπορεί να εμπλέκουν διάφορους εταίρους και μεθόδους πληρωμής.

Στην ενότητα αυτή συζητάμε σύντομα μερικά συστήματα ηλεκτρονικής πληρωμής.

Ειδικότερα, εστιάζουμε σε συστήματα ηλεκτρονικού χρήματος, ηλεκτρονικών επιταγών, πληρωμών με πιστωτικές κάρτες και μικροπληρωμών.

Πέρα όμως απ' αυτές, υπάρχουν και κάποιες άλλες μορφές ηλεκτρονικών πληρωμών, όπως εντολές πληρωμής, τραπεζικές επιταγές, πληρωμές με κάρτες ανάληψης, εντολές αγοράς και ταξιδιωτικές επιταγές. Επιπλέον, υπάρχουν και κάποια συστήματα ηλεκτρονικών πληρωμών που δε χρησιμοποιούν καθόλου κρυπτογραφία. Πιθανόν το πιο γνωστό σύστημα αυτής της κατηγορίας είναι το σύστημα της First Virtual Holdings Inc., στο οποίο οι χρήστες εγγράφονται δίνοντας πληροφορίες σχετικές με την ταυτότητά τους
και την πιστωτική τους κάρτα. Η εταιρεία, στη συνέχεια, τους δίνει ένα μοναδικό αριθμό αναγνώρισης. Όταν ο χρήστης θελήσει να κάνει μια πληρωμή, στέλνει το μοναδικό του αριθμό αναγνώρισης στον έμπορο.

Ο έμπορος, με τη σειρά του, επιβεβαιώνει τον αριθμό αναγνώρισης με το σύστημα και το σύστημα επιβεβαιώνει την πληρωμή με τον πελάτη. Με τη λήψη της επιβεβαίωσης, τα χρήματα μεταφέρονται off–line. Η εταιρεία χρησιμοποιεί ηλεκτρονικό ταχυδρομείο για την τοποθέτηση και επιβεβαίωση εντολών πληρωμής, ενώ η μεταφορά χρημάτων γίνεται off–line, μέσω ιδιωτικών δικτύων.

Στον πυρήνα οποιουδήποτε συστήματος ηλεκτρονικών πληρωμών βρίσκεται ένα ή περισσότερα ***πρωτόκολλα πληρωμής***. Αυτά είναι γενικής φύσης και δεν πρέπει να εξαρτώνται από τα χρησιμοποιούμενα μέσα μεταφοράς. Στην πραγματικότητα ένα πρωτόκολλο πληρωμής μπορεί να υλοποιηθεί μέσα σε WWW browsers που χρησιμοποιούν HTTP, μέσα σε πράκτορες ηλεκτρονικού ταχυδρομείου που χρησιμοποι-

ούν SMTP, ή μέσα σε κάποιο άλλο πρόγραμμα που χρησιμοποιεί ένα συγκεκριμένο πρωτόκολλο εφαρμογής. Σε κάθε περίπτωση πρέπει να είναι βέβαιο ότι τα δεδομένα που εμπλέκονται στην εκτέλεση ενός πρωτοκόλλου ηλεκτρονικής πληρωμής είναι ασφαλή ακόμη και αν το μέσο δεν είναι. Στην περίπτωση που το ανασφαλές μέσο δεχτεί επίθεση, ο επιτιθέμενος πρέπει να μη μπορεί να κερδίσει τίποτε περισσότερο από δεδομένα χωρίς νόημα.

Είναι δυνατό και πολύ πιθανό να δούμε πολλά συστήματα ηλεκτρονικών πληρωμών να συνυπάρχουν στο μέλλον. Επομένως, πρέπει να υπάρχει ένα *στρώμα διαπραγμάτευσης* πάνω από τα αντίστοιχα συστήματα. Το Δεκέμβριο του 1995 το WWW Consortium και το CommerceNet Consortium συγχρηματοδότησαν την ***Κοινή Πρωτοβουλία Ηλεκτρονικού Εμπορίου (Joint Electronic Payment Initiative – JEPI)***, με σκοπό τη συνεργασία των βασικών παικτών της βιομηχανίας στην κατεύθυνση της εξασφάλισης ότι διαφορετικά συστήματα πληρωμής, πρωτόκολλα και μηχανισμοί μεταφοράς θα μπορούν να συνεργαστούν μέσω του Internet.

Συνοπτικά, η JEPI έχει ως σκοπό την πραγματοποίηση της έννοιας της αυτόματης διαπραγμάτευσης πληρωμής, όπου οι υπολογιστές κάνουν τις διαπραγματεύσεις και οι χρήστες παίρνουν τις τελικές αποφάσεις. Τεχνικά, η JEPI προδιαγράφει ένα ζεύγος πρωτοκόλλων δια-πραγμάτευσης:

• Ένα *πρωτόκολλο διαπραγμάτευσης γενικού σκοπού*, που βασίζεται στο πρωτόκολλο επέκτασης πρωτοκόλλων Protocol Extension Protocol – PEP, το οποίο επεκτείνει το HTTP, έτσι ώστε να μπορεί δυναμικά να αναπτύσσει εφαρμογές που απαιτούν περισσότερες λειτουργίες απ' αυτές που μπορεί να υποστηρίξει το HTTP.

• Ένα συγκεκριμένο *υποσύστημα επέκτασης*, που ονομάζεται Universal Payment Preamble (UPP), και τοποθετείται πάνω από το PEP. Το UPP επιτρέπει στους πελάτες να χρησιμοποιήσουν ένα πορτοφόλι πολυ–πληρωμών και να μετακινούνται εύκολα από πληρωμή σε πληρωμή. Οι διαπραγματεύσεις UPP γίνονται μέσω ανταλλαγής επικεφαλίδων PEP, πριν ή κατά τη διάρκεια των αγορών, και μπορούν να χρησιμοποιηθούν για να συμφωνηθεί η μέθοδος πληρωμής, το πρωτόκολλο και κάποιες άλλες παράμετροι, όπως, για παράδειγμα, ο τύπος της πιστωτικής κάρτας (Visa, Diners, Mastercard, Amex κτλ.) στην περίπτωση πληρωμής με πιστωτική κάρτα.

4.3 Ηλεκτρονικό χρήμα

Το ***ψηφιακό*** ή ***ηλεκτρονικό χρήμα*** είναι το ηλεκτρονικό ανάλογο του φυσικού χρήματος. Εκδίδεται από τράπεζες και οι πελάτες μπορούν να το χρησιμοποιήσουν για να αγοράσουν αγαθά ή υπηρεσίες από εμπόρους που αποδέχονται αυτήν τη μορφή ηλεκτρονικής πληρωμής. Τρία μέρη εμπλέκονται σε ένα σύστημα ηλεκτρονικού χρήματος:

• Μια *Τράπεζα*, που εκδίδει το ηλεκτρονικό χρήμα
• Ένας *Πελάτης*
• Ένας *Έμπορος*

Ο Πελάτης και ο Έμπορος μπορεί να έχουν λογαριασμούς και σε άλλες τράπεζες. Στηνπερίπτωση αυτή, οι τράπεζες αυτές αναφέρονται ως *Τράπεζα Πελάτη* και *Τράπεζα Εμπόρου*, αντίστοιχα.

Μια συναλλαγή ηλεκτρονικού χρήματος ολοκληρώνεται σε τρεις διακριτές και ανεξάρτητες φάσεις, οι οποίες φαίνονται σχηματικά στο Σχήμα 4.2:

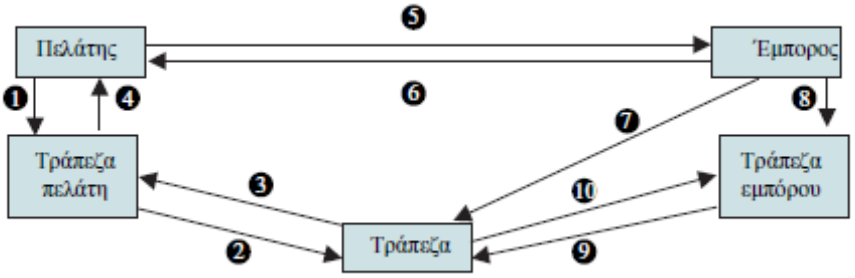
• Στην πρώτη φάση, ο Πελάτης **αποκτάει** ηλεκτρονικό χρήμα. Ζητάει από την Τράπεζα Πελάτη να μεταφέρει χρήματα από το λογαριασμό του στην Τράπεζα (Βήμα 1). Μετά τη μεταφορά αυτή (Βήματα 2 και 3), η Τράπεζα Πελάτη στέλνει το αντίστοιχο ποσό ηλεκτρονικού χρήματος στον Πελάτη (Βήμα 4) και αυτός αποθηκεύει το ηλεκτρονικό χρήμα τοπικά στο δίσκο του ή στην έξυπνη κάρτα του.

• Στη δεύτερη φάση, ο Πελάτης **χρησιμοποιεί** το ηλεκτρονικό χρήμα για να κάνει κάποιες αγορές. Ειδικότερα, επιλέγει αγαθά ή υπηρεσίες και μεταφέρει τα αντίστοιχα ποσά ηλεκτρονικού χρήματος στον Έμπορο (Βήμα 5). Ο Έμπορος, με τη σειρά του, προμηθεύει τα αγαθά ή τις υπηρεσίες στον Πελάτη (Βήμα 6).

• Στην τρίτη φάση, ο Έμπορος **εξαργυρώνει** το ηλεκτρονικό χρήμα που εισέπραξε από τον Πελάτη, μεταφέροντας το ηλεκτρονικό χρήμα στην Τράπεζα (Βήμα 7).

Εναλλακτικά, ο Έμπορος μπορεί να μεταφέρει το ηλεκτρονικό χρήμα στην Τράπεζα Εμπόρου (Βήμα 8) και αυτή, με τη σειρά της, να το εξαργυρώσει από την Τράπεζα (Βήμα 9). Στην περίπτωση αυτή η

Τράπεζα μεταφέρει χρήματα στην Τράπεζα Εμπόρου, προς πίστωση του λογαριασμού του Εμπόρου (Βήμα 10).



Είναι κοινά αποδεκτό ότι το ηλεκτρονικό χρήμα πρέπει να έχει ορισμένες ιδιότητες.

Για παράδειγμα, το ηλεκτρονικό χρήμα πρέπει να είναι **ανεξάρτητο**, με την έννοια ότι η ύπαρξή του δεν πρέπει να εξαρτάται από συγκεκριμένες πλατφόρμες ή συστήματα. Πιθανόν ένα από τα ξεχωριστά χαρακτηριστικά του πραγματικού χρήματος είναι η **ανωνυμία** του, με την έννοια ότι το χρήμα δεν πρέπει να παρέχει πληροφορίες που να επιτρέπουν την αναγνώριση των προηγούμενων ιδιοκτητών του. Είναι λογικό, λοιπόν, να απαιτούμε και από το ηλεκτρονικό χρήμα να έχει την ιδιότητα αυτή. Συνεπώς, το ηλεκτρονικό χρήμα πρέπει να μπορεί να μεταφέρεται από άτομο σε άτομο, και μάλιστα με τέτοιον τρόπο ώστε να μην είναι δυνατόν να ανακαλυφθεί ποιος το κατείχε προηγουμένως. Στην περίπτωση αυτή όμως πρέπει να είναι βέβαιο ότι κάθε ηλεκτρονικό νόμισμα **χρησιμοποιείται μόνο μία φορά** και ότι κάθε απόπειρα διπλής χρήσης είναι ανιχνεύσιμη. Επίσης, το ηλεκτρονικό χρήμα πρέπει να είναι **διαθέσιμο σε διάφορα ποσά** και να είναι **διαιρετό**, όπως και το πραγματικό.

Τέλος, το ηλεκτρονικό χρήμα πρέπει να είναι **δυνατόν να αποθηκευτεί με ασφάλεια** σε σκληρό δίσκο ή σε έξυπνη κάρτα. Μερικά μόνο από τα συστήματα ηλεκτρονικού χρήματος που προτάθηκαν στο παρελθόν ικανοποιούσαν όλες αυτές τις ιδιότητες. Για παράδειγμα, η ιδιότητα της ανωνυμίας αποτελεί ακόμη αντικείμενο συζήτησης, αφού η εκπλήρωσή της οδηγεί στη δυνατότητα ξεπλύματος παράνομου χρήματος ή στην απόκρυψη χρήματος που προήλθε από παράνομες ενέργειες. Η διαπίστωση αυτή οδήγησε στην ανάπτυξη **σχεδόν** ανώνυμων συστημάτων ηλεκτρονικού χρήματος, στα οποία η ταυτότητα του πελάτη είναι δυνατόν να αποκαλυφθεί, υπό συγκεκριμένους όρους.

4.4 Πληρωμές με πιστωτικές κάρτες

Τελευταία, τα ηλεκτρονικά συστήματα πληρωμής με πιστωτικές κάρτες κυριαρχούν ανάμεσα στους χρήστες του Internet. Υπάρχουν διάφορες απαιτήσεις ασφάλειας που αυτά τα συστήματα πρέπει να πληρούν. Για παράδειγμα, πρέπει να υπάρχει ένας μηχανισμός που θα **αυθεντικοποιεί** τα διάφορα εμπλεκόμενα μέρη, δηλαδή τους πελάτες, τους εμπόρους και τις συμμετέχουσες τράπεζες. Πρέπει, επίσης, να υπάρχει ένας άλλος μηχανισμός που θα **προστατεύει** τις πληροφορίες της κάρτας και της πληρωμής καθώς αυτές μεταδίδονται μέσω του Internet. Τέλος, πρέπει να συμφωνηθεί μια **διαδικασία επίλυσης διαφορών** μεταξύ των εμπλεκόμενων μερών.

Έχουν σχεδιαστεί αρκετά συστήματα ηλεκτρονικών πληρωμών με πιστωτικές κάρτες που αντιμετωπίζουν αυτές τις απαιτήσεις. Τα περισσότερα απ' αυτά έχουν και επιπλέον πλεονεκτήματα. Για παράδειγμα, σε κάποια απ' αυτά τα συστήματα οι πληροφορίες της πιστωτικής κάρτας δεν αποκαλύπτονται στον έμπορο.

Το χαρακτηριστικό αυτό δεν υπάρχει στα συμβατικά συστήματα πληρωμής με πιστωτικές κάρτες. Επομένως, ένα ηλεκτρονικό σύστημα πληρωμής με πιστωτικές κάρτες μπορεί να παρέχει μεγαλύτερη ασφάλεια απ' ό,τι το συμβατικό σύστημα. Επίσης, ένα ηλεκτρονικό σύστημα πληρωμής με πιστωτικές κάρτες μπορεί να σχεδιαστεί έτσι ώστε να κάνει σχεδόν άμεσα την πληρωμή στον έμπορο. Στο συμβατικό σύστημα απαιτείται αρκετός χρόνος μέχρι ο έμπορος να πάει τις αποδείξεις στην τράπεζα και η τράπεζα να εκκαθαρίσει το προς πληρωμή ποσό.

Πέντε οντότητες συμμετέχουν στα ηλεκτρονικά συστήματα πληρωμής με πιστωτικές κάρτες:

• Ο *Πελάτης* (κάτοχος της κάρτας)
• Ο *Έμπορος*
• Η *Τράπεζα Εμπόρου*
• Ένα *Κέντρο Διαχείρισης Πιστοποιητικών* (ΚΔΠ)
• Η *Τράπεζα που εκδίδει την κάρτα (Εκδότρια Τράπεζα)*

Ο Πελάτης χρησιμοποιεί την κάρτα του για να αγοράσει αγαθά ή υπηρεσίες από τον Έμπορο.

Ο Έμπορος συναλλάσσεται με την Τράπεζα Εμπόρου. Μια πολύ σημαντική οντότητα στα ηλεκτρονικά συστήματα πληρωμής με πιστωτικές κάρτες είναι το Κέντρο Διαχείρισης Πιστοποιητικών (ΚΔΠ), που παρέχει υπηρεσίες δημόσιου κλειδιού και εκδίδει πιστοποιητικά δημόσιου κλειδιού στα εμπλεκόμενα μέρη.

Επιπλέον, υπάρχουν συνήθως δύο δίκτυα που εμπλέκονται σε ένα ηλεκτρονικό σύστημα πληρωμής με πιστωτικές κάρτες: ένα ***δημόσιο δίκτυο*** (συνήθως το Internet) και ένα ***ιδιωτικό***, που ανήκει στις τράπεζες, οι οποίες και το διαχειρίζονται. Το δίκτυο αυτό αναφέρεται ως ***Banknet***. Η βασική υπόθεση είναι ότι οι επικοινωνίες μέσω του Banknet είναι αρκετά ασφαλείς, ενώ οι επικοινωνίες μέσω του Internet είναι εγγενώς ανασφαλείς και πρέπει να προστατευτούν κρυπτογραφικά. Συνεπώς, ένα πρωτόκολλο ηλεκτρονικού συστήματος πληρωμής με πιστωτικές κάρτες κυρίως εστιάζει στις επικοινωνίες που γίνονται μέσω του Internet και δεν ασχολείται με επικοινωνίες μέσω του Banknet.

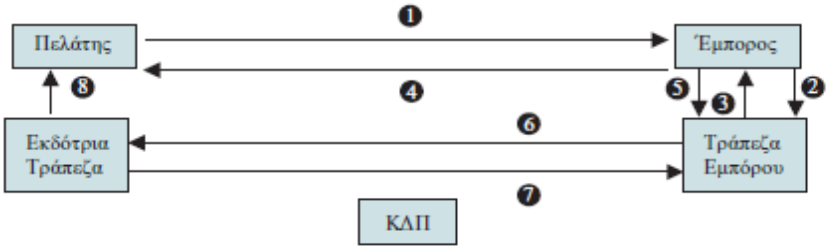
Μια ηλεκτρονική συναλλαγή πληρωμής με πιστωτική κάρτα εκτελείται σε τρεις κύριες φάσεις, που φαίνονται σχηματικά στο Σχήμα 4.4:

• Στην πρώτη φάση, ο Πελάτης **εξετάζει** τι προσφέρει ο Έμπορος και **αγοράζει** κάποια αγαθά ή υπηρεσίες (Βήμα 1). Δηλώνει ότι προτίθεται να πληρώσει με πιστωτική κάρτα και ο Έμπορος επικοινωνεί με την Τράπεζά του προκειμένου να πάρει την εξουσιοδότηση πίστωσης για τον Πελάτη και το ποσό που αντιστοιχεί στην αγορά (Βήματα 2 και 3).

Γενικά, η εξουσιοδότηση αυτή απαιτείται μόνο όταν το ποσό της αγοράς υπερβαίνει κάποιο προκαθορισμένο όριο. Στην περίπτωση αυτή η Τράπεζα Εμπόρου ολοκληρώνει την εξουσιοδότηση και ενημερώνει τον Έμπορο αν πρέπει να προχωρήσει ή όχι. Τέλος, ο Έμπορος ειδοποιεί τον Πελάτη ότι η συναλλαγή έκλεισε (Βήμα 4).

• Στη δεύτερη φάση, ο Έμπορος **επικοινωνεί** με την Τράπεζά του και της δίνει όσες αποδείξεις ηλεκτρονικών πληρωμών με πιστωτικές κάρτες έχει συγκεντρώσει (Βήμα 5). Η Τράπεζα Εμπόρου επικοινωνεί με την Εκδότρια Τράπεζα ώστε να λάβει τα χρήματα για λογαριασμό του Εμπόρου (Βήματα 6 και 7).

• Στην τρίτη φάση, η Εκδότρια Τράπεζα **ενημερώνει** τον Πελάτη για το ποσό των χρημάτων που μεταφέρθηκαν σε άλλα μέρη ως αποτέλεσμα των αγορών του (Βήμα 8). Ο Πελάτης μπορεί να ενημερώνεται μια φορά το μήνα με κανονικό ή (ασφαλές) ηλεκτρονικό ταχυδρομείο.



Κεφάλαιο 5ο

Τεχνολογία Έξυπνων Καρτών

5.1 Τι Είναι η Έξυπνη Κάρτα

Μια έξυπνη κάρτα είναι μια πλαστική κάρτα με ενσωματωμένο τσιπ μικροεπεξεργαστών. Η κάρτα μοιάζει με μια κανονική πιστωτική κάρτα εκτός από την μεταλλική επαφή της (στην κάρτα επαφών μόνο), αλλά οι εφαρμογές που διενεργούνται θα μπορούσαν συνολικά, να είναι διαφορετικές. Εκτός από τις κανονικές λειτουργίες των πιστωτικών και

bank καρτών, μια έξυπνη κάρτα θα μπορούσε να ενεργήσει ως ηλεκτρονικό πορτοφόλι όπου τα ηλεκτρονικά μετρητά κρατιούνται. Με το κατάλληλο λογισμικό, θα μπορούσε επίσης να χρησιμοποιηθεί ως ασφαλής έλεγχος πρόσβασης.

Ο όρος "έξυπνη κάρτα" έχει διαφορετικές έννοιες σε κάποια βιβλία [Guthery1998, Rankl1997] επειδή οι έξυπνες κάρτες έχουν χρησιμοποιηθεί σε διαφορετικές εφαρμογές.

Στο άρθρο "Smart cards: A primer "[DiGiorgio1997a], η έξυπνη κάρτα ορίζεται ως μια" πιστωτική κάρτα "με έναν" εγκέφαλο " πάνω της, ο οποίος είναι ένα μικρό ενσωματωμένο τσιπ υπολογιστών. Λόγω αυτού του "ενσωματωμένου εγκεφάλου", η έξυπνη κάρτα είναι επίσης γνωστή ως τσιπ ή κάρτα ολοκληρωμένων κυκλωμάτων (IC). Μερικοί τύποι έξυπνων καρτών μπορούν να ενσωματώσουν έναν μικροεπεξεργαστή, ενώ άλλοι μπορούν να περιέχουν μόνο περιεχόμενο μη-μετάβλητης μνήμης. Γενικά, μια πλαστική κάρτα με ένα ενσωματωμένο τσιπ εσωτερικά μπορεί να θεωρηθεί ως έξυπνη κάρτα.

Σε καθέναν τύπο έξυπνης κάρτας, η ικανότητα αποθήκευσης του περιεχομένου μνήμης της είναι πολύ μεγαλύτερη από αυτή των μαγνητικών καρτών λωρίδων. Η συνολική ικανότητα αποθήκευσης μιας μαγνητικής κάρτας λωρίδων είναι 125 ψηφιολέξεις ενώ η χαρακτηριστική ικανότητα αποθήκευσης μιας έξυπνης κάρτας κυμαίνεται από 1K ως 64K ψηφιολέξεων. Με άλλα λόγια, το περιεχόμενο μνήμης μιας έξυπνης κάρτας μεγάλης περιεκτικότητας μπορεί να κρατήσει τα δεδομένα περισσότερων από 500 μαγνητικών καρτών λωρίδων.

Προφανώς, η μεγάλη ικανότητα αποθήκευσης είναι ένα από τα πλεονεκτήματα της έξυπνης κάρτας, αλλά το πιο σημαντικό χαρακτηριστικό γνώρισμα της έξυπνης κάρτας απ' όλα, είναι το γεγονός ότι τα αποθηκευμένα δεδομένα τους μπορούν να προστατευθούν από μη εξουσιοδοτημένη πρόσβαση και να επέμβει. Μέσα σε μια έξυπνη κάρτα, η πρόσβαση στο περιεχόμενο μνήμης ελέγχεται από ένα ασφαλές logic system μέσα στο τσιπ. Δεδομένου ότι η πρόσβαση στα δεδομένα μπορεί να εκτελεσθεί μόνο μέσω μιας τμηματικής διεπαφής που εποπτεύεται από

το λειτουργικό σύστημα και το ασφαλές logic system, το εμπιστευτικό στοιχείο που γράφεται επάνω στην κάρτα προστατεύεται από μη εξουσιοδοτημένη εξωτερική πρόσβαση. Αυτό το μυστικό στοιχείο μπορεί μόνο να υποβληθεί σε επεξεργασία εσωτερικά από το μικροεπεξεργαστή.

Λόγω του υψηλού επιπέδου ασφάλειας έξυπνων καρτών και της off-line φύσης τους, είναι εξαιρετικά δύσκολο να προσβληθεί από hacker η αξία μιας κάρτας, ή ειδάλλως να τεθούν μη εξουσιοδοτημένες πληροφορίες στην κάρτα. Επειδή είναι δύσκολο να ανακτηθούν δεδομένα χωρίς έγκριση, μια έξυπνη κάρτα είναι μοναδικά κατάλληλη για την ασφαλή και κατάλληλη αποθήκευση δεδομένων. Χωρίς άδεια του κατόχου καρτών, τα στοιχεία δεν θα μπορούσαν να ληφθούν ή να τροποποιηθούν. Επομένως, η έξυπνη κάρτα θα μπορούσε περαιτέρω να ενισχύσει την ιδιωτικότητα στοιχείων του χρήστη.

Επομένως, η έξυπνη κάρτα είναι όχι μόνο μία "αποθήκη" στοιχείων, αλλά και μια προγραμματίσημη, φορητή, ανθεκτική στην πλαστογράφηση μνήμη αποθηκευμένων δεδομένων. Η Microsoft θεωρεί την έξυπνη κάρτα ως επέκταση ενός προσωπικού υπολογιστή και του βασικού συστατικού της υποδομής δημοσίου-κλειδιού στα Windows 98 και το 2000 της Microsoft (προηγούμενος γνωστά ως WINDOWS NT 5.0) [Microsoft1997a].

5.1.2 Ιστορίας της Ανάπτυξης της Έξυπνης Κάρτας

Μια κάρτα που ενσωματώθηκε με έναν μικροεπεξεργαστή εφευρέθηκε αρχικά από δύο Γερμανούς μηχανικούς το 1967. Δεν κοινοποιήθηκε μέχρι ο Roland Moreno, ένας Γάλλος δημοσιογράφος, ανήγγειλε το δίπλωμα ευρεσιτεχνίας Έξυπνης Κάρτας στη Γαλλία το 1974 [Rankl1997]. Με τις προόδους στην τεχνολογία κατασκευής μικροεπεξεργαστών, το κόστος ανάπτυξης της έξυπνης κάρτας έχει μειωθεί πολύ. Το 1984, μια σημαντική ανακάλυψη επιτεύχθηκε όταν πραγματοποίησαν επιτυχώς οι γαλλικές ταχυδρομικές και

τηλεπικοινωνιακές υπηρεσίες (PTT) μια υπαίθρια δοκιμή με τις τηλεφωνικές κάρτες. Από τότε, οι έξυπνες κάρτες δεν είναι πλέον "δεμένες" με την παραδοσιακή αγορά bank καρτών, ακόμα κι αν η αγορά τηλεφωνικών καρτών είναι ακόμα η μεγαλύτερη αγορά των έξυπνων καρτών το 1997.

Λόγω της καθιέρωσης της προδιαγραφής ISO- 7816 το 1987 (ένα παγκόσμιο πρότυπο διεπαφής έξυπνων καρτών), το format των έξυπνων καρτών είναι τώρα τυποποιημένο. Σήμερα, οι έξυπνες κάρτες από διαφορετικούς προμηθευτές θα μπορούσαν να επικοινωνήσουν με τη host μηχανή χρησιμοποιώντας μία κοινή γλώσσα.

5.2 Διαφορετικοί Τύποι Έξυπνων Καρτών

Σύμφωνα με τους ορισμούς της "έξυπνης κάρτας" στην τεχνολογία των έξυπνων καρτών, βάση της λίστας των πιο συχνών ερωτήσεων [Priisalu1995], η λέξη "έξυπνη κάρτα" έχει τρεις διαφορετικές έννοιες:

- κάρτα ολοκληρωμένου κυκλώματος με τη διεπαφή ISO 7816
- κάρτα ολοκληρωμένου κυκλώματος επεξεργαστών
- προσωπική ταυτότητα που περιέχει ICs

Βασικά, βασισμένος στα φυσικά χαρακτηριστικά τους, οι κάρτες ολοκληρωμένου κυκλώματος μπορούν να ταξινομηθούν σε 4 κύριους τύπους, την κάρτα μνήμης, την contact CPU κάρτα, την κάρτα contactless και την κάρτα combi.

5.2.1 Κάρτες Μνήμης

Μια κάρτα μνήμης είναι μια κάρτα με μνήμη και λογική πρόσβασης μόνο onboard. Παρόμοια στις μαγνητικές κάρτες λωρίδων, μια κάρτα

μνήμης μπορεί μόνο να χρησιμοποιηθεί για την αποθήκευση στοιχείων. Καμία ικανότητα επεξεργασίας δεδομένων δεν πρέπει να αναμένεται. Χωρίς την on-board CPU, οι κάρτες μνήμης χρησιμοποιούν έναν σύγχρονο μηχανισμό επικοινωνίας μεταξύ του αναγνώστη και της κάρτας, όπου το κανάλι επικοινωνίας είναι πάντα υπό άμεσο έλεγχο του αναγνώστη των καρτών. Τα δεδομένα που αποθηκεύονται στην κάρτα μπορούν να ανακτηθούν με μια κατάλληλη εντολή στην κάρτα.

Στις παραδοσιακές κάρτες μνήμης, καμία λογική ελέγχου ασφάλειας δεν συμπεριλαμβάνεται. Επομένως, η μη εξουσιοδοτημένη πρόσβαση στο περιεχόμενο μνήμης της κάρτας δεν θα μπορούσε να αποτραπεί.

Ενώ στις πρόσφατες κάρτες μνήμης, με την ασφάλεια της λογικής ελέγχου που προγραμματίζεται στην κάρτα, η πρόσβαση στη ζώνη προστασίας περιορίζεται μόνο στους χρήστες με τον κατάλληλο κωδικό πρόσβασης.

5.2.2 Contact CPU Κάρτες

Μια περιπλοκότερη έκδοση της έξυπνης κάρτας είναι η κάρτα contact CPU. Ένας μικροεπεξεργαστής ενσωματώνεται στην κάρτα. Με αυτόν τον πραγματικό "εγκέφαλο", το πρόγραμμα που αποθηκεύεται μέσα στο τσιπ μπορεί να εκτελεσθεί. Μέσα στο ίδιο τσιπ, υπάρχουν τέσσερις άλλοι λειτουργικοί φραγμοί: η μάσκα-ROM, η αμετάβλητη μνήμη, η RAM και η I/O θύρα [HKSAR1997, Rankl1997].

Εκτός από τη μονάδα μικροεπεξεργαστών, μια κάρτα μνήμης περιέχει σχεδόν όλα τα συστατικά που συμπεριλαμβάνονται σε μια κάρτα επικοινωνίας CPU. Και οι δύο αποτελούνται από την αμετάβλητη μνήμη, τη RAM, τη ROM και την I/O μονάδα. Βασιζόμενη στις προδιαγραφές του ISO 7816 , η εξωτερική εμφάνιση αυτών των έξυπνων καρτών επικοινωνίας είναι ακριβώς η ίδια. Η μόνη διαφορά είναι η ύπαρξη της CPU και η χρήση της ROM. Στην κάρτα CPU, η ROM είναι καλυμμένη με το λειτουργικό σύστημα του τσιπ που εκτελεί τις εντολές που εκδίδονται από το τερματικό, και επιστρέφει τα αντίστοιχα

αποτελέσματα. Οι κώδικες εφαρμογής του προγράμματος και τα δεδομένα, αποθηκεύονται στην αμετάβλητη μνήμη, συνήθως EEPROM, το οποίο θα μπορούσε να τροποποιηθεί μετά από το στάδιο κατασκευής καρτών.

Ένα από τα κύρια χαρακτηριστικά γνωρίσματα μιας contact CPU κάρτας είναι η ασφάλεια. Στην πραγματικότητα, η contact CPU κάρτα έχει υιοθετηθεί κυρίως για την ασφαλή συναλλαγή στοιχείων.

Εάν ένας χρήστης δεν θα μπορούσε να επικυρώσει επιτυχώς τον εαυτό του/της στην CPU, τα δεδομένα που κρατήθηκαν στην κάρτα δεν θα μπορούσαν να ανακτηθούν. Επομένως, ακόμα και όταν χάνεται μια έξυπνη κάρτα, τα δεδομένα που αποθηκεύονται μέσα στην κάρτα δεν θα εκτεθούν εάν αυτά αποθηκευτούν κατάλληλα [Rankl1997]. Επίσης, ως ασφαλής φορητός υπολογιστής, μια κάρτα CPU μπορεί να επεξεργαστεί οποιαδήποτε εσωτερικά δεδομένα με ασφάλεια και να εξάγει το υπολογισμένο αποτέλεσμα στο τερματικό.

5.2.3 Contactless Κάρτες

Ακόμα κι αν η έξυπνη κάρτα contact CPU είναι ασφαλέστερη από την κάρτα μνήμης, μπορεί να μην είναι κατάλληλη για όλα τα είδη εφαρμογών, ειδικά όπου οι ογκώδεις συναλλαγές περιλαμβάνονται, όπως οι χρήσεις μεταφορών. Επειδή για χρήσεις δημόσιων μεταφορών , τα προσωπικά στοιχεία πρέπει να ληφθούν από τον αναγνώστη εντός μιας μικρής χρονικής περιόδου, η έξυπνη κάρτα contact CPU που απαιτεί ο χρήστης να παρεμβάλει την κάρτα στον αναγνώστη προτού να μπορέσουν τα στοιχεία να ληφθούν από την κάρτα, δεν θα ήταν μια κατάλληλη επιλογή. Με τη χρήση της ραδιοσυχνότητας, η έξυπνη κάρτα χωρίς επικοινωνία μπορεί να μεταδώσει τα στοιχεία χρηστών από αρκετά μεγάλη απόσταση εντός μιας μικρής χρονικής περιόδου ενεργοποίησης. Ο κάτοχος καρτών δεν θα έπρεπε να παρεμβάλει την κάρτα στον αναγνώστη. Ολόκληρη η διαδικασία συναλλαγής θα μπορούσε να εκτελεσθεί χωρίς αφαίρεση της κάρτας από το πορτοφόλι του χρήστη.

Οι έξυπνες κάρτες contactless χρησιμοποιούν μια τεχνολογία που επιτρέπει στους αναγνώστες καρτών να διασφαλίσουν την ενέργεια για τις συναλλαγές και τις επικοινωνίες χωρίς παραγωγή της φυσικής επαφής με τις κάρτες. Συνήθως το ηλεκτρομαγνητικό σήμα χρησιμοποιείται για την επικοινωνία μεταξύ της κάρτας και του αναγνώστη. Η απαραίτητη ισχύς για να "τρέξει" το τσιπ στην κάρτα θα μπορούσε είτε να παρασχεθεί από την μπαταρία που ενσωματώθηκε στην κάρτα είτε που διαβιβάστηκε στις συχνότητες μικροκυμάτων από τον αναγνώστη επάνω στην κάρτα.

Η contactless κάρτα είναι ιδιαίτερα κατάλληλη για μεγάλη ποσότητα πρόσβασης καρτών και συναλλαγής στοιχείων. Εντούτοις, η contactless έξυπνη κάρτα δεν έχει τυποποιηθεί. Υπάρχουν περίπου 16 διαφορετικές τεχνολογίες contactless καρτών και τύποι καρτών στην αγορά [ADE]. Κάθε μια από αυτές τις κάρτες έχει τα πλεονεκτήματά της, αλλά μπορεί να μην είναι συμβατές η μία με τον άλλη. Εντούτοις, λόγω του υψηλού κόστους παραγωγής και της τεχνολογίας που είναι σχετικά νέα, αυτός ο τύπος καρτών δεν έχει υιοθετηθεί ευρέως.

5.2.4 Κάρτες Combi

Στο τρέχον στάδιο, η contact και contactless έξυπνες κάρτες χρησιμοποιούν δύο διαφορετικά πρωτόκολλα επικοινωνίας και διαδικασίες ανάπτυξης. Και οι δύο κάρτες έχουν τα πλεονεκτήματα και τα μειονεκτήματά τους. Οι έξυπνες κάρτες contact έχουν το πιό υψηλό επίπεδο ασφάλειας και readily-available υποδομής, ενώ οι contactless έξυπνες κάρτες παρέχουν ένα αποδοτικότερο και κατάλληλο περιβάλλον συναλλαγής. Προκειμένου να παρασχεθούν στους πελάτες τα πλεονεκτήματα αυτών των δύο καρτών, δύο μέθοδοι θα μπορούσαν να υιοθετηθούν. Η πρώτη μέθοδος είναι να φτιαχτεί ένας υβριδικός αναγνώστης καρτών, ο οποίος θα μπορούσε να καταλάβει τα πρωτόκολλα και των δύο τύπων καρτών. Η δεύτερη μέθοδος είναι να δημιουργηθεί μια κάρτα που συνδυάζει τις λειτουργίες contact με τις

contactless λειτουργίες. Επειδή το κόστος παραγωγής του υβριδικού αναγνώστη είναι πολύ ακριβό, η τελευταία λύση επιλέγεται συνήθως.

Μερικές φορές, ο όρος "κάρτα combi" χρησιμοποιείται με λάθος τρόπο από τους κατασκευαστές. Γενικά, υπάρχουν δύο τύποι που συνδυάζουν τις contact-contactless έξυπνες κάρτες, η υβριδική κάρτα και η κάρτα combi. Και οι δύο κάρτες ενσωματώνουν τα contact και contactless μέρη, μαζί στην πλαστική κάρτα. Εντούτοις, στην υβριδική κάρτα, το τσιπ ολοκληρωμένου κυκλώματος contact και το contactless τσιπ είναι χωριστές ενότητες. Καμία ηλεκτρική σύνδεση δεν έχει περιληφθεί για την επικοινωνία μεταξύ των δύο τσιπ. Αυτές οι δύο ενότητες μπορούν να θεωρηθούν ως χωριστές αλλά συνυπάρχουν στην ίδια κάρτα. Ενώ στην κάρτα combi, τα contact και τα contactless τσιπ θα μπορούσαν να επικοινωνήσουν μεταξύ τους, δίνοντας κατά συνέπεια στην κάρτα combi την ικανότητα να "μιλήσει" με το εξωτερικό περιβάλλον μέσω είτε της contact είτε της contactless μεθόδου.

Δεδομένου ότι η κάρτα combi κατέχει τα πλεονεκτήματα και των contact και των contactless καρτών, ο μόνος λόγος που εμποδίζει την αποδοχή του, είναι το κόστος. Όταν το κόστος και τα τεχνικά εμπόδια θα υπερνικηθούν, οι κάρτες combi θα γίνουν μια δημοφιλής λύση έξυπνων καρτών.

5.3 Διάφορα Πρότυπα για τις Έξυπνες Κάρτες

Σε όλη την ιστορία της ανάπτυξης έξυπνων καρτών, έχουν καθιερωθεί διάφορα πρότυπα για την επίλυση του προβλήματος της διαλειτουργικότητας. Το πρώτο -πρώτο πρότυπο είναι το ISO 7816 πρότυπο έξυπνων καρτών, που δημοσιεύεται από τον Διεθνή Οργανισμό για την Τυποποίηση (ISO) το 1987. Πριν από αυτό, οι προμηθευτές και οι κατασκευαστές καρτών ανέπτυξαν τις δικές τους ιδιόκτητες κάρτες και τους αναγνώστες τους που δεν μπορούσαν να επικοινωνήσουν. Με το πρότυπο του ISO, οι έξυπνες κάρτες θα μπορούσαν να επικοινωνήσουν

χρησιμοποιώντας το ίδιο πρωτόκολλο. Η φυσική εμφάνιση και οι διαστάσεις μιας κάρτας καθορίζονται επίσης. Η έννοια και η θέση των επαφών, τα πρωτόκολλα και τα περιεχόμενα των υψηλών και χαμηλών μηνυμάτων που ανταλλάσσονται με την κάρτα ολοκληρωμένου κυκλώματος είναι όλα τυποποιημένα. Αυτό εξασφαλίζει ότι η κάρτα που κατασκευάζεται και που εκδίδεται από μια επιχείρηση μπορεί να γίνει αποδεκτή από μια συσκευή άλλης επιχείρησης.

Δύο άλλα σημαντικά πρότυπα σε αυτόν τον τομέα είναι τα EMV (Europay, mastercard και Visa) και GSM (σφαιρικά πρότυπα για την κινητή επικοινωνία). Το πρότυπο EMV είναι για τη χρέωση/τις πιστωτικές κάρτες όπου σημαντικοί διεθνής χρηματοδοτικοί οργανισμοί όπως οι Visa, mastercard και Europay περιλαμβάνονται. Άρχισε το 1993 και οριστικοποιήθηκε το 1996 [HKSAR1997]. Αυτό το πρότυπο καλύπτουν το ηλεκτρομηχανικό κομμάτι, το πρωτόκολλο, τα στοιχεία δεδομένων και τα μέρη οδηγιών μαζί με τις συναλλαγές που περιλαμβάνουν τις έξυπνες κάρτες bank μικροεπεξεργαστών. Ο στόχος της προδιαγραφής EMV για τα συστήματα πληρωμής, είναι να μοιραστεί ένα κοινό Σημείο του Τερματικού Πωλήσεων (Point of Sales (POS)), όπως κάνουν για τις μαγνητικές εφαρμογές λωρίδων. Επειδή η τραπεζική κάρτα που βασίζεται στην κάρτα μαγνητικής λωρίδας θα αντικατασταθεί σύντομα από την έξυπνη κάρτα, αυτό το πρότυπο πρέπει να καθιερωθεί για να εξασφαλιστεί ότι η νέα έξυπνη κάρτα που βασίζεται στην bank κάρτα θα είναι συμβατή με το σύστημα συναλλαγής τραπεζών. Με βάση αυτήν την προδιαγραφή, όλες οι bank-related λύσεις έξυπνων καρτών θα ήταν συμβατές η μία με την άλλη καθώς επίσης και με την προηγούμενη μαγνητική λύση καρτών λωρίδων. Οι τελικοί κατασκευαστές θα μπορούσαν να αναπτύξουν και να τροποποιήσουν τα σύνολα του API τους στα πρότυπα EMV για τα τερματικά τους, έτσι ώστα αυτά τα τερματικά να μπορούσαν να χρησιμοποιηθούν σε διαφορετικά συστήματα πληρωμής. Η πίστωση, η χρέωση, το ηλεκτρονικό πορτοφόλι και οι λειτουργίες "πίστης", θα μπορούσαν να υποβληθούν σε επεξεργασία σε αυτά τα EMV-compliant τερματικά. Με την ευελιξία που παρέχεται από το πρότυπο EMV, οι τράπεζες έχουν την άδεια για να

προσθέσουν τις επιλογές και τις ειδικές απαιτήσεις τους στο σύστημα πληρωμής των έξυπνων καρτών.

Το πρότυπο GSM είναι μια από τα σημαντικότερα πρότυπα για την έξυπνη κάρτα και τα ψηφιακά κινητά τηλεπικοινωνιών. Η προδιαγραφή GSM άρχισε το 1982 κάτω από το CEPT (Conference Europeenne des Postes et Telecommunications) και συνεχίστηκε αργότερα από το ETSI (European Telecommunications Standards Institute-Ευρωπαϊκό Ίδρυμα Προτύπων Τηλεπικοινωνιών). Αρχικά, αυτή η προδιαγραφή υποδεικνύεται για το κινητό τηλεφωνικό δίκτυο. Εντούτοις, όταν χρησιμοποιείται η έξυπνη κάρτα πρότυπα στο κινητό τηλεφωνικό σύστημα ως Subscriber Identification Module-Ενότητα Προσδιορισμού Συνδρομητών (SIM), τα μέρη της προδιαγραφής GSM γίνονται και πρότυπο των έξυπνων καρτών. Αυτό το μέρος της προδιαγραφής GSM άρχισε τον Ιανουάριο του 1988 από την Ομάδα Εμπειρογνωμόνων Ενότητας Προσδιορισμού Συνδρομητών-Subscriber Identification Module Expert Group (SIMEG).

Μέσα σε ένα δίκτυο GSM, σε όλους τους συνδρομητές GSM θα εκδίδονταν μια κάρτα SIM που μπορεί να αντιμετωπισθεί ως κλειδί του συνδρομητή στο δίκτυο. Το μέγεθος μιας κάρτας SIM καθορίζεται να είναι είτε μέγεθος της κανονικής πιστωτικής κάρτας, είτε στο μέγεθος των μίνι καρτών. Επειδή αυτή η κάρτα χρησιμοποιείται για το χειρισμό των λειτουργιών δικτύων GSM, ένας μικροελεγκτής κατά προτίμηση υψηλής απόδοσης (ένας δεκαεξάμπιτος μικροεπεξεργαστής) χρησιμοποιείται και η μνήμη EEPROM αφιερώνεται για την αποθήκευση των στοιχείων εφαρμογής, συμπεριλαμβανομένων των παραμέτρων δικτύων και των στοιχείων συνδρομητών.

Η προδιαγραφή GSM διαιρείται σε δύο τμήματα. Το πρώτο τμήμα περιγράφει τα γενικά λειτουργικά χαρακτηριστικά, ενώ το δεύτερο τμήμα εξετάζει την περιγραφή διεπαφών και τις λογικές δομές μιας κάρτας SIM. Οι λεπτομέρειες αυτής της προδιαγραφής δίνονται μέσα [Scourias].

Προτού να μπορέσει η έξυπνη κάρτα να υιοθετηθεί ευρέως από την αγορά, ένα ή περισσότερα τυποποιημένα περιβάλλοντα ανάπτυξης

καρτών απαιτούνται. Αυτήν την περίοδο, τέσσερα σημαντικά πρότυπα έξυπνων καρτών έχουν καθιερωθεί στην βιομηχανία έξυπνων καρτών, τα οποία είναι: το PC/SC, το πλαίσιο OpenCard, JavaCard και MULTOS και όλα τους είναι συμβατά με το πρότυπο του ISO έξυπνων καρτών.

5.4 Πρόσφατες Εφαρμογές των Έξυπνων Καρτών

Εισαγωγικές Παρατηρήσεις

Με τη γρήγορη επέκταση της τεχνολογίας Διαδικτύου και του ηλεκτρονικού εμπορίου, οι έξυπνες κάρτες τώρα γίνονται αποδεκτές ευρύτερα στην εμπορική αγορά ως stored-value και εξασφαλίζουν τις κάρτες αποθήκευσης. Επιπλέον, επίσης έχει χρησιμοποιηθεί ευρέως ως κάρτα ταυτότητας. Παραδείγματος χάριν, στην πόλη University του Χονγκ Κονγκ, ο παλιές σπουδαστικές/ προσωπικού κάρτες έχουν αντικατασταθεί από τις hybrid-card based κάρτες ταυτότητας. Αυτή η κάρτα ταυτότητας μπορεί να χρησιμοποιηθεί για τον κανονικό έλεγχο πρόσβασης καθώς επίσης και την ηλεκτρονική πληρωμή.

Η έξυπνη κάρτα έχει χρησιμοποιηθεί επίσης στη μεταφορά όπως η κάρτα Octopus που έχει υιοθετηθεί από το MTRC και το KCRC για να αντικαταστήσει της παλαιάς κάρτας λωρίδων Magnetic. Το ιατρικό αρχείο μπορεί επίσης να αποθηκευτεί στην έξυπνη κάρτα. Αυτό επιτρέπει στις κρίσιμες πληροφορίες του ασθενή, να ανακτούνται όποτε απαιτείται. Με τη βοήθεια της τεχνολογίας έξυπνων καρτών, πολλοί εξασφαλίζουν δεδομένα όπως το όνομα σύνδεσης υπολογιστών και ο κωδικός πρόσβασης ο οποίος μπορεί επίσης να κρατηθεί και έτσι ο χρήστης δεν χρειάζεται να θυμηθεί έναν μεγάλο αριθμό κωδικών πρόσβασης.

5.4.1 Ηλεκτρονικό Πορτοφόλι

Το Electronic Purse-Ηλεκτρονικό Πορτοφόλι είναι επίσης γνωστό ως ηλεκτρονικά μετρητά. Τα Ταμεία μπορούν να φορτωθούν επάνω σε μια κάρτα για τη χρήση ως μετρητά. Τα ηλεκτρονικά μετρητά μπορούν να

χρησιμοποιηθούν για τις μικρές αγορές χωρίς απαραιτήτως να απαιτήσουν την έγκριση ενός PIN. Η κάρτα πιστώνεται από τον τραπεζικό λογαριασμό του κατόχου κάρτας ή με μερικούς άλλους τρόπους. Όταν χρησιμοποιείται για να αγοράσει τα αγαθά ή τις υπηρεσίες, η ηλεκτρονική αξία αφαιρείται από την κάρτα και μεταφέρεται στον λογαριασμό του λιανοπωλητή. Παρόμοια με ένα πραγματικό πορτοφόλι, ο κάτοχος κάρτας θα μπορούσε να πιστώσει την κάρτα του/της στην τράπεζα οποτεδήποτε σε περίπτωση ανάγκης.

Οι ηλεκτρονικές συναλλαγές μετρητών δεν απαιτούν συνήθως τη χρήση ενός PIN. Αυτό επιταχύνει τις συναλλαγές, αλλά τα ηλεκτρονικά μετρητά στην κάρτα είναι έπειτα ευπρόσβλητα όπως τα συμβατικά μετρητά. Τα ποσά, ευτυχώς, είναι συνήθως μικρά και έτσι οι απώλειες δεν είναι σημαντικές. Η διαδεδομένη υιοθέτηση των ηλεκτρονικών μετρητών θα μειώσει τις δαπάνες στις τράπεζες και οι λιανοπωλητές θα χειρίζονται μεγάλες ποσοτήτες μετρητών.

Από το 1994, έχει υπάρξει σημαντική ανάπτυξη των ηλεκτρονικών εφαρμογών πορτοφολιών Intersector στην Ευρώπη που έχει επεκταθεί έξω από την Ευρώπη. Διάφορα σφαιρικά προγράμματα καρτών έχουν αναπτυχθεί για αυτόν το λόγο, όπως η κάρτα Proton από Banksys, VisaCash από την κάρτα Visa International και Mondex από mastercard [Bull1998]. Αυτά όλα έχουν υιοθετηθεί από τα καταστήματα σε όλο τον κόσμο.

5.4.2 Stored Value Κάρτες

Μια άλλη χρήση των έξυπνων καρτών στο ηλεκτρονικό εμπόριο είναι σημείο Electronic. Είναι ένα παράδειγμα της κάρτας stored-value. Η αρχή είναι ότι κάποια μνήμη στην έξυπνη κάρτα τίθεται κατά μέρος για να αποθηκεύσει τα ηλεκτρονικά σημεία ή τα ηλεκτρονικά εισιτήρια. Μια έξυπνη κάρτα μπορεί να αποθηκεύσει τα σημεία για τις διαφορετικές

υπηρεσίες και κάθε ένα από τα σημεία μπορεί να ξαναγεμιστεί, ανάλογα με τους τύπους των καρτών μνήμης. Αυτό επιτρέπει στο κόστος να κατανεμηθεί πέρα από έναν αριθμό υπηρεσιών και μια πολύ μακρύτερη διάρκεια ζωής.

Παραδείγματος χάριν, η κάρτα θα μπορούσε να χρησιμοποιηθεί για να πληρώσει το αέριο και αντί της τοποθέτησης των νομισμάτων σε έναν μετρητή χώρων στάθμευσης. Οι καταναλωτές "φορτώνουν" επάνω στην κάρτα από μια μηχανή πώλησης. Η κάρτα μπορεί έπειτα να χρησιμοποιηθεί για να ενεργοποιήσει τους μετρητές. Ένα πλεονέκτημα αυτού του συστήματος είναι ότι οι συλλογές των νομισμάτων δεν θα ήταν πλέον απαραίτητες. Αυτό θα μείωνε την υπερυψωμένη λειτουργία και θα απέβαλλε την κλοπή. Αυτό θα ωφελούσε επίσης τον καταναλωτή δεδομένου ότι τα σημεία μπόρεσαν να αγοραστούν και να αποθηκευτούν στην κάρτα εκ των προτέρων και έτσι δεν είναι απαραίτητο να διακομιστούν πολλά βαριά νομίσματα γύρω. Είναι επίσης δυνατό, η κάρτα να μπορούσε να ελέγξει τον τρόπο χρήσης της και να επιστρέψει τις πληροφορίες στον έμπορο καθώς επίσης και τον καταναλωτή, ώστε θα μπορούσε να παραχθεί το καλύτερο πρότυπο αγορών [McCrindle1990].

5.5 Εφαρμογές στην Ασφάλεια και την Πιστοποίηση

5.5.1 Κρυπτογραφική Χρήση

Από την άποψη του προμηθευτή και του χειριστή συστημάτων, η κύρια απαίτηση σχεδόν όλων των αναγνώσιμων από συστημάτων machine-readable καρτών, είναι να εξασφαλιστεί ότι η κάρτα που παρουσιάζεται ισχύει και ο κάτοχος κάρτας είναι πράγματι το πρόσωπο που έχει το δικαίωμα για να χρησιμοποιήσει εκείνη την ιδιαίτερη κάρτα. Για να

ελέγξουν την ταυτότητα του κατόχου κάρτας, οι χρήστες πρέπει για να πληκτρολογήσουν τον κωδικό PIN τους (προσωπικός αριθμός αναγνώρισης). Αυτός ο κώδικας PIN κρατιέται στην κάρτα παρά στα τερματικά ή τις host μηχανές.

Οι διαδικασίες προσδιορισμού και επικύρωσης πραγματοποιούνται στο τερματικό καρτών. Ένα από τα προβλήματα είναι να εξασφαλιστεί ότι η κάρτα εφοδιάζει κάποιο είδος machine-readable κριτηρίου αυθεντικότητας. Αυτό μπορεί να λυθεί με την χρήση των κρυπτογραφημένων επικοινωνιών μεταξύ της κάρτας και του τερματικού. Είναι ευρέως γνωστό ότι η κρυπτογράφηση μπορεί να χρησιμοποιηθεί για να εξασφαλίσει μυστικότητα των μηνυμάτων που στέλνονται και επίσης για να επικυρώσει τα μηνύματα.

Προκειμένου να εκτελεσθεί η διαδικασία κρυπτογράφησης, οι κρυπτογραφικές έξυπνες κάρτες πρέπει να έχουν τις ακόλουθες ιδιότητες:

- οι κάρτες πρέπει να έχουν την ικανοποιητική υπολογιστική δύναμη να εκτελέσουν τους κρυπτογραφικούς αλγορίθμους.
- οι κρυπτογραφικοί αλγόριθμοι πρέπει να είναι θεωρητικά ασφαλείς. Αυτό σημαίνει ότι δεν είναι δυνατό να αντληθεί το μυστικό κλειδί από τα αντίστοιχα κείμενα.
- οι έξυπνες κάρτες πρέπει να είναι φυσικά ασφαλείς. Δεν πρέπει να είναι δυνατό να εξαχθεί το μυστικό κλειδί από τη μνήμη της κάρτας.

Υπό τον όρο, ότι αυτοί οι όροι ικανοποιούνται, και με τις προόδους στην τεχνολογία μικροελεγκτών καρτών, η βασισμένη σε μικροεπεξεργαστή έξυπνη κάρτα μπορεί να καταφέρει να συναντήσει το απαραίτητο επίπεδο ασφάλειας [Chaum1989].

Παραδείγματος χάριν, οι Verisign και Schlumberger έχουν αναπτύξει τη χρήση της έξυπνης κάρτας Cryptoflex για τη μεταφορά μιας Verisign

Class 1 ψηφιακής ταυτότητας [Verisign9701]. Η κάρτα Cryptoflex είναι η πρώτη κρυπτογραφική έξυπνη κάρτα στη βιομηχανία, η οποία σχεδιάζεται βασισμένη στις προδιαγραφές PC/SC. Αυτό επιτρέπει τη χρήση της έξυπνης κάρτας για τη φορητή πρόσβαση Διαδικτύου με Microsoft Internet Explorer 3.0 επί όλων των τόπων δεχόμενη Verisign Digital IDs.

Στο Μίτσιγκαν University, η κάρτα Cyberflex έχει χρησιμοποιηθεί για την αποθήκευση των κλειδιών Kerberos σε ένα ασφαλές πρόγραμμα σύνδεσης [Michigan9701].

5.5.2 Identity Κάρτα

Ο προσδιορισμός μίας οντότητας είναι μια από τις πιό σύνθετες διαδικασίες στον τομέα Information Technology. Απαιτεί και η ίδια η οντότητα να προσδιοριστεί από μόνη της και για το σύστημα, για να αναγνωρίσει ότι η εισερχόμενη σύνδεση παράγεται από έναν νομικό χρήστη. Το σύστημα δέχεται έπειτα την ευθύνη για όλες τις επόμενες ενέργειες, συνετά γνωρίζοντας ότι ο χρήστης έχει την έγκριση για να κάνει οτιδήποτε του ζητηθεί από το σύστημα.

Εάν μια έξυπνη κάρτα χρησιμοποιείται, οι πληροφορίες που αποθηκεύονται στην κάρτα μπορούν να επαληθευθούν τοπικά ενάντια σε έναν 'κωδικό πρόσβασης' ή PIN προτού να γίνει η σύνδεση στον host. Αυτό αποτρέπει τον κωδικό πρόσβασης από να "κρυφακουστεί" από τους δράστες στο διαδίκτυο.

Μερικές από τις έξυπνες κάρτες θα αποθηκεύσουν τα προσωπικά στοιχεία στην κάρτα.Παραδείγματος χάριν, το όνομα του κατόχου κάρτας, αριθμός ταυτότητας, και ημερομηνία γέννησης [Devargas1992].

5.5.3 Access control Κάρτα

Οι πιό κοινές συσκευές που χρησιμοποιούνται για να ελέγξουν την πρόσβαση στις ιδιωτικές περιοχές όπου η ευαίσθητη εργασία εκτελείται ή πού τα δεδομένα φυλάσσονται, είναι κλειδιά, διακριτικά και μαγνητικές κάρτες. Όλα αυτά έχουν τα ίδια βασικά μειονεκτήματα: μπορούν εύκολα να αναπαραχθούν και όταν τα κλέβουν ή πάψουν να υπάρχουν, μπορούν να επιτρέψουν την είσοδο από ένα αναρμόδιο πρόσωπο. Η έξυπνη κάρτα υπερνικά αυτές τις αδυναμίες καθιστώντας πολύ δύσκολη την αναπαραγωγή και αποδοχή τους στη θέση των ψηφιοποιημένων προσωπικών χαρακτηριστικών. Με τον κατάλληλο εξοπλισμό επαλήθευσης, αυτό το στοιχείο μπορεί να χρησιμοποιηθεί στό σημείο της εισόδου που προσδιορίζει εάν ο χρήστης είναι ο εξουσιοδοτημένος κάτοχος κάρτας. Η κάρτα μπορεί επίσης να προσωποποιηθεί χωριστά για να επιτρέψει την πρόσβαση στις περιορισμένες εγκαταστάσεις, ανάλογα με την εκκαθάριση ασφάλειας του κατόχου. Ένα log των κινήσεων του κατόχου, μέσω ενός συστήματος ασφάλειας, μπορεί να αποθηκευτεί στην κάρτα ως διαδρομή του ελέγχου ασφάλειας [McCrindle1990].

Η κάρτα θα μπορούσε να περιέχει τις πληροφορίες για τα προνόμια του χρήστη (δηλ. πρόσβαση στους ασφαλείς τομείς του κτηρίου, του αυτόματου προσδιορισμού οχημάτων στις εισόδους στα πάρκα αυτοκινήτων επιχείρησης, κ.λπ....) και χρονικούς περιορισμούς. Όλες οι πληροφορίες ελέγχονται στην ίδια την κάρτα. Η πρόσβαση στις διαφορετικές περιοχές του κτηρίου μπορεί να διακριθεί από διαφορετικά PINs. Επιπλέον, μπορεί επίσης να ακολουθήσει τη μετακίνηση του χρήστη γύρω από το κτήριο [Devargas1992].

5.5.4 Ψηφιακή Πιστοποιητικό

Τα σημαντικότερα μέτρα ασφάλειας που αντιμετωπίζουμε στην καθημερινή επιχείρησή μας δεν έχουν καμία σχέση με κλειδαριές και φύλακες. Ένας συνδυασμός ενός υπογεγραμμένου μηνύματος και η χρήση του δημόσιου βασικού κρυπτογραφικού συστήματος,

αποκαλούμενη ως **ψηφιακή υπογραφή**, χρησιμοποιούνται χαρακτηριστικά.

Ένα ψηφιακά υπογεγραμμένο μήνυμα που περιέχει ένα δημόσιο κλειδί καλείται πιστοποιητικό. Εκτός από ένα δημόσιο κλειδί, ένα πιστοποιητικό περιέχει τυπικά ένα όνομα, διεύθυνση και άλλες πληροφορίες που περιγράφουν τον κάτοχο του αντίστοιχου μυστικού κλειδιού.

Όλα αυτά φέρνουν την ψηφιακή υπογραφή μιας υπηρεσίας ληξιαρχείων που καταγράφει τα δημόσια κλειδιά για όλα τα μέλη της κοινότητας. Για να γίνει μέλος αυτής της κοινότητας, ένας συνδρομητής πρέπει να κάνει δύο πράγματα:

- παρέχετε στην υπηρεσία καταλόγου με ένα δημόσιο κλειδί καθώς και σχετικές πληροφορίες προσδιορισμού έτσι ώστε άλλοι άνθρωποι θα είναι σε θέση να ελέγξουν την υπογραφή του/της.
- λάβετε το δημόσιο κλειδί της υπηρεσίας καταλόγου έτσι ώστε μπορεί να ελέγξει τις υπογραφές άλλων ανθρώπων.

Επειδή τα πιστοποιητικά είναι εξαιρετικά ανθεκτικά στην πλαστογράφηση, η αυθεντικότητα ενός πιστοποιητικού είναι ιδιοκτησία του ίδιου του πιστοποιητικού, παρά της αυθεντικότητας του καναλιού πέρα από το οποίο παραλήφθηκε. Αυτή η σημαντική ιδιοκτησία επιτρέπει στα πιστοποιητικά να χρησιμοποιηθούν με παρόμοιο τρόπο με ένα διαβατήριο. Η αστυνομία συνόρων αναμένει να δει το διαβατήριό σας και να βασιστεί στις περισσότερες περιπτώσεις στην αντίσταση πλαστογραφήσεων του διαβατηρίου για να εγγυηθεί την αυθεντικότητά της. Λόγω του εύθραυστου των πιστοποιητικών εγγράφου, εντούτοις, υπάρχουν περιστάσεις στις οποίες αυτό δεν θεωρείται επαρκές. Οι προγενέστερες ρυθμίσεις πρέπει να έχουν γίνει χρησιμοποιώντας τα κανάλια που διατηρούνται για το σκοπό. Επειδή τα δημόσια βασικά πιστοποιητικά είναι ασφαλέστερα από οποιοδήποτε έγγραφο, μπορούν να

επικυρωθούν ακίνδυνα από την άμεση υπογραφή ελέγχοντας και κανένας εμπιστευμένος κατάλογος δεν απαιτείται.

5.5.5 Computer Login

Η πρόσβαση στο Computer room και τις υπηρεσίες του μπορεί να ελεγχθεί από την έξυπνη κάρτα. Από την άποψη της πρόσβασης στο δίκτυο, η έξυπνη κάρτα μπορεί να επικυρώσει το χρήστη στον host.

Επιπλέον, ανάλογα με το περιβάλλον που προστατεύεται η κάρτα πρόσβασης στο δίκτυο μπορεί επίσης να εκτελέσει τις ακόλουθες λειτουργίες:

- χειρισμός των διαφορετικών κωδίκων επικύρωσης για τα διαφορετικά επίπεδα ασφάλειας.
- χρήση των βιομετρικών τεχνικών ως προστιθέμενο μέτρο ασφάλειας.
- διατήρηση μιας διαδρομής του ελέγχου των αποτυχιών και των αποπειραθεισών παραβιάσεων.

Εν τω μεταξύ, από την άποψη της πρόσβασης στο δωμάτιο υπολογιστών, ο έλεγχος PIN μπορεί να γίνει στην κάρτα χωρίς την ανάγκη για σύνδεση των σημείων πρόσβασης σε έναν κεντρικό υπολογιστή.

Ο προσδιορισμός ενός χρήστη γίνεται συνήθως με τη βοήθεια ενός **(Personal Identification Number) PIN**. Το PIN ελέγχεται από το μικροϋπολογιστή της κάρτας με το PIN να αποθηκεύεται σε RAM του. Εάν η σύγκριση είναι αρνητική, η CPU θα αρνηθεί να λειτουργήσει. Το τσιπ κρατά επίσης τον αριθμό των διαδοχικών λανθασμένων καταχωρήσεων PIN. Εάν αυτός ο αριθμός φθάνει σε ένα

προκαθορισμένο κατώτατο όριο, η κάρτα εμποδίζεται ενάντια σε περαιτέρω χρήση.

5.6 Τεχνολογικές Απόψεις Σχετικά με τις Έξυπνες Κάρτες

Από τεχνική άποψη, οι έξυπνες κάρτες μπορούν να ταξινομηθούν σε δύο κύριους τύπους: **προγραμματίσημος** και **μη προγραμματίσιμος**. Ένας προγραμματιστής εφαρμογής έξυπνων καρτών μπορεί είτε να βάλει τη λογική εφαρμογής στο τερματικό, την κάρτα (εάν είναι μια προγραμματίσημη κάρτα) ή και τα δύο. Μπορούμε να δούμε τις μη προγραμματίσιμες έξυπνες κάρτες ως εξωτερική αποθήκευση, ακριβώς όπως μια δισκέτα, με τα χαρακτηριστικά γνωρίσματα ασφάλειας. Επομένως, μπορούμε να σχεδιάσουμε για να αποθηκεύσουμε ορισμένες φορητές πληροφορίες για την έξυπνη κάρτα και η εφαρμογή λογικής διατίθεται στην τελική πλευρά. Αφ' ετέρου, η προγραμματίσημη έξυπνη κάρτα, όπως η Java κάρτα, επιτρέπει στη εφαρμογή λογικής (νοημοσύνη) να στηριχτεί μερικώς στην έξυπνη κάρτα. Σε αυτό το κεφάλαιο, πρόκειται του προγραμματισμού να περιγράψουμε τις έννοιες επισκόπησης έξυπνων καρτών.

5.6.1 Επισκόπηση των Προτύπων ISO 7816

Ο ISO 7816 είναι το πρότυπο διεπαφών για την έξυπνη κάρτα. Οι ακόλουθοι υποτομείς είναι ενδιαφέροντες στον προγραμματιστή εφαρμογής έξυπνων καρτών:

ISO 7816-1: Φυσικά χαρακτηριστικά των καρτών

Καθορίζει τις διαστάσεις των καρτών και των φυσικών περιορισμών.

ISO 7816-2: Διαστάσεις και θέσεις των επαφών

Καθορίζει τις διαστάσεις, τη θέση και το ρόλο των ηλεκτρικών επαφών (η δύναμη VCC, το έδαφος GND, το ρολόι CLK, η αναστοιχειοθέτηση RST, η θύρα I/O I/O, δύναμη προγραμματισμού VPP και δύο πρόσθετες διατηρημένες επαφές για τη μελλοντική χρήση) στο μικροτσίπ.

ISO 7816-3: Ηλεκτρονικά σήματα και πρωτόκολλα μετάδοσης

Καθορίζει τα χαρακτηριστικά ηλεκτρονικών σημάτων που ανταλλάσσονται μεταξύ της κάρτας και του τερματικού και δύο πρωτοκόλλων επικοινωνίας: T=0 (κατά το ήμισυ διπλό πρωτόκολλο μετάδοσης χαρακτήρα Asynchronous) και T=1 (κατά το ήμισυ διπλό πρωτόκολλο μετάδοσης φραγμών Asynchronous)

ISO 7816-4: Inter-industry εντολές για την ανταλλαγή

Καθορίζει ένα σύνολο τυποποιημένων εντολών και μιας ιεραρχικής δομής συστημάτων αρχείων.

ISO 7816-5: Σύστημα αρίθμησης και διαδικασία εγγραφής για τα προσδιοριστικά εφαρμογής

Καθορίζει ένα μοναδικό όνομα εφαρμογής καρτών.

ISO 7816-7: Inter-industry εντολές για Structured Card Query Language (SCQL)

Καθορίζει ένα σύνολο εντολών για πρόσβαση στο περιεχόμενο των έξυπνων καρτών και της συγγενούς δομής βάσεων δεδομένων.

5.6.2 Πρωτόκολλο επικοινωνίας μεταξύ των τελικών και έξυπνων καρτών

Τα πρωτόκολλα επικοινωνίας μεταξύ της τελικής και έξυπνης κάρτας περιγράφονται στο ISO 7816-3 (Transport Protocol) και το ISO 7816-4 (Application Protocol). Αυτά τα δύο πρωτόκολλα περιγράφονται εν συντομία σε αυτό το τμήμα.

Το τερματικό μονογράφει μια έξυπνη κάρτα με τη διαβίβαση ενός σήματος στην επαφή αναστοιχειοθέτησης (RST) της κάρτας. Η κάρτα θα απαντήσει με τη διαβίβαση μιας σειράς των ψηφιολέξεων στο τερματικό αποκαλούμενο ATR (Answer-To- Reset). Αυτή η σειρά των ψηφιολέξεων αποτελείται από δύο μέρη: οι ψηφιολέξεις πρωτοκόλλου παρέχουν τις πληροφορίες για τα πρωτόκολλα επικοινωνίας που υποστηρίζονται από την κάρτα και οι ιστορικές ψηφιολέξεις παρέχουν τις πληροφορίες για τον τύπο κάρτας. Ένα παράδειγμα δίνεται για τον ATR της έξυπνης κάρτας ACS ACOS1 (που είναι ένας τύπος κάρτας μνήμης της επιχείρησης Advanced Card System):

Protocol Bytes	Historical Bytes
3B BE 11 00 00	41 01 10 04 00 12 00 00 00 00 00 02 90 00 (in hexidecimal)

Οι λεπτομέρειες του ATR περιγράφονται στα πρότυπα του ISO 7816-3. Περιγράφουμε εν συντομία τις πρώτες τρεις ψηφιολέξεις στις ψηφιολέξεις πρωτοκόλλου εδώ. Οι ψηφιολέξεις "3B" περιμένουν για τη μέθοδο μεταφοράς κομματιών. "Το BE" σημαίνει ότι υπάρχουν πρόσθετες πληροφορίες (14 ιστορικές ψηφιολέξεις). Οι ψηφιολέξεις "11" περιγράφουν τις πληροφορίες της ταχύτητας ρολογιών και του ποσοστού μεταφοράς κομματιών. Οι ιστορικές ψηφιολέξεις δίνουν τις πληροφορίες

για τις αναφορές και τις εκδόσεις του τσιπ της κάρτας και του λειτουργικού συστήματος.

Αφότου διαβιβάστηκε ο ATR, το τερματικό μπορεί να επικοινωνήσει με την έξυπνη κάρτα με την αποστολή των εντολών. Οι εντολές είναι ενθυλακωμένες σε πακέτα. Αυτά τα πακέτα καλούνται **Transport Protocol Data Unit (TPDU)**. Κάθε πακέτο αρχίζει με τις ακόλουθες πέντε ψηφιολέξεις (Header) που ακολουθούνται από διάφορες ψηφιολέξεις για τον τομέα Data εάν είναι απαραίτητο:

CLA	**INS**	**P1**	**P2**	**P3**

TPDU Header

class byte (CLA): Μια κατηγορία οδηγιών. Οι τιμές μερικών class byte μπορούν να έχουν μια συγκεκριμένη σημασία αναφερόμενες σε μια ορισμένη κατηγορία εντολών. Παραδείγματος χάριν, η ψηφιολέξη κατηγορίας της έξυπνης κάρτας ACS ACOS1 είναι 80_H και Gemplus 32 bit Java Card είναι $A8_H$.

instruction byte (INS): Μια ιδιαίτερη οδηγία. Παραδείγματος χάριν, η οδηγία SUBMIT CODE της έξυπνης κάρτας ACS ACOS1 είναι 20_H.

parameter bytes (P1 & P2): Οι παράμετροι για την οδηγία. Παραδείγματος χάριν, οι παράμετροι της εντολής SUBMIT PIN είναι $P1 = 06_H$ και $P2 = 00_H$.

parameter byte (P3): Ο αριθμός ψηφιολέξεων στοιχείων που διαβιβάζονται με την εντολή κατά τη διάρκεια της ανταλλαγής. Αυτή η ψηφιολέξη μπορεί να δείξει τον αριθμό ψηφιολέξεων που το τερματικό

θα στείλει στην κάρτα (Lc) ή τον αριθμό ψηφιολέξεων που το τερματικό αναμένει να λάβει από την κάρτα (Le). Παραδείγματος χάριν, P3 στην οδηγία SUBMIT PIN CODE είναι 08_H δεδομένου ότι ο (Personal Identification Number) κώδικας PIN στην έξυπνη κάρτα ACS ACOS1 είναι 8 ψηφιολέξεις μακριές.

Μετά λαμβάνοντας το header, το τερματικό περιμένει μια ψηφιολέξη διαδικασίας από την έξυπνη κάρτα:

- acknowledge byte: Με βάση την ψηφιολέξη INS, μπορεί να δείξει ότι το τερματικό πρέπει να στείλει τα στοιχεία ή να αναμείνει να λάβει τα στοιχεία. Με βάση αναγνωρίστε την ψηφιολέξη, η εντολή πρωτοκόλλου APDU επιπέδων εφαρμογής (Application Protocol Data Units) διαμορφώνεται με την επιγραφή TPDU. Υπάρχουν τέσσερα πιθανά σχήματα της εντολής APDU:

1. καμία ανταλλαγή ψηφιολέξεων στοιχείων που απαιτείται.

CLA	INS	P1	P2

Format 1 of APDU command

2. Μόνο τελικός λάβετε τις ψηφιολέξεις στοιχείων από την έξυπνη κάρτα (Le).

CLA	INS	P1	P2	Le

Format 2 of APDU command

3. Μόνο τελικός στέλνει τις ψηφιολέξεις στοιχείων στην έξυπνη κάρτα (Lc).

CLA	INS	P1	P2	Lc	Data

Format 3 of APDU command

4. Το τερματικό στέλνει τις ψηφιολέξεις στοιχείων στην έξυπνη κάρτα (Lc) και λαμβάνει επίσης τις ψηφιολέξεις στοιχείων από την έξυπνη κάρτα (Le).

CLA	INS	P1	P2	Lc	Data	Le

Format 4 of APDU command

Εάν Le = 0,κατόπιν ο αριθμός ψηφιολέξεων αναμενόμενος είναι απροσδιόριστος και πρέπει να παρασχεθεί από την έξυπνη κάρτα (μέγιστες 256 ψηφιολέξεις). Όταν οι ψηφιολέξεις στοιχείων διαβιβαστούν, το τερματικό αναμένει μια νέα ψηφιολέξη διαδικασίας.

- NUL byte (value 0x60) : η έξυπνη κάρτα ζητά περισσότερο χρόνο επεξεργασίας. Το τερματικό πρέπει να επαναρυθμίσει το χρονόμετρο διαλείμματος καρτών του και να περιμένει μια άλλη ψηφιολέξη διαδικασίας.
- status word (SW1 και SW2) : Η status word τελειώνει την εντολή. Είναι μέσα στο πρότυπο ISO-7816-4. Εδώ είναι ένα υποσύνολο κοινών status words:

SW1	SW2	1.1.1.1.1 Meaning
90	**00**	**O.K.**
67	**00**	**Wrong P3**
69	**66**	**Command not available**
6A	**86**	**P1-P2 incorrect**

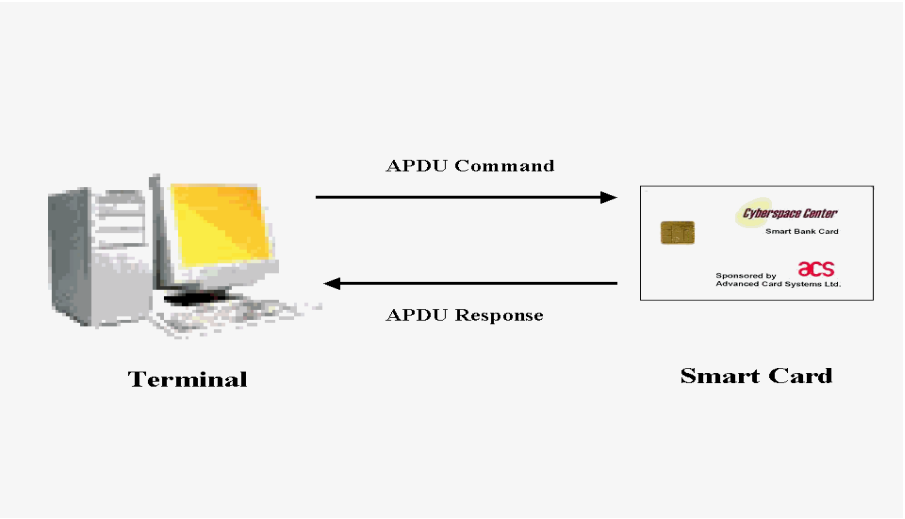
6D	**00**	**Unknown INS**
6E	**00**	**Invalid CLA**

Με βάση SW1 και SW2, ένα APDU θα επιστραφεί με το ακόλουθο σχήμα. Το μέρος Data είναι προαιρετικό, επειδή μερικές εντολές APDU δεν απαιτούν οποιαδήποτε στοιχεία από την έξυπνη κάρτα όπως σε περιπτώσεις 1 και 3 ανωτέρω.

Data	**SW1**	**SW2**

Format of response APDU

Η επικοινωνία μεταξύ της τελικής και έξυπνης κάρτας (όπως φαίνεται στο σχήμα 4-1) περιλαμβάνει μια εντολή APDU που στέλνεται από το τερματικό στην έξυπνη κάρτα και μια απάντηση APDU από την έξυπνη κάρτα στο τερματικό βασισμένο στο αποτέλεσμα της εντολής APDU. Αυτές οι ανταλλαγές όλες κωδικοποιούνται στο επίπεδο TPDUs πρωτοκόλλου μεταφορών.
Μια ανταλλαγή εντολής/απάντησης στο επίπεδο APDU πρωτοκόλλου εφαρμογής μπορεί να απαιτήσει περισσότερες από μια ανταλλαγές TPDU.



Εδώ είναι ένα παράδειγμα της εντολής/της απάντησης APDU μεταξύ της έξυπνης κάρτας *ACS ACOS1* και ενός τερματικού. Η εντολή χρησιμοποιείται από την έξυπνη κάρτα για να υποβάλει τον κώδικα PIN για την επικύρωση στο τερματικό.

ΥΠΟΒΑΛΤΕ PIN:

Για να υποβάλει έναν μυστικό κώδικα (PIN) στο έξυπνο catd.

Εντολή APDU:

CLA	INS	P1	P2	P3	DATA
80	20	6	00	08	PIN Code or DES(PIN Code,#Ks)

PIN Code **Eight bytes PIN Code**

DES(Code,#Ks) **Eight bytes PIN Code encrypted with Session Key (Ks)**

Απάντηση APDU:

1.1.1.2 SW1	SW2
Status	

Συγκεκριμένοι Status Codes:

SW1	SW2	Meaning
63	Cn	Wrong Code; n = remaining number of re-tries
69	83	The specified Code is locked
69	85	Mutual Authentication not successfully completed prior to the SUBMIT PIN CODE command

Στη διαδικασία SUBMIT PIN, το τερματικό μπορεί είτε να υποβάλει τον κώδικα PIN με το σαφές σχήμα κειμένων (χωρίς κρυπτογράφηση) είτε με κρυπτογραφημένο το DES σχήμα εάν το αντίστοιχο κομμάτι DES επιλογής στο Security Option Register τίθεται.

5.6.3 Επισκόπηση των Συστημάτων Αρχείων

Το σύστημα αρχείων στα ISO-7816-4 είναι ένα από τα σημαντικά συστατικά στην έξυπνη κάρτα για την αποθήκευση στοιχείων. Το σύστημα αρχείων είναι ένα ιεραρχικό σύστημα αρχείων όπως το MS-DOS:

- ένα σύστημα αρχείων έχει μια ρίζα, η οποία καλείται *master file (MF)*.
- οι κατάλογοι που καλούνται *dedicated files* χρησιμοποιούνται για να οργανώσουν *(DF)*.
- τα κανονικά αρχεία καλούνται *elementary files (EF)*.

Τα αρχεία παραπέμπονται από ένα *file identifier* (FID) που είναι δύο ψηφιολέξεις μακριές. Υπάρχουν διάφορα είδη στοιχειωδών αρχείων:

- διαφανή αρχεία, τα οποία θεωρούνται ως ακολουθία ψηφιολέξεων.
- γραμμικά σταθερά αρχεία, τα οποία θεωρούνται ως ακολουθία καθορισμένου μήκους αρχείων.
- γραμμικά μεταβλητά αρχεία, τα οποία θεωρούνται ως ακολουθία αρχείων μεταβλητός-μήκους.
- κυκλικά αρχεία, τα οποία θεωρούνται ως ατελείωτη ακολουθία αρχεssων καθορssζω-μεγέθους.

Στην έξυπνη κάρτα *ACS ACOS1*, τα αρχεία καθορίζονται και κατασκευάζονται στο στάδιο εξατομίκευσης. Το πρόγραμμα εφαρμογής που τρέχει για το τερματικό μπορεί έπειτα να έχει πρόσβαση στα αρχεία χρησιμοποιώντας τις εντολές APDU εάν επικυρώνεται. Εδώ είναι ένα παράδειγμα της εντολής SELECT FILE που χρησιμοποιείται για να

επιλέξει ένα αρχείο στοιχείων για τις επόμενες εντολές READ RECORD και WRITE RECORD.

ΕΠΙΛΕΞΤΕ ΤΟ ΑΡΧΕΙΟ:

Για να επιλέξει ένα αρχείο στοιχείων για τις επόμενες εντολές READ RECORD και WRITE RECORD.

- **Εντολή APDU:**

CLA	INS	P1	P2	P3	DATA
80	A4	00	00	02	File ID

File ID **Two bytes file identifier**

Απάντηση APDU:

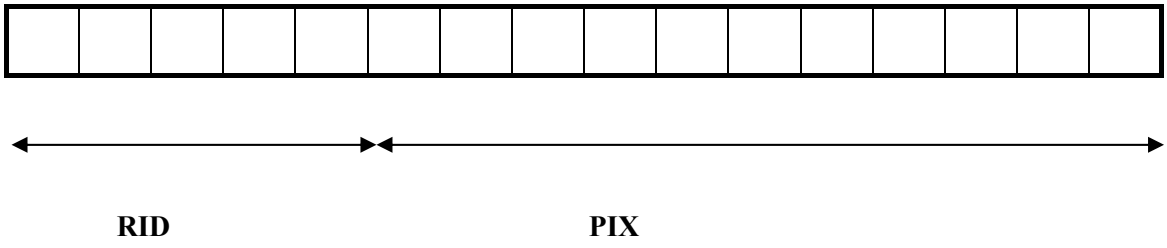
1.1.1.3 SW1	SW2
Status	

Specific Status Codes:

SW1	SW2	Meaning
6A	82	File does not exist.
91	xx	File selected. xx is the number of the record in the User File Management File which contains the File Definition Block of the selected file.

5.6.4 Επισκόπηση Ονομαστικού Σχεδίου

Το πρότυπο του ISO 7816-5 καθορίζει ένα ονομαστικό σχέδιο για τις εφαρμογές των έξυπνων καρτών. Κάθε εφαρμογή προσδιορίζεται από ένα προσδιοριστικό εφαρμογής (AID). Το AID είναι μεταξύ 1 έως 16 ψηφιολέξεων μακριών. Ο προμηθευτής έξυπνων καρτών πρέπει να πάρει ένα καταχωρημένο προσδιοριστικό προμηθευτών εφαρμογής (RID) από τον ISO. Το AID κατασκευάζεται όπως παρουσιάζεται κατωτέρω:



Οι πρώτες πέντε ψηφιολέξεις είναι το RID, και οι τελευταίες 11 ψηφιολέξεις (PIX) μπορούν να οριστούν ελεύθερα από τον προμηθευτή έξυπνων καρτών.

5.6.5 Επισκόπηση Αρχιτεκτονικής Ασφαλείας

Υπάρχουν δύο κύριοι μηχανισμοί ασφάλειας που παρέχονται τις εφαρμογές για έξυπνων καρτών: έλεγχος και σύστημα κρυπτογραφία πρόσβασης. Για τον έλεγχο πρόσβασης, η εφαρμογή ή ο κάτοχος κάρτας μπορεί να πρέπει να υποβάλει ένα PIN (Personal Identification Number) πριν από οποιαδήποτε εντολή APDU. Στην έξυπνη κάρτα *ACS ACOS1*, κατασκευαστή η εφαρμογή πρέπει επίσης να υποβάλει το Issuer Code (IC) που ορίζεται από τον έξυπνων καρτών προκειμένου να υποβληθεί οποιαδήποτε εντολή APDU. Επιπλέον, υπάρχει ένα σύνολο Application Codes (AC) που μπορεί να τεθεί ως στόχος προκειμένου να ενισχυθεί ο έλεγχος πρόσβασης στο σύστημα αρχείων. Σε κάθε αρχείο ορίζεται μια ιδιότητα ασφάλειας Read και Write. Η ασφάλεια Attributes καθορίζει τους όρους ασφάλειας που πρέπει να τηρηθούν για να επιτρέψουν την αντίστοιχη λειτουργία. Το κανάλι επικοινωνίας μεταξύ της έξυπνης κάρτας και του τερματικού μπορεί να προστατευθεί από το σύστημα κρυπτογραφία όπως DES (συμμετρικός αλγόριθμος) και τη ΔΝΑ (δημόσιος-βασικός αλγόριθμος). Επιπλέον, μπορούν να υπάρξουν άλλοι διαφορετικοί κατασκευαστές συγκεκριμένοι μηχανισμοί ασφάλειας που παρέχονται από τους διαφορετικούς έξυπνων καρτών. Παραδείγματος χάριν, οι ακόλουθοι μηχανισμοί ασφάλειας παρέχονται από την έξυπνη κάρτα *ACS ACOS1*:

- ***DES και MAC υπολογισμός***:
  Ο DES αναφέρεται στον αλγόριθμο DEA για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Η MAC αναφέρεται στον αλγόριθμο για την παραγωγή κρυπτογραφικού checksum.

- ***Αμοιβαίο Authentication και Session Key βασισμένο σε Random Numbers***:
  Αμοιβαίο Authentication είναι μια διαδικασία στην οποία ο αναγνώστης και η έξυπνη κάρτα και έξυπνων καρτών ελέγχουν την ο

ένας του άλλου ισχύ. Το Session Key είναι ένα αποτέλεσμα της επιτυχούς εκτέλεσης της διαδικασίας Mutual Authentication. Χρησιμοποιείται για τα στοιχεία κρυπτογράφηση και αποκρυπτογράφηση κατά τη διάρκεια μιας συνόδου.Μια σύνοδος ορίζεται ως ο χρόνος μεταξύ της επιτυχούς εκτέλεσης μιας διαδικασίας Mutual Authentication και μιας αναστοιχειοθέτησης της κάρτας ή της εκτέλεσης μιας άλλης εντολής START SESSION.

- ***Μυστικοί Κώδικες****:*
  Οι Μυστικοί Κώδικες και ο κώδικας PIN χρησιμοποιούνται για να επιτρέψουν επιλεκτικά την πρόσβαση στα στοιχεία που αποθηκεύονται στην κάρτα και στα χαρακτηριστικά γνωρίσματα και τις λειτουργίες που παρέχονται από την έξυπνη κάρτα.

- ***Secure Account Transaction Processing****:*
  Ο Account Transaction Processing παρέχει έναν μηχανισμό για τον ασφαλή και ελέγξιμο χειρισμό των στοιχείων στο Account Data Structure.

5.6.6 Ένα παράδειγμα της εφαρμογής έξυπνων καρτών: SmartFlow σύστημα πληρωμής Διαδικτύου

Το ηλεκτρονικό εμπόριο στο διαδίκτυο είναι ένας δημοφιλής ερευνητικός τομέας, αλλά η έλλειψη ασφαλούς πρωτοκόλλου μεταφοράς πληρωμής είναι το κύριο εμπόδιο για να προωθήσει τις βασισμένες στο WEB επιχειρησιακές δραστηριότητες. Η τεχνολογία έξυπνων καρτών προσφέρει ένα σύνολο πολύτιμων χαρακτηριστικών γνωρισμάτων όπως ο προσδιορισμός, η ασφάλεια και η αυθεντικότητα για πολλές διαφορετικές

εφαρμογές, ειδικά για τις συναλλαγές πληρωμής. Το σύστημα SmartFlow, που αναπτύσσεται από το Cyberspace Center, όπως φαίνεται στον αριθμό 4-2 ενσωματώνει την υπάρχουσα τεχνολογία της έξυπνης κάρτας, Διαδικτύου και της ροής της δουλειάς για να καταδείξει ένα νέο πρωτότυπο για το ασφαλές σε μη απευθείας σύνδεση περιβάλλον συναλλαγής μικροϋπολογιστής-πληρωμής. Η σε μη απευθείας σύνδεση μικροϋπολογιστής-πληρωμή είναι κατάλληλη για τη χαμηλές συναλλαγή αξίας και την προστασία μυστικότητας.

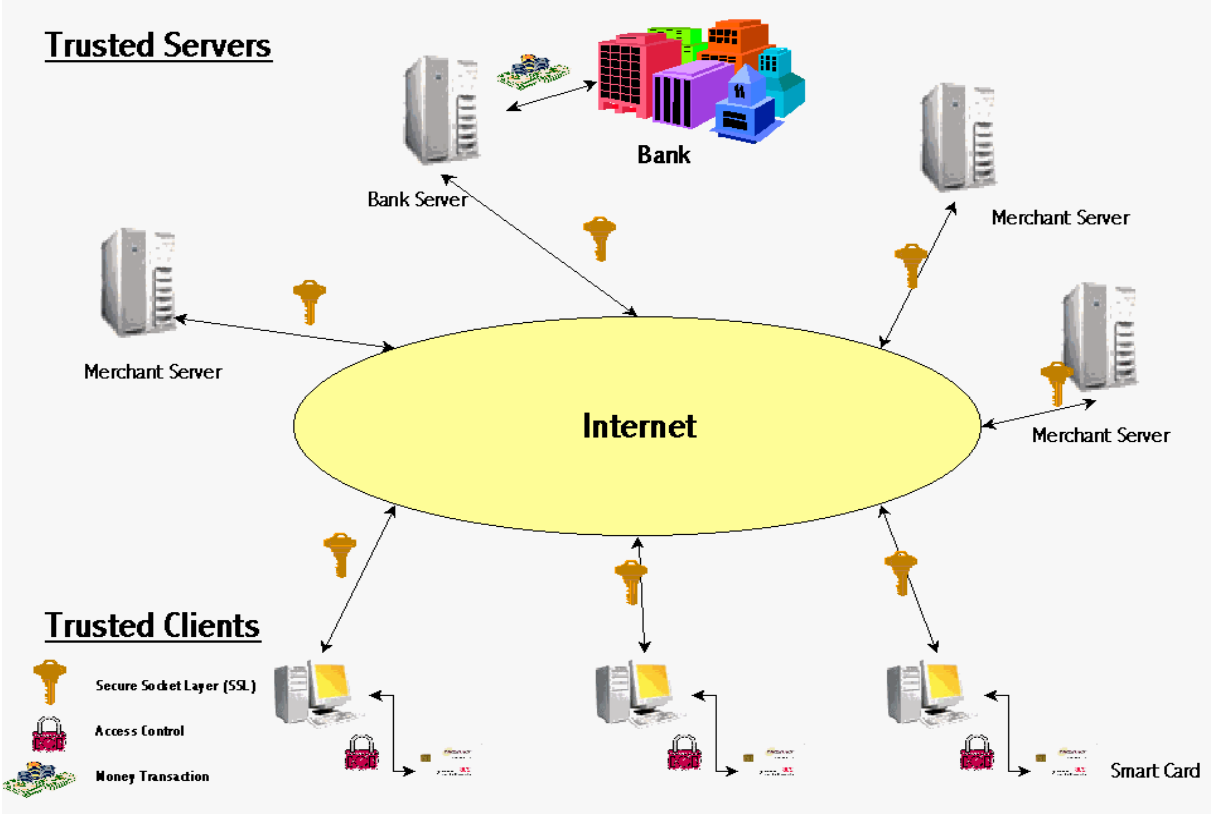


Figure 4-2. Architecture of SmartFlow Internet Payment System.

Η πρώτη έκδοση του συστήματος πρωτοτύπων SmartFlow έχει εφαρμοστεί και είναι έτοιμο για την επίδειξη στο Cyberspace Center σε The Χογκ Κογκ University Science και Technology. Το *Smart Bank Card* εφαρμόζεται από την έξυπνη κάρτα *ACS ACSO1* όπως φαίνεται στο σχήμα 4-3. Αυτό είναι μια κάρτα μνήμης 1-kbyte EEPROM που φυλάσσει τα στοιχεία εφαρμογής. Η έξυπνη κάρτα *ACS ACOS1* είναι μια κάρτα μνήμης με τη λογική ελέγχου ασφάλειας που είναι υποχωρητική

με τον ISO 7816-3, T=0 πρωτόκολλο (ημιαμφίδρομο), με τις ικανότητες DES και της MAC. Περιέχει επίσης τον κώδικα εκδοτών και τον κωδικό πρόσβασης χρηστών που μπορούν από ο χρήστης να αλλάξουν. Η λογική ελέγχου ασφάλειας προστατεύει τη μνήμη για να αποτρέψει την παράνομη τροποποίηση, αλλά τα στοιχεία μπορούν να διαβαστούν όταν υποβάλλονται σωστά ο κώδικας και ο κωδικός πρόσβασης εκδοτών. Επίσης, οι διαφορετικές θέσεις μνήμης μπορούν να προστατευθούν από τους διαφορετικούς ελέγχους ασφάλειας.

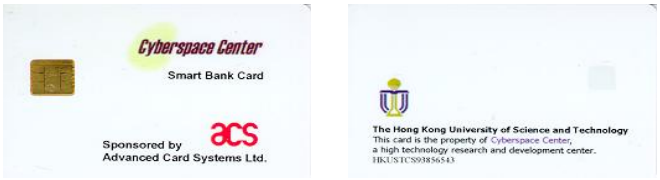


Figure 4-3. ACS ACSO1 Smart Card in Cyberspace Center.

Το σύστημα αναπτύσσεται στο Windows Platform χρησιμοποιώντας ActiveX που γράφεται σε Visual Basic για να χτίσει τη λογική και front-end συστημάτων. Το οπίσθιο μέρος υποστηρίζεται από τα WINDOWS NT Server και όλα τα σχετικά στοιχεία αποθηκεύονται και ρυθμίζονται από τα κράτη μέλη SQL Database Server. Το σύστημα υποστηρίζεται από τον Internet Information Server που τρέχει στα WINDOWS NT Server, και το κανάλι επικοινωνίας εξασφαλίζεται από Secure Socket Layer (SSL). Χρησιμοποιούμε Internet Explorer 4,0 για τον browser επειδή το σύστημα αναπτύσσεται σε Active X που υποστηρίζεται μόνο από Internet Explorer όπως φαίνεται στο σχήμα 4-4.

Figure 4-4. SmartFlow Internet Payment System.

Για την απεικόνιση, είναι εδώ ο κώδικας πηγής της λειτουργίασ *Select_File* στο SmartFlow Διαδίκτυο Payment System. Αυτή η λειτουργία χρησιμοποιείται για να επιλέξει ένα αρχείο στην έξυπνη κάρτα. Η εντολή APDU SELECT FILE περιγράφηκε νωρίτερα, το CLA είναι 80 $_{\chi}$, το INS είναι A4 $_{\chi}$, P1 είναι 00 $_{\chi}$, P2 είναι 00 $_{\chi}$ και P3 (Lc) είναι 02 $_{\chi}$ επειδή το προσδιοριστικό αρχείων είναι δύο ψηφιολέξεις μακριές και το LE είναι 00 $_{\chi}$ που σημαίνει να χρησιμοποιήσει την προκαθορισμένη αξία που είναι 256 ψηφιολέξεις μακριές. Η λειτουργία

APDUExchangeFull API αρχίζει τη σύνοδο επικοινωνίας με την έξυπνη κάρτα και έπειτα η εντολή APDU (SELECT FILE) υποβάλλεται στην έξυπνη κάρτα. Η απάντηση APDU (SW1 και SW2) και Data (ResponseTempOut), ενδεχομένως, θα επιστραφούν από την έξυπνη κάρτα στην εφαρμογή (τερματικό).

```
Public Const CONST_SELECT_FILE = "80A400000200"

Dim TempCLA As String

Dim TempINS As String

Dim TempP1 As String

Dim TempP2 As String

Dim TempLc As String

Dim TempLe As String


Public Sub Select_File( ResponseTempOut As String,  FileIdentifier As String,  SW1Out As String,  SW2Out As String)


   Dim DummyDataOut As String


   TempCLA = LTrim(Mid(CONST_SELECT_FILE, 1, 2))

   TempINS = LTrim(Mid(CONST_SELECT_FILE, 3, 2))

   TempP1 = LTrim(Mid(CONST_SELECT_FILE, 5, 2))

   TempP2 = LTrim(Mid(CONST_SELECT_FILE, 7, 2))

   TempLc = LTrim(Mid(CONST_SELECT_FILE, 9, 2))
```

```
TempLe = LTrim(Mid(CONST_SELECT_FILE, 11, 2))


Call APDUExchangeFull(TempCLA, TempINS, TempP1, TempP2,
TempLc, TempLe, SW1Out, SW2Out, FileIdentifier, ResponseTempOut,
DummyDataOut)
End Sub
```

5.7 Έξυπνες Κάρτες στο E-Commerce

Μια άλλη κατευθυντήρια δύναμη πίσω από την αύξηση των έξυπνων καρτών είναι η αύξηση στα δίκτυα υπολογιστών και η εμφάνιση του Διαδικτύου ως τρόποι και ηλεκτρονικής επικοινωνίας και εμπορίου. Μαζί, έχουν δημιουργήσει μια ανάγκη για την ασφαλή πρόσβαση στο στοιχείο που αποθηκεύεται όλο και περισσότερο στο δίκτυο. Επειδή μια έξυπνη κάρτα μπορεί να περιλάβει τις πολύ ακριβείς πληροφορίες πρόσβασης για να προστατεύσει την ασφάλεια μυστικότητας και στοιχείων, οι έξυπνες κάρτες θα γίνουν μια όλο και περισσότερο ελκυστική εναλλακτική λύση για το PC και πρόσβαση Διαδικτύου έναντι των παραδοσιακών μεθόδων. Αυτές οι εφαρμογές κάνουν την έξυπνη κάρτα μια άμεση, ασφαλή επέκταση του δικτύου PC.

Οι πρόσφατοι αριθμοί από την Price Waterhouse που δίνεται στο Information Strategy, Ιούνιος 1998, παρουσιάζουν ότι οι business-to-business σε απευθείας σύνδεση εμπορικές συναλλαγές διπλασιάζονται κάθε 3-4 μήνες και οι καταναλωτικές σε απευθείας σύνδεση αγορές τίθενται ως στόχος να αυξηθούν 1.800% από το 1997 ως το 2002 [Birch1998]. Πολλοί άνθρωποι υποστηρίζουν ότι η ασφάλεια είναι το μόνο οδόφραγμα στο ηλεκτρονικό εμπόριο. Στην πραγματικότητα, η ασφάλεια δεν είναι το μόνο οδόφραγμα στο ηλεκτρονικό εμπόριο, τα

πιθανά εμπόδια περιλαμβάνουν την πρόσβαση στην υποδομή, την εμπιστοσύνη καταναλωτών και επιχειρήσεων, τα ρυθμιστικά ζητήματα αβεβαιότητας, φορολογίας και πνευματικών δικαιωμάτων.

Οι περισσότεροι καταναλωτές ανησυχούν για την κλοπή των πληροφοριών πιστωτικών καρτών τους και τη μυστικότητα των προσωπικών στοιχείων τους. Αφ' ετέρου, οι επιχειρήσεις ανησυχούν για το ότι τα εσωτερικά συστήματα και τα δίκτυά τους θα προσβληθούν από hackers. Εντούτοις, σύμφωνα με μια έκθεση σε Business Week στις 19$ Ιουνίου 1998, on-line που αγοράζει αναρριχείται σταθερά ακόμη και ελλείψει μιας περιεκτικής υποδομής ασφάλειας.

Στα περισσότερα συστήματα ηλεκτρονικού εμπορίου, το λογισμικό δεν μπορεί μόνο να παραδώσει το επίπεδο ασφάλειας που απαιτείται για να υποστηρίξει το ηλεκτρονικό εμπόριο. Κάποια μορφή "σκληρής" ασφάλειας απαιτείται, και στη μαζική αγορά, οι έξυπνες κάρτες μπορούν να παραδώσουν την πλαστογράφηση-αντίσταση, τη φορητότητα και την οικειότητα.

Η μετάβαση από τα ιδιόκτητες συστήματα οι πλατφόρμες και τις εφαρμογές έξυπνων καρτών λειτουργικά για να ανοιχτούν πολυ-εφαρμογής έξυπνων καρτών όπως MULTOS και η Java Card πρέπει να επιταχύνει την ενσωμάτωση των έξυπνων καρτών στο εμπόριο Διαδικτύου.

Όταν οι έξυπνες κάρτες χρησιμοποιούνται στην ηλεκτρονική πληρωμή, η προστασία ασφάλειας θα μπορούσε να ενισχυθεί με την επέκταση της προστασίας από τη δευτερεύουσα επαλήθευση καρτών κεντρικών υπολογιστών στη δευτερεύουσα επικύρωση πελατών. Η έξυπνη κάρτα μαζί με την αυτόματη αναγραφή τραπεζών των συναλλαγών μπορεί να αποτρέψει τα λάθη και χαμένος και κλεμμένος συναλλαγές καρτών.

Επιπλέον, με την εφαρμογή ενός κατάλληλου πρωτοκόλλου πληρωμής, και οι τράπεζες και οι λιανοπωλητές θα μπορούσαν να προστατευθούν από την ψευδή χρήση καρτών. Με τηn online επικύρωση από τις τράπεζες που το υποστηρίζουν, οι κλεμμένες ή χαμένες κάρτες θα μπορούσαν να προσδιοριστούν.

5.7.1 Πρωτόκολλο Πληρωμής Έξυπνων Καρτών

Ο σημαντικότερος παράγοντας στην ασφάλεια χρησιμοποιείται στο πρωτόκολλο πληρωμής. Η πληρωμή στην έξυπνη κάρτα μοιράζεται την ίδια αρχή με άλλα σε απευθείας σύνδεση σχέδια πληρωμής, εκτός από το ότι των έξυπνων καρτών πρέπει να έχει την offline δυνατότητα συναλλαγής επίσης, διαφορετικά το όφελος της έξυπνης κάρτας δεν μπορεί να πραγματοποιηθεί πλήρως.

Διάφορα πρωτόκολλα πληρωμής έχουν αναπτυχθεί για τις πληρωμές, παραδείγματος χάριν, Mondex, Visa Cash, C-SET και Open Trading Protocol έξυπνων καρτών (OTP). Τα περισσότερα από αυτά τα πρωτόκολλα προέρχονται πρότυπα από τραπεζικών εργασιών ή ύπαρξης της πληρωμής. Εντούτοις, όλοι υποθέτουν ότι η συναλλαγή γίνεται στην τοπική περιοχή ή απαιτούν ένα ασφαλές κανάλι επικοινωνίας. Η υπόθεση μπορεί να είναι αληθινή όταν περιορίζεται η συναλλαγή στην online σύνδεση συναλλαγή μέσω των καναλιών της τράπεζας. Για την online πληρωμή Διαδικτύου, το πρωτόκολλο των συναλλαγών χρησιμοποιούμενο έχει επιπτώσεις πολύ στην ασφάλεια έξυπνων καρτών. Επομένως μερικές επιχειρήσεις έχουν αρχίσει να εξετάζουν αυτό το ζήτημα και έχουν αναπτύξει τα ασφαλή πρωτόκολλα πληρωμής τους.

Τα πρωτόκολλα στην πληρωμή έξυπνων καρτών ενδιαφέρονται κυρίως για τα ζητήματα μυστικότητας, ασφάλειας και αποκατάστασης. Εάν η έξυπνη κάρτα πρόκειται να αντικαταστήσει τα φυσικά μετρητά, τα ζητήματα μυστικότητας και ασφάλειας θα ήταν πολύ σημαντικά. Για να εξασφαλίσουν τη μυστικότητα και την ασφάλεια, τα νέα πρωτόκολλα πληρωμής πρέπει να παραχθούν. Επειδή τις συνδέσεις μπόρεσαν να σπάσουν οποιαδήποτε στιγμή, εάν κανένα σχέδιο αποκατάστασης δεν χρησιμοποιείται για την παρεμπόδιση της απώλειας ή του διπλασιασμού αυτές ηλεκτρονικά μετρητά, το χάος θα οδηγούσε. Αυτά τα ζητήματα έχουν προκύψει και η προτεινόμενη λύση μας δημοσιεύεται μέσα [Chan1998]. Η περαιτέρω συζήτηση σχετικά με αυτό το θέμα θα

μπορούσε να βρεθεί στο εγχειρίδιο Electronic Payment Systems συντρόφων μας. Δεδομένου ότι αυτό είναι ένα αυξανόμενο πρόβλημα, οι καλύτερες λύσεις θα απαιτούνταν.

5.7.2 Έξυπνη κάρτα ως προπληρωμένη και κάρτα πιστότητας

Η έξυπνη κάρτα έχει χρησιμοποιηθεί στο ηλεκτρονικό εμπόριο ως προπληρωμένη, χρεωστική κάρτα για μια χρονική περίοδο. Τα γνωστά παραδείγματα περιλαμβάνουν τις κάρτες κερματοδεκτών, Mondex και Visa Cash. Αυτό αλλάζει το οικονομικό πρότυπο της πληρωμής. Επειδή τα χρήματα υπάρχουν τώρα και με ηλεκτρονικές και φυσικές μορφές, η παραδοσιακή μέθοδος πληρωμής θα έπρεπε να τροποποιηθεί.

Από την άποψη ασφάλειας, η έξυπνη κάρτα είναι ασφαλέστερη από το κανονικό πορτοφόλι. Οι κωδικοί πρόσβασης θα μπορούσαν να χρησιμοποιηθούν για να αποτρέψουν την απώλεια χρημάτων όταν κλέβεται η κάρτα. Με την κατάλληλη ασφάλεια που θέτει, οι άκυρες προσπάθειες κωδικού πρόσβασης θα μπορούσαν να οδηγήσουν στην απενεργοποίηση της έξυπνης κάρτας.

Ένα άλλο ελκυστικό χαρακτηριστικό γνώρισμα της έξυπνης κάρτας χρεώσεων είναι η χρηστικότητά της. Η έξυπνη κάρτα χρεώσεων είναι μια ενδιάμεση λύση μεταξύ των μετρητών και της πιστωτικής κάρτας. Δεδομένου ότι η κάρτα είναι βασικά χρησιμοποιείται ως αντικατάσταση των νομισμάτων (δηλ. μετρητά), η απώλεια μερικών νομισμάτων δεν θα προκαλέσει την απώλεια στον τραπεζικό λογαριασμό.

Πολλά επιτυχή σχέδια ηλεκτρονικών πορτοφολιών έχουν εφαρμοστεί στις "στενές κοινότητες" συμπεριλαμβανομένων των πανεπιστημιουπόλεων, κολλεγίων και των ογκωδών υπηρεσιών μεταφορών. Θα μπορούσε να εφαρμοστεί στις εξόδους γρήγορων τροφίμων, laundromats, τις μηχανές φωτοτυπιών, τις υπηρεσίες fax και τις μηχανές πώλησης. Γενικά, η χρέωση και οι προπληρωμένες κάρτες

για τις μικρές πληρωμές αξίας θα είναι σύντομα κοινές όταν δέχονται περισσότεροι έμποροι αυτό το σχέδιο πληρωμής.

Το μέλλον της έξυπνης κάρτας στο ηλεκτρονικό εμπόριο είναι όχι μόνο στις κάρτες πληρωμής, αλλά και τις κάρτες πίστης, τα εισιτήρια αερογραμμών και άλλες προστιθεμένης αξίας κάρτες. Οι προτιμήσεις των πελατών, το επίδομα και άλλες πληροφορίες θα μπορούσαν να κρατηθούν στην κάρτα. Οι επιχειρήσεις θα μπορούσαν έπειτα να λάβουν τις προτιμήσεις των πελατών τους και τις ιστορίες αγορών για τον προγραμματισμό περισσότερων προσανατολισμένων στους πελάτες εμπορικών στρατηγικών. Η κάρτα θα μπορούσε επίσης να προσωποποιηθεί για να κρατήσει το σχεδιάγραμμα του κατόχου κάρτας [Gemplus9801]. Κατ' αυτό τον τρόπο, οι επιχειρήσεις θα μπορούσαν να γίνουν ανταγωνιστικότερες στην προσέλκυση των πελατών.

5.7.3 Έξυπνη κάρτα ως ηλεκτρονικό πορτοφόλι

Στο μέλλον, η έξυπνη κάρτα θα χρησιμοποιούταν για την πληρωμή στις διαφορετικές πτυχές. Θα μπορούσαν να χρησιμοποιηθούν και για bankcard και για τις προπληρωμένες λειτουργίες χρεωστικών καρτών. Επιπλέον, επειδή η έξυπνη κάρτα είναι εύκολα φορητή [Gemplus9801], θα μπορούσε να χρησιμοποιηθεί και για online και για offline πληρωμή.

Στον τομέα του ηλεκτρονικού εμπορίου, οι έξυπνες κάρτες μπορούν να χρησιμοποιηθούν για την αποθήκευση και την προστασία διάφορων κλειδιών [Gemplus9801]. Με τη χρήση της έξυπνης κάρτας για την πληρωμή μέσω του Διαδικτύου, ο κίνδυνος ασφάλειας θα μπορούσε να μειωθεί όπως κάθε συναλλαγή θεωρείται μεμονωμένο γεγονός. Επιπλέον, ακόμα κι αν μια ιδιαίτερη έξυπνη κάρτα χαράσσεται, ο απολογισμός χρηστών θα είναι ακόμα ασφαλής.

Μαζί με τη χρήση του ψηφιακού πιστοποιητικού, οι τραπεζικοί λογαριασμοί θα μπορούσαν να αποτραπούν από την αναρμόδια

πρόσβαση και η ιδιωτικότητα και η ασφάλεια του χρήστη θα μπορούσαν να επιτευχθούν.

Αν και πολλοί προμηθευτές έχουν αναπτύξει την ηλεκτρονική λειτουργία πορτοφολιών στις έξυπνες κάρτες τους, είναι ασφαλέστερο να αποθηκευτεί κάθε μια μεταφόρτωσε την ηλεκτρονική αξία μετρητών ως σημείο στην κάρτα. Δεδομένου ότι κάθε σημείο έχει έναν αύξοντα αριθμό που πρωτόκολλο πληρωμής παράγεται από την τράπεζα, ακόμα κι αν το έξυπνων καρτών χαράσσεται, ο αύξων αριθμός του ηλεκτρονικού σημείου μπορεί να συλληφθεί και η ψεύτικη συναλλαγή μπορεί να προσδιοριστεί εύκολα [Chan1998]. Επιπλέον, με το ηλεκτρονικό συμβολικό σχέδιο, οι χρήστες μπορούν να ψωνίσουν ιδιαιτέρως στο δίκτυο χωρίς έκθεση της ταυτότητάς τους.

Όταν η ηλεκτρονική πληρωμή γίνεται αποδεκτή ευρέως σε καθημερινές χρήσεις, οι συναλλαγές θα γίνονταν αποδοτικότερες. Μια ενιαία κάρτα θα μπορούσε να χρησιμοποιηθεί για τις διαφορετικές εφαρμογές Στο μέλλον, η έξυπνη κάρτα θα χρησιμοποιούταν για την πληρωμή στις διαφορετικές πτυχές. Θα μπορούσαν να χρησιμοποιηθούν και για bankcard και για τις προπληρωμένες λειτουργίες χρεωστικών καρτών. Επιπλέον, επειδή η έξυπνη κάρτα είναι εύκολα φορητή [Gemplus9801], θα μπορούσε να χρησιμοποιηθεί και για online και για offline πληρωμή.

Στον τομέα του ηλεκτρονικού εμπορίου, οι έξυπνες κάρτες μπορούν να χρησιμοποιηθούν για την αποθήκευση και την προστασία διάφορων κλειδιών [Gemplus9801]. Με τη χρήση της έξυπνης κάρτας για την πληρωμή μέσω του Διαδικτύου, ο κίνδυνος ασφάλειας θα μπορούσε να μειωθεί όπως κάθε συναλλαγή θεωρείται μεμονωμένο γεγονός. Επιπλέον, ακόμα κι αν μια ιδιαίτερη έξυπνη κάρτα χαράσσεται, ο απολογισμός χρηστών θα είναι ακόμα ασφαλής.

Μαζί με τη χρήση του ψηφιακού πιστοποιητικού, οι τραπεζικοί λογαριασμοί θα μπορούσαν να αποτραπούν από την αναρμόδια

πρόσβαση και η ιδιωτικότητα και η ασφάλεια του χρήστη θα μπορούσαν να επιτευχθούν.

Αν και πολλοί προμηθευτές έχουν αναπτύξει την ηλεκτρονική λειτουργία πορτοφολιών στις έξυπνες κάρτες τους, είναι ασφαλέστερο να αποθηκευτεί κάθε μια μεταφόρτωσε την ηλεκτρονική αξία μετρητών ως σημείο στην κάρτα. Δεδομένου ότι κάθε σημείο έχει έναν αύξοντα αριθμό που πρωτόκολλο πληρωμής παράγεται από την τράπεζα, ακόμα κι αν το έξυπνων καρτών χαράσσεται, ο αύξων αριθμός του ηλεκτρονικού σημείου μπορεί να συλληφθεί και η ψεύτικη συναλλαγή μπορεί να προσδιοριστεί εύκολα [Chan1998]. Επιπλέον, με το ηλεκτρονικό συμβολικό σχέδιο, οι χρήστες μπορούν να ψωνίσουν ιδιαιτέρως στο δίκτυο χωρίς έκθεση της ταυτότητάς τους.

Όταν η ηλεκτρονική πληρωμή γίνεται αποδεκτή ευρέως σε καθημερινές χρήσεις, οι συναλλαγές θα γίνονταν αποδοτικότερες. Μια ενιαία κάρτα θα μπορούσε να χρησιμοποιηθεί για τις διαφορετικές εφαρμογές.

5.7.4 Ηλεκτρονική Πληρωμή στις Κινητές Τηλεπικοινωνίες

Οι δύο κύριες κατευθυντήριες δυνάμεις (εφαρμογές τη βιομηχανία) για έξυπνων καρτών είναι ηλεκτρονικό εμπόριο και τηλεπικοινωνίες. Όταν μια πολυσύνθετη έξυπνη κάρτα χρησιμοποιείται για λόγους τηλεπικοινωνιών, μπορεί επίσης να χρησιμοποιηθεί για να καλύψει τις σχετικές εφαρμογές ηλεκτρονικού εμπορίου. Αυτό επεκτείνει τη χρησιμότητα της κάρτας πέρα από την απλή τηλεφωνική κάρτα.

Στη Φινλανδία, ο PTT έχει αρχίσει ήδη μια πειραματική υπηρεσία με το οποίο οι καταναλωτές μπορούν να πληρώσουν στις αφύλακτες pos θέσεις χρησιμοποιώντας τα τηλέφωνα GSM τους. Οι δαπάνες προστίθενται απλά στον κινητό τηλεφωνικό λογαριασμό τους στο τέλος του μήνα [Birch1998].

Το ELab του Hyperion έχει συμπεριλάβει στη διαμόρφωση πρωτοτύπου μερικά στοιχεία του ανωτέρω σχεδίου [Birch1998]. Οι καταναλωτές που χρησιμοποιούν την υπηρεσία μπορούν να καταθέσουν και να αποσύρουν τα μετρητά από τους τραπεζικούς λογαριασμούς τους, και να αγοράσουν τα αγαθά και τις υπηρεσίες on-line. Οι συσκευές που χρησιμοποιούνται αυτήν την περίοδο στο σχέδιο περιλαμβάνουν αναγνώστες το GSM Communicator της Nokia, το Newton MessagePad και Windows PC, κάθε ένα που εγκαθίσταται με τους τυποποιημένους έξυπνων καρτών. Το σχέδιο χρησιμοποιεί αυτήν την περίοδο τα ηλεκτρονικά πορτοφόλια Proton και Mondex. Σε αυτό το πρωτόκολλο, που είναι παρόμοιο με το Open Trading Protocol (OTP), η πληρωμή πραγματοποιείται μεταξύ του καταναλωτικού ηλεκτρονικού πορτοφολιού και ενός κεντρικού υπολογιστή πληρωμής. Αφότου έχει λάβει ο κεντρικός υπολογιστής το ποσό πληρωμής, παράγει μια παραλαβή για τον έμπορο. Επομένως, ο έμπορος δεν χρειάζεται την αλλαγή το τρέχον λογισμικό του. Πρέπει μόνο να επεξεργαστεί την παραλαβή στο κανάλι επικοινωνίας τραπεζών.

Όταν το πολυσύνθετο ηλεκτρονικό πορτοφόλι αναπτύσσεται επιτυχώς στην κάρτα SIM, η ηλεκτρονική πληρωμή που χρησιμοποιεί το κανάλι κινητής επικοινωνίας θα γίνει ο μελλοντικός μηχανισμός συναλλαγής. Η Visa International προγραμματίζει επίσης να υιοθετήσει το ηλεκτρονικό σύστημα πληρωμής μέσω των καναλιών τηλεπικοινωνιών στην πλατφόρμα Visa της Open. Επομένως όταν η Java-based κάρτα Visa γίνεται ένα ενσωματωμένο συστατικό στην κάρτα SIM, η ηλεκτρονική πληρωμή θα μπορούσε να εκτελεσθεί μέσω του κινητού καναλιού τηλεπικοινωνιών [NewsEdge1998a].

5.8 Έξυπνες Κάρτες στην Ασφάλεια Διαδικτύου

Επειδή μια έξυπνη κάρτα μπορεί να περιλάβει τις πολύ ακριβείς πληροφορίες πρόσβασης για να προστατεύσει την ασφάλεια μυστικότητας και στοιχείων, οι έξυπνες κάρτες θα γίνουν μια όλο και περισσότερο ελκυστική εναλλακτική λύση για την πρόσβαση PC και

Διαδικτύου. Αυτή η εφαρμογή κάνει την έξυπνη κάρτα μια άμεση και ασφαλή επέκταση ενός δικτύου PC.

Στην περιοχή ασφάλειας συστημάτων, οι έξυπνες κάρτες μπορούν να χρησιμοποιηθούν για να φυλάξουν τα προσωπικά στοιχεία όπως ο κωδικός πρόσβασης σύνδεσης του χρήστη και άλλες συγκεκριμένες πληροφορίες χρηστών. Με τη χρήση μιας έξυπνης κάρτας, ο χρήστης δεν ειναι απαραίτητο να θυμηθεί τους κωδικούς πρόσβασης για τις διαφορετικές μηχανές επειδή όλοι οι κωδικοί πρόσβασης μπορούν να αποθηκευτούν σε μια ενιαία κάρτα. Με ένα κατάλληλο PIN για την έξυπνη κάρτα, ο χρήστης θα μπορούσε σύνδεση σε οποιοδήποτε συγκρότημα ηλεκτρονικών υπολογιστών.

Στην πλατφόρμα των WINDOWS NT 5.0, οι χρήστες μπορούν να χρησιμοποιήσουν τις έξυπνες κάρτες στη σύνδεση στο Personal τους Computer. Αυτό εξασφαλίζει ότι ένας χρήστης θα μπορούσε μόνο να έχει πρόσβαση σε ένα PC τη φορά. Εάν οι πληροφορίες παραμέτρων χρήστη αποθηκεύονται για την έξυπνη κάρτα, μπορεί ακόμη και σύνδεση οπουδήποτε στο δίκτυο με τις μοναδικές παραμέτρους χρήστη του/της. Επιπλέον, η πρόσβαση στην ασφαλείς βάση δεδομένων και τον κεντρικό υπολογιστή Διαδικτύου μπορεί να προστατευθεί με την χρήση της έξυπνης κάρτας. Οι διαδικασίες ανίχνευσης παρείσφρυσης μπορούν να γίνουν ευκολότερες.

Υπάρχουν διάφορες εφαρμογές για τις έξυπνες κάρτες στη σχετική με την ασφάλεια περιοχή. Θα εστιάσουμε στην ακόλουθη ταυτότητα Digital – τεσσάρων θεμάτων, τα συστήματα ανίχνευσης Computer Logon, Intrusion, και τις βιομετρικές επικυρώσεις.

5.8 .1 Έξυπνες Κάρτες ως Digital ID

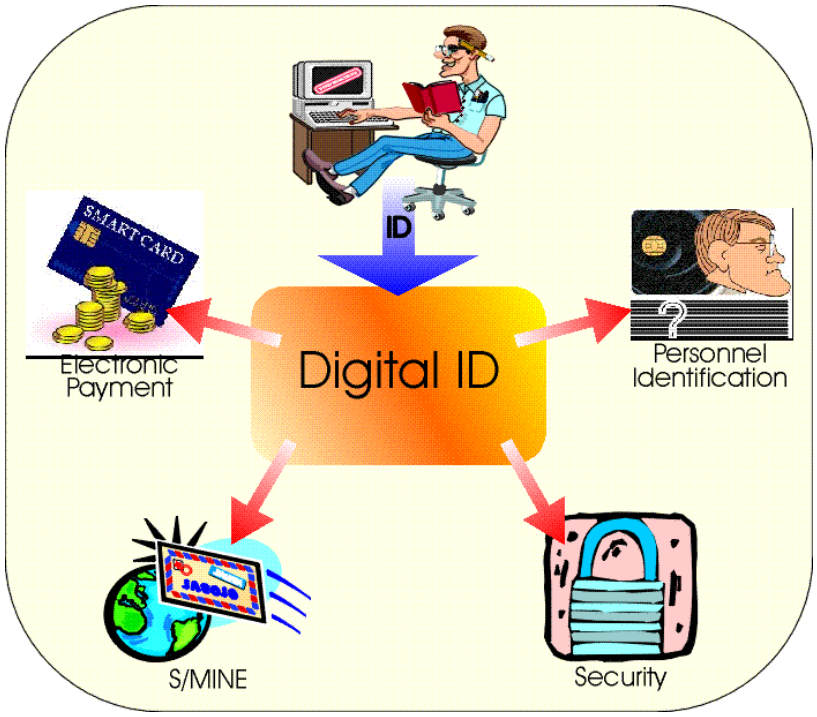
Ο προσδιορισμός και η εμπιστοσύνη είναι ένα ζωτικής σημασίας συστατικό στο ηλεκτρονικό εμπόριο. Για να κάνουν επιχειρήσεις on-line, οι άνθρωποι πρέπει να είναι σε θέση να καθιερώσουν την εμπιστοσύνη

με τα αντίστοιχά τους. Στο μελλοντικό τραπεζικό πρότυπο, εκτός από τα ασφαλή κανάλια συναλλαγής, το λογισμικό ψηφιακό IDs και το ασφαλές λογισμικό πληρωμής απαιτούνται επίσης. Σύμφωνα με μια έκθεση που δίνεται από Newsbytes News το δίκτυο τον Νοέμβριο του 1997, η απάτη Διαδικτύου έχει αυξηθεί κατά 300% κατά τη διάρκεια του περασμένου χρόνου. Ένας από τους κύριους λόγους για αυτήν την αύξηση είναι χρήστες είναι ανίκανος να προσδιορίσει θετικά τις ταυτότητες των αντίστοιχών τους. Εάν οι καταναλωτές μπορούν να είναι βέβαιοι για την ταυτότητα των αντίστοιχών τους και να έχουν έναν γρήγορο και απλό τρόπο τα πιστοποιητικά τους έπειτα αυτό το είδος απατών θα μπορούσε να περιοριστεί. Τα ψηφιακά πιστοποιητικά έχουν εισαχθεί για την επίλυση αυτού του προβλήματος. Το ψηφιακό πιστοποιητικό είναι ένα αρχείο στοιχείων που περιέχει το δημόσιο κλειδί ενός ατόμου μαζί με άλλες πληροφορίες προσδιορισμού, συμπεριλαμβανομένου του ονόματος του ιδιοκτήτη, τα στοιχεία αύξοντος αριθμού του πιστοποιητικού και λήξης, και ενδεχομένως άλλες χρήστης-παρεχόμενες πληροφορίες. Επιπλέον, ένα ψηφιακό πιστοποιητικό περιέχει επίσης το όνομα και την ψηφιακή υπογραφή της αρχής (CA) πιστοποίησης που εξέδωσε το πιστοποιητικό. Η αρχή πιστοποίησης είναι έμπιστος τρίτος, όπως μια τράπεζα, μια κυβερνητική αντιπροσωπεία ή ένας εργοδότης που ελέγχουν την ταυτότητα του ιδιοκτήτη του πιστοποιητικού πρίν εκδώσουν το πιστοποιητικό [Gemplus1998f].

Στην πράξη, το δημόσιο κλειδί γίνεται εύκολα διαθέσιμο ενώ το ιδιωτικό κλειδί εξασφαλίζεται και προσιτός μόνο από το νόμιμο ιδιοκτήτη. Αυτά τα δημόσια και ιδιωτικά κλειδιά παράγονται συνήθως ανά τα ζευγάρια. Με άλλα λόγια, σε έναν ψηφιακό κάτοχο πιστοποιητικών θα δοθεί ένα ιδιωτικό και δημόσιο κλειδί. Με ένα ψηφιακό πιστοποιητικό, καθένα με την πρόσβαση στο ιδιωτικό κλειδί υποτίθεται ότι είχε τη νόμιμη ιδιοκτησία του πιστοποιητικού. Δεδομένου ότι το ιδιωτικό κλειδί είναι το σημαντικότερο συστατικό του ψηφιακού πιστοποιητικού, η προστασία του ιδιωτικού κλειδιού είναι η ενιαία σημαντικότερη πτυχή της χρησιμοποίησης των ψηφιακών

πιστοποιητικών. Όποτε το ιδιωτικό κλειδί εκτίθεται ή χάνεται, το ψηφιακό πιστοποιητικό θα έπρεπε να ακυρωθεί και ο νέος.

Η τρέχουσα ψηφιακή ταυτότητα παράγεται από μια αρχή πιστοποίησης όπως Verisign μέσω του Διαδικτύου. Αυτό το



Σχήμα 7-6. Μια γενική εικόνα στις ψηφιακές εφαρμογές ταυτότητας.

πιστοποιητικό αποθηκεύεται συνήθως στον υπολογιστή του χρήστη. Εντούτοις, επειδή το πιστοποιητικό κρατιέται στον υπολογιστή, ο χρήστης θα έχει τη δυσκολία σε χρησιμοποίηση του ίδιου προσδιορισμού στις διαφορετικές φυσικές θέσεις. Επιπλέον, δεδομένου ότι το πιστοποιητικό είναι ο προσωπικός προσδιορισμός του χρήστη, δεν πρέπει να είναι προσιτός από άλλους χρήστες. Όλο και περισσότεροι υπολογιστές σχεδιάζονται για να υποστηρίξουν τους πολλαπλάσιους χρήστες, και όλο και περισσότεροι υπολογιστές συνδέονται μόνιμα με το Διαδίκτυο. Επομένως το πιστοποιητικό που κρατήθηκε σε έναν

υπολογιστή θα μπορούσε να προσεγγιστεί από άλλους χρήστες. Ακόμη και με το σκληρότερο να υποθέσει τον κωδικό πρόσβασης, το πιστοποιητικό θα μπορούσε να ληφθεί με να αντιγράψει τον άμεσα από το σκληρό δίσκο.

Για να προστατεύσουν αυτό το ψηφιακό πιστοποιητικό, οι χρήστες θα μπορούσαν να χρησιμοποιήσουν την έξυπνη κάρτα για να κρατήσουν αυτήν την ψηφιακή ταυτότητα [DigiCash1994, DigiCash1996]. Οι έξυπνες κάρτες υιοθετούνται ευρέως ως βασικό συστατικό στο ηλεκτρονικό εμπόριο επειδή παρέχουν τα ασφαλή, φορητά και προσωπικά μέσα να μεταφέρουν και να χρησιμοποιήσουν τα κρυπτογραφικά κλειδιά στη μαζική αγορά. Συνήθως, οι κρυπτογραφικές έξυπνες κάρτες όπως η κάρτα Cryptoflex Schlumberger και η κάρτα GemSafe Gemplus χρησιμοποιούνται.

Οι πειραματικές δοκιμές πραγματοποιήθηκαν από Verisign και Schlumberger τις 1998, Ιανουαρίου κατηγορία 1 Verisign ψηφιακό IDs μπορεί να διανεμηθεί και να μεταφορτωθεί στις κάρτες Cryptoflex. Μπορεί επίσης να χρησιμοποιηθεί για την πρόσβαση Διαδικτύου με τη Microsoft ΔΗΛ. και τον ξεφυλλιστή Netscape.

Δεδομένου ότι το ηλεκτρονικό εμπόριο απαιτεί το ψηφιακό πιστοποιητικό για την επικύρωση, οι έξυπνες κάρτες μπορούν να εκδοθούν για αυτήν την εφαρμογή. Προαγμένος από τη Microsoft, την IBM/το Lotus και Netscape, S/MIME, που χρησιμοποιεί ψηφιακό IDs για την επικύρωση, έχει υιοθετηθεί ως μια από τις επιλογές για το ασφαλές μήνυμα. Με τη χρήση του ψηφιακού πιστοποιητικού σε μια έξυπνη κάρτα, ο χρήστης μπορεί να χρησιμοποιήσει τον τυποποιημένο browser Ιστού για να υπογράψει ψηφιακά τις μορφές HTML ή το ηλεκτρονικό ταχυδρομείο.

Το ψηφιακό πιστοποιητικό σε μια έξυπνη κάρτα είναι όχι μόνο μια κάρτα για την επικύρωση στον κυβερνοχώρο. Με τα ψηφιακά πιστοποιητικά που κρατήθηκαν στην έξυπνη κάρτα, οι άνθρωποι θα μπορούσαν να έχουν πρόσβαση στα διάφορα συστήματα διοικητικών πληροφοριών μέσω οποιουδήποτε κατάλληλα εξοπλισμένου τερματικού

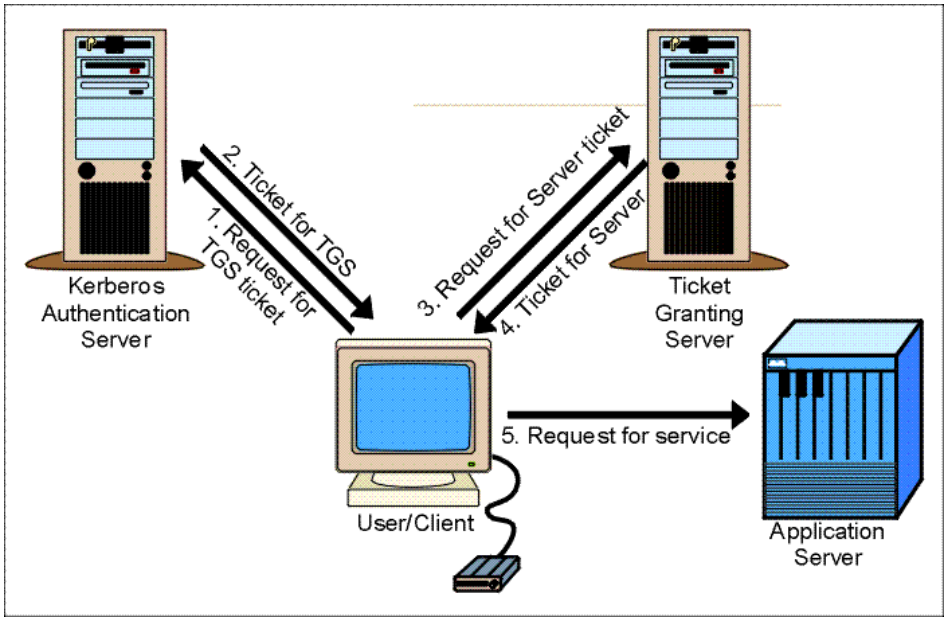
Διαδικτύου [Birch1998, DigiCash1994, DigiCash1996]. Το ψηφιακό πιστοποιητικό σε μια έξυπνη κάρτα θεωρείται για να χρησιμοποιηθεί ευρέως στο μέλλον.

Ο προσδιορισμός στο διαδίκτυο είναι πολύ σημαντικός. Τα ψηφιακά πιστοποιητικά επιτρέπουν στις οργανώσεις και τα άτομα για να επικοινωνήσουν ασφαλώς (χρησιμοποιώντας την κρυπτογράφηση) πέρα από τα untrusted δίκτυα και να επικυρώσουν τα μακρινά αντίστοιχά τους. Επομένως, με την αναμενόμενη διαδεδομένη υιοθέτηση του ηλεκτρονικού εμπορίου στο μέλλον, ψηφιακό IDs θα γίνει οι προσωπικές πληροφορίες ταυτότητας και οι έξυπνες κάρτες θα γίνουν οι ψηφιακές κάρτες ταυτότητας.

5.8.2 Έξυπνες Κάρτες ως Computer access logon key

Τον Μάρτιο του 1997, το Hewlett-Packard, λογισμικό Informix και Gemplus κατέδειξαν μια από κοινού αναπτυγμένη εταιρική επιχειρησιακή κάρτα ασφάλειας ενδοδικτύου και Διαδικτύου. Αυτή η κάρτα χρησιμοποιείται για την ασφάλεια Ιστού και την ασφάλεια πρόσβασης Διαδικτύου.

Στο σχέδιο PC/SC της Microsoft, τις λειτουργίες μια από της έξυπνης



κάρτας είναι ως ασφαλής αποθήκευση για τα ψηφιακά πιστοποιητικά.

Επιπλέον, η Microsoft έχει εισαγάγει επίσης τις έξυπνες κάρτες στο τους **G**raphical **I**dentification a**N**d **A**uthentication (GINA) σύστημα. Με αυτόν τον μηχανισμό σύνδεσης, η έξυπνη κάρτα χρησιμοποιείται ως κλειδί για τη διαδικασία επικύρωσης σύνδεσης υπολογιστών. Οι κατάλογοι ελέγχου πρόσβασης και οι πληροφορίες άδειας των ιδιαίτερων χρηστών ανακτώνται από την κάρτα και τον κεντρικό υπολογιστή Kerberos.

Με αυτό το σύστημα επικύρωσης σύνδεσης παραθύρων της Microsoft, η ταυτότητα του χρήστη, που είναι βασισμένη στο ψηφιακό πιστοποιητικό, κρατιέται μέσα στην κάρτα. Χρησιμοποιώντας την αρχή πιστοποίησης στη Microsoft WINDOWS NT 5.0, μια ψηφιακή ταυτότητα θα διανεμηθεί και θα σταλεί στην έξυπνη κάρτα. Για να επιτρέψουν αυτόν τον μηχανισμό, οι μηχανές της Microsoft WINDOWS NT αναγνώστη 5.0 πρέπει να διαμορφωθούν για να γνωρίζουν τον εγκατεστημένο έξυπνων καρτών. Η πλήρης τεκμηρίωση είναι διαθέσιμη "στην εγγραφή πιστοποιητικών έξυπνων καρτών" [Microsoft1998d].

Αυτή τη στιγνή, μόνο η Microsoft WINDOWS NT 5.0 σχέδιο επικύρωσης και παράθυρα 98 καρτών Αυτή τη έχει αυτό το ενσωματωμένο έξυπνων. Με την ανάπτυξη της GINA DLL που είναι έξυπνη κάρτα ενήμερη, μια έξυπνη κάρτα που περιέχει τα δημόσιος-βασικά πιστοποιητικά παίρνει τη λειτουργία μιας πιστοποιητικής κρύπτης που μπορεί να χρησιμοποιηθεί για να καταγράψει έναν χρήστη επάνω στις πολλαπλές περιοχές.

Περαιτέρω επεκτείνοντας αυτήν την ιδέα, οι έξυπνες κάρτες θα μπορούσαν να περιληφθούν στην επικύρωση πελατών πέρα από ένα ασφαλές πρωτόκολλο όπως το ασφαλές στρώμα υποδοχών (SSL) 3,0. Μετά από την ολοκλήρωση των τμημάτων έξυπνων καρτών επικύρωσης μέσα στον browser, μια έξυπνη κάρτα μπορεί να χρησιμοποιηθεί για να ενισχύσει τη διαδικασία επικύρωσης ως ασφαλές κατάστημα για ιδιωτικό το βασικό ή ακόμα και ως κρυπτογραφική μηχανή σε συνδυασμό με browser.

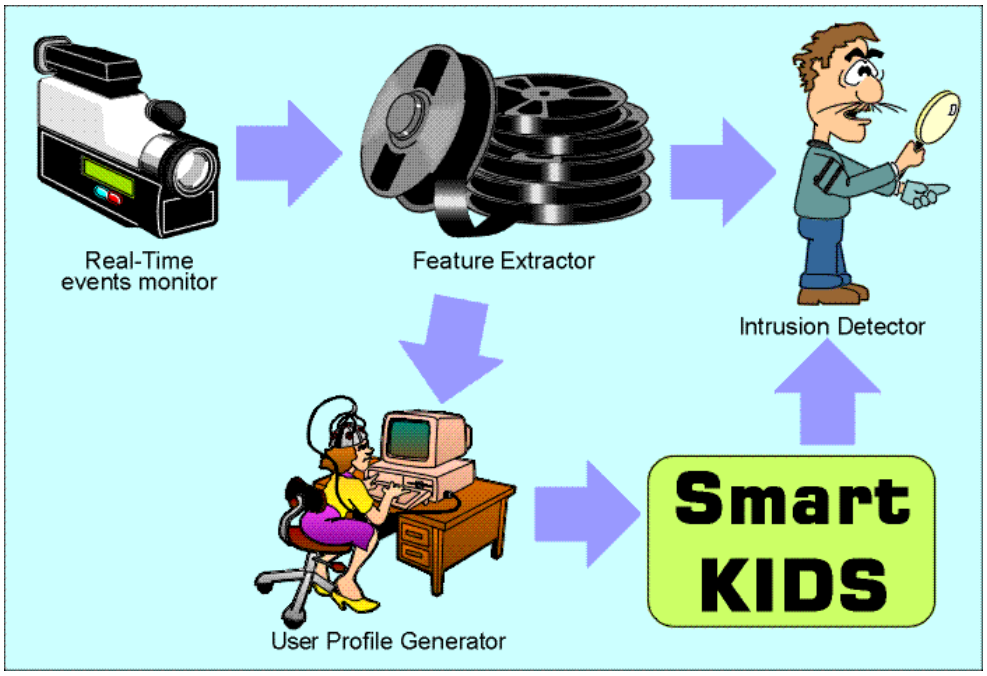
Κατά την άποψή μας, η έξυπνη κάρτα θα γίνει το κλειδί στον ενιαίο sign-on μηχανισμό. Στο μέλλον, οι χρήστες θα ήταν σε θέση να καταγράψουν επάνω στους πολλαπλάσιους κεντρικούς υπολογιστές με την ενιαία έξυπνη κάρτα.

5.8.3 Έξυπνες Κάρτες στο σύστημα ανίχνευσης παρείσφρυσης

Όλο και περισσότερες επιχειρήσεις χρησιμοποιούν Intranets και Extranets ως ασφαλή μέσα συναλλαγής τους. Αυτό αυξάνει την ανταγωνιστικότητα μιας επιχείρησης αφ' ενός αλλά προσελκύει τα misfeasors, τους μασκαρεμένους και τους μυστικούς χρήστες αφ' ετέρου.

Οι μελέτες για την ανίχνευση παρείσφρυσης [Pipkin1997, ISS, ISS1998, ήλιος] έχουν δείξει ότι οι περισσότεροι εισβολείς και χάκερ στους χώρους διαδικτύου ή τα επιχειρηματικά δίκτυα είναι μέλη εκείνων των περιοχών. Για να παλέψει ενάντια σε εκείνους τους εισβολείς, βασισμένη η στο χρήστης-σχεδιάγραμμα στατιστική ανίχνευση ανωμαλίας θα ήταν μια καταλληλότερη μέθοδος από την προσέγγιση ανίχνευσης κακής χρήσης, ειδικά μέσα σε ένα επιχειρηματικό δίκτυο. Εντούτοις, όπου τα χρήστης-σχεδιαγράμματα πρέπει αποθηκεύεται είναι ένα από τα κύρια προβλήματα. Αυτό το πρόβλημα θα γίνει πιό προεξέχον όταν περιλαμβάνεται ένα παγκόσμιο επιχειρηματικό δίκτυο. Εάν αυτά τα σχεδιαγράμματα αποθηκεύονται μόνο σε έναν εντοπισμένο κεντρικό υπολογιστή σχεδιαγράμματος περιοχών, όποτε ένας χρήστης πρέπει να έχει πρόσβαση στο δίκτυο επιχείρησης στα επιχειρησιακά ταξίδια, κάποιο θα πρέπει είτε να ζητήσει από το διοικητή δικτύων για να μεταφέρει το σχεδιάγραμμά κάποιου σε μια άλλη περιοχή είτε για να το φέρει σε άλλες

περιοχές από τους χρήστες οι ίδιοι. Η καλύτερη μέθοδος είναι να επιτραπούν οι χρήστες για να φέρει τα σχεδιαγράμματά τους με τους. Όπως χρήστης-σχεδιαγράμματα περιέχετε τα ευαίσθητα στοιχεία, πρέπει να αποθηκευτούν μέσα μιας στα ιδιαίτερα ασφαλή απομνημόνευσης, που κρατούν τους εισβολείς από στην πρόσβαση σε τους. Μια ο συχνότερα προτεινόμενη λύση είναι να υιοθετηθεί ο έξυπνος κάρτα ως ασφαλή μέσα απομνημόνευσησ [Gemplus1998 γ , Gemplus1998 δ, Gemplus1998 ε, SLB1998 α].



Σχήμα 7-8. Ένα απλό διάγραμμα των Smart KIDS.

με τη χρήση της τεχνολογίας έξυπνων καρτών, τα στοιχεία που κρατήθηκαν στην έξυπνη κάρτα θα μπορούσαν μόνο να προσεγγιστούν ή να τροποποιηθούν από τους εξουσιοδοτημένο χρήστες ή το σύστημα.

Εκτός αυτού, με την υπολογιστική δύναμη της κάρτας τσιπ, η κρυπτογράφηση και άλλες ασφαλείς διαδικασίες επικύρωσης θα μπορούσαν να εκτελεσθούν εξ ολοκλήρου στην κάρτα, καθιστώντας τα αποθηκευμένα στοιχεία ασφαλέστερα. Επίσης, με την εφαρμογή των προτύπων PC/SC έξυπνων καρτών, η έξυπνη κάρτα θα γίνει μια τυποποιημένη συσκευή στους προσωπικούς υπολογιστές καθώς επίσης και τους τερματικούς σταθμούς Unix. Επιπλέον, το σχέδιο επικύρωσης σύνδεσης υπολογιστών θα εφαρμοστεί σύντομα και θα χρησιμοποιηθεί στα συστήματα των WINDOWS NT, έτσι η χρήση της έξυπνης κάρτας βασισμένο στο στο χρήστης-σχεδιάγραμμα σύστημα ανίχνευσης παρείσφρυσης είναι μια λογική προβολή.

Σε ένα άρθρο που παρουσιάστηκε στο RAID 98 [Ieong1998b], προτείναμε αποκαλούμενα Smart KIDS τα έξυπνα κάρτα-βασισμένα παρείσφρυσης ανίχνευσης συστημάτων (για την προστασία ασφάλειας επιχειρηματικών δικτύων). Όταν ένας εξουσιοδοτημένος χρήστης με μια έγκυρη κάρτα έχει πρόσβαση σε οποιαδήποτε μηχανή σε αυτό το επιχειρηματικό δίκτυο, το σχέδιο ανίχνευσης παρείσφρυσης αρχίζει αυτόματα μετά από τη σύνδεση επικύρωσης που πετυχαίνουν. Μαζί με τις σχετικές με την επικύρωση προσωπικές πληροφορίες και σχετικά με τα την επιχείρηση προνόμια χρηστών που κρατιούνται στην κάρτα, η ασφάλεια συστημάτων μπορεί να επιβληθεί.

Επιπλέον, τις συγκεκριμένες προτιμήσεις χρηστών που αποθηκεύτηκαν με, οι προτιμήσεις χρηστών και η διαμόρφωση συστημάτων θα μπορούσαν να αποκατασταθούν μετά από τη διαδικασία σύνδεσης.

Όταν μια σύνδεση χρηστών σε μια μηχανή επιχειρηματικών δικτύων που χρησιμοποιεί αυτό το σχέδιο επικύρωσης, ό,τι πρέπει να κάνει πρόκειται να παρεμβάλει την Smart KIDS κάρτα του/της. Η διαδικασία επικύρωσης θα εκτελεσθεί αυτόματα και ο πράκτορας που κατοικεί σε εκείνη την μηχανή θα ορίσει έναν πίνακα δρομολόγησης από εκείνη την

μηχανή στις προορισμένες μηχανές και την πύλη δυναμικά σύμφωνα με τις πληροφορίες δικτύων που λαμβάνονται από την Smart KIDS κάρτα και τον κεντρικό υπολογιστή επικύρωσης. Αυτό ελέγχει τη δυνατότητα πρόσβασης του χρήστη βασισμένου στην ταυτότητα και τα δικαιώματά του/της. Οι συμπεριφορές του χρήστη συλλαμβάνονται και μαζί με το χρήστης-σχεδιάγραμμα στην και μαζί με το χρήστης-σχεδιάγραμμα στην Smart KIDS κάρτα, η συμπεριφορά "υπογραφή" ενός χρήστη παράγεται. Αυτή η υπογραφή παράγεται από το στατιστικό σύστημα ανίχνευσης ανωμαλίας που συνοψίζει τους χρόνους σύνδεσης και πρόσβασης χρηστών, τη συχνότερη θέση και τα αρχεία σύνδεσης, και την ταχύτητα πληκτρολόγησης. Επίσης, ο πράκτορας θα ελέγξει και θα παραγάγει τις επιφυλακές εάν οι ενέργειες του χρήστη υπερβούν το προνόμιο που έχει δικαίωμα αυτός/αυτή. Σε περίπτωση αυστηρού συμβιβασμού, η μηχανή θα αποσυνδεθεί από το δίκτυο με να θέσει εκτός λειτουργίας του πίνακα δρομολόγησης.

Βασισμένη σε αυτόν τον τύπο συστήματος ανίχνευσης παρείσφρυσης, η έξυπνη κάρτα χρησιμοποιείται όχι μόνο ως μηχανισμός επικύρωσης, αλλά και ως βασικό συστατικό για την ανίχνευση χάκερ. κάρτα, η συμπεριφορά "υπογραφή" ενός χρήστη παράγεται. Αυτή η υπογραφή παράγεται από το στατιστικό σύστημα ανίχνευσης ανωμαλίας που συνοψίζει τους χρόνους σύνδεσης και πρόσβασης χρηστών, τη συχνότερη θέση και τα αρχεία σύνδεσης, και την ταχύτητα πληκτρολόγησης. Επίσης, ο πράκτορας θα ελέγξει και θα παραγάγει τις επιφυλακές εάν οι ενέργειες του χρήστη υπερβούν το προνόμιο που έχει δικαίωμα αυτός/αυτή. Σε περίπτωση αυστηρού συμβιβασμού, η μηχανή θα αποσυνδεθεί από το δίκτυο με να θέσει εκτός λειτουργίας του πίνακα δρομολόγησης.

Βασισμένη σε αυτόν τον τύπο συστήματος ανίχνευσης παρείσφρυσης, η έξυπνη κάρτα χρησιμοποιείται όχι μόνο ως μηχανισμός επικύρωσης, αλλά και ως βασικό συστατικό για την ανίχνευση χάκερ.

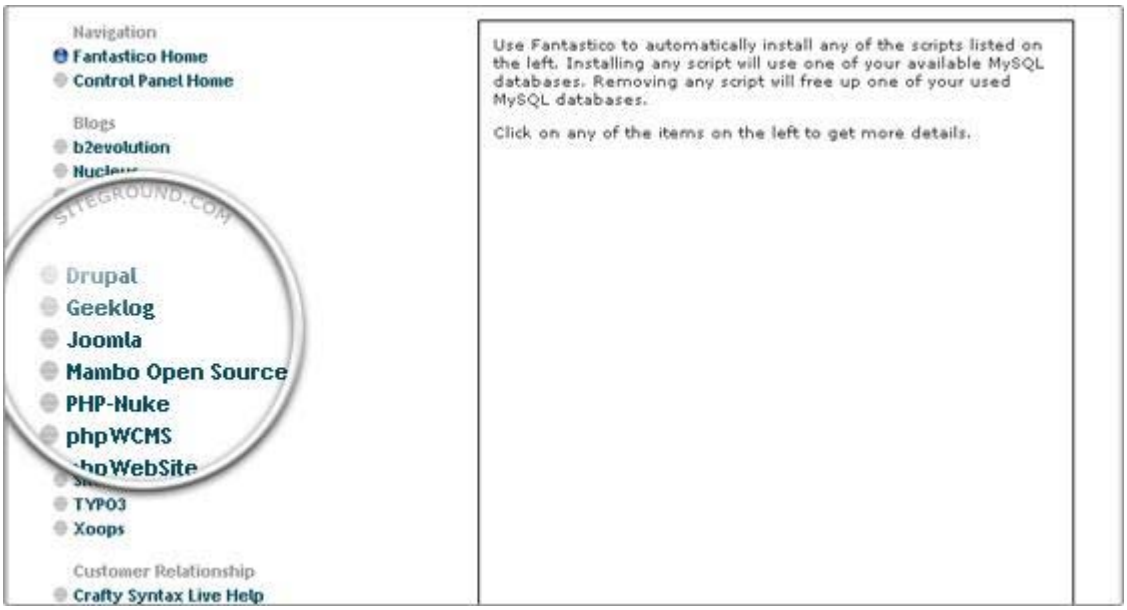
ΠΑΡΑΡΤΗΜΑ

ΠΡΑΚΤΙΚΟ ΜΕΡΟΣ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

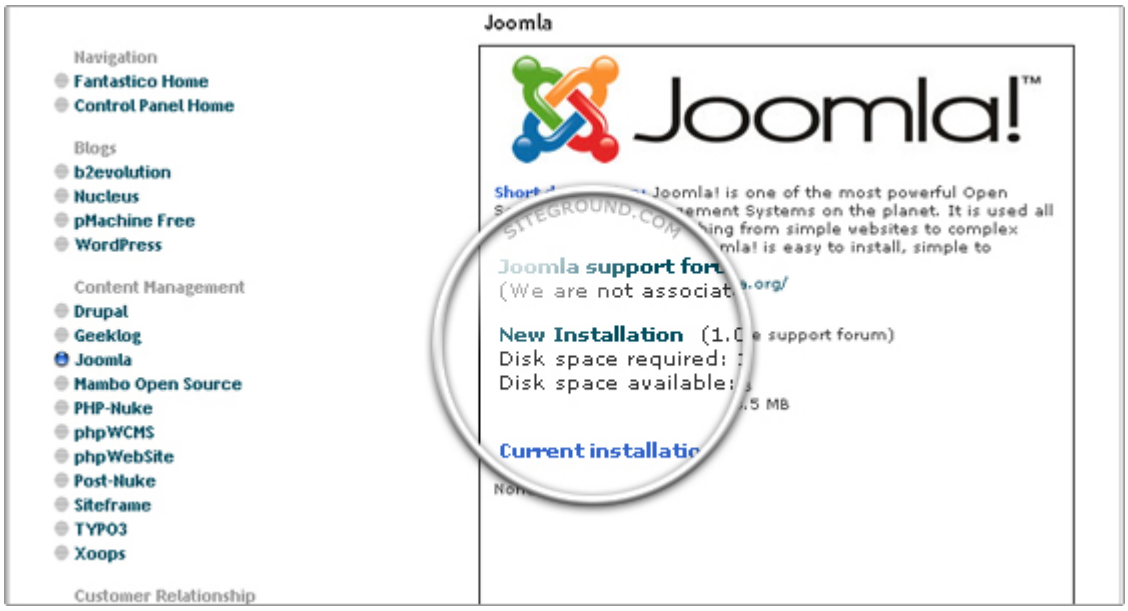
1.2 Πώς να εγκαταστήσεται το Joomla CMS με Fantastico

Προκειμένου να εγκατασταθεί Joomla CMS με Fantastico κανετε login στο cpanel σας και κάνετε κλικ στην μπλε εικόνα smiley ( ) στο κατώτατο σημείο της σελίδας.

Επιλέγετε το Joomla "από τον κατάλογο επιλογών σχετικά με την αριστερή πλευρά



και χτυπήστε **στη νέα εγκατάσταση**.



Θα παρουσιαστεί με μια μορφή που ζητά όλες τις απαραίτητες πληροφορίες για το μελλοντικό ιστοχώρο Joomla σας.
Εξήγηση μορφής:

- **Εγκαταστήστε στον κατάλογο** - αυτό καθορίζει τη διεύθυνση όπου η εγκατάσταση Joomla σας θα είναι προσιτή. Εάν θέλετε να χρησιμοποιήσετε Joomla για την αρχική σελίδα σας, αφήστε ακριβώς αυτό το κενό τομέων.
- **Στοιχεία πρόσβασης Admin** - το όνομα χρήστη και ο κωδικός πρόσβασης για την πρόσβαση της επιτροπής διοίκησης της εγκατάστασης Joomla σας.
- **Ηλεκτρονικό ταχυδρομείο Admin διαμόρφωσης βάσεων** - η διεύθυνση ηλεκτρονικού ταχυδρομείου σας
- **Πλήρες όνομα Admin** - το πλήρες όνομά σας
- **Όνομα περιοχών** - το όνομα του ιστοχώρου σας που θα επιδειχθεί στην μπροστινή σελίδα

Μόλις συμπληρώσετε τη φόρμα, παρακαλώ κάνετε κλικ "Install Joomla" button Θα κληθείτε να επιβεβαιώσετε την εγκατάσταση στην επόμενη σελίδα. Τέλος, παίρνετε μια σελίδα που σας ενημερώνει για μια επιτυχή εγκατάσταση.

SYSTEM REQUIRMENTS AND DOWNLOAD INSTRUCTIONS MANUAL INSTALL FOR JOOMLA

(χειροκίνητη εγκατάσταση)

Οι απαιτήσεις συστημάτων για Joomla 1,5 είναι:

- Apache 1.x ή 2.x
- 4,3 Πέσος Φιλιππίνων ή ανωτέρω
- MySQL 3,23 ή ανωτέρω
- Για τις τοπικές δοκιμές στον υπολογιστή σας, μπορείτε να χρησιμοποιήσετε Συσκευασία WAMP.

Ακολουθήστε τα βήματα κατωτέρω:

»Το βήμα 1. δημιουργεί μια βάση δεδομένων Mysql και προσθέτει έναν χρήστη σε την. Αυτό μπορεί να γίνει εύκολα με Cpanel με χρήση MySQL σεμινάριο βάσεων δεδομένων.

Σε περίπτωση που δεν χρησιμοποιείτε Cpanel αναφερθείτε στο εγχειρίδιο MySQL στη δημιουργία των βάσεων δεδομένων και την προσθήκη των χρηστών

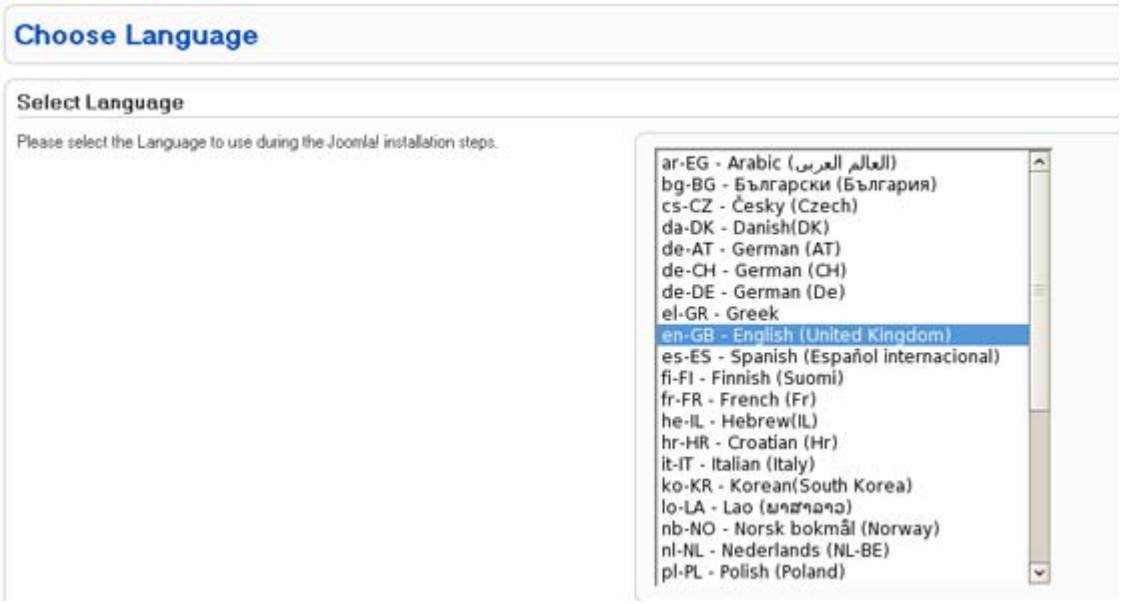
»Το βήμα 2. έπειτα στον υπολογιστή γραφείου σας και δημιουργεί έναν φάκελλο αποκαλούμενο install.

»Το βήμα 3. Το Joomla μεταφορτώνει τη σελίδα. Μεταφορτώστε το αρχείο zip **φορτώνει** το φάκελλο και τον εξάγει εκεί.

»Το βήμα 4. φορτώνει όλο το περιεχόμενο στον κατάλογο στον κεντρικό υπολογιστή όπου Joomla 1,5 θα εγκατασταθεί. Το SiteGround στήνει το FTP για αυτόν το λόγο και Το σεμινάριο FTP θα σας καθοδηγήσει μέσω των απαραίτητων βημάτων.

»Το βήμα 5. ανοίγετε το URL των πρόσφατα φορτωμένων αρχείων Joomla. Αυτό θα είναι είτε http://your_domain_name.com είτε ένα subdirectory όπως http://your_domain_name.com/example.

»Βήμα 6. Θα αναπροσανατολιστείτε στη σελίδα εγκαταστάσεων Joomla:



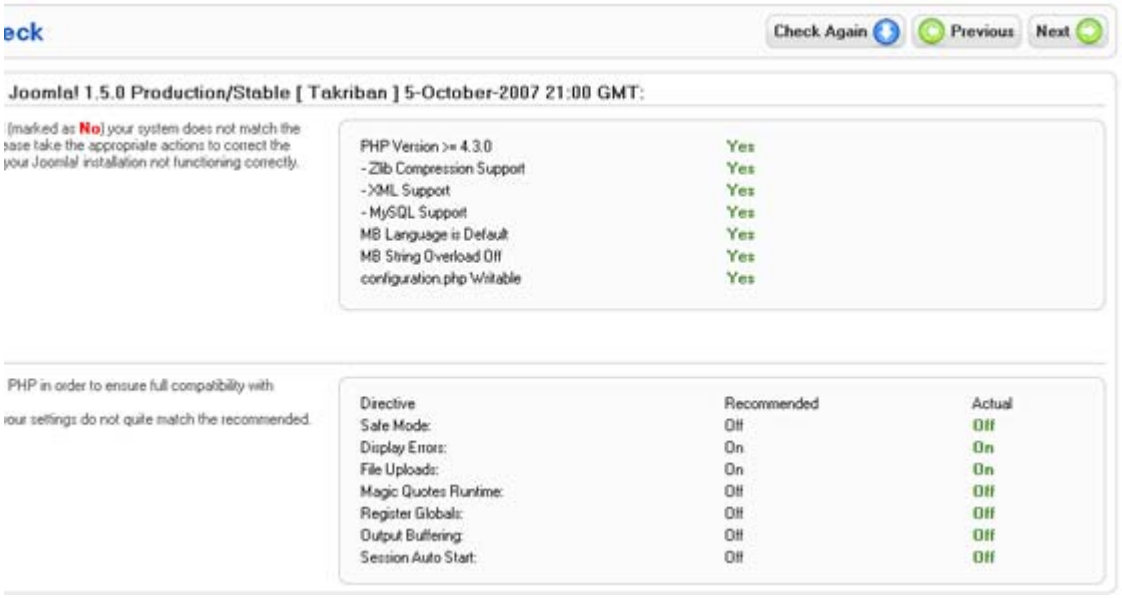
Στην πρώτη σελίδα της εγκατάστασης θα είστε σε θέση να επιλέξετε τη **γλώσσα** για την εγκατάσταση.

Η επιλεγμένη γλώσσα θα ισχύσει μόνο για τη διαδικασία εγκαταστάσεων. Μόλις εγκατασταθεί Joomla θα είναι πίσω στα αγγλικά.

Συστήνουμε "τα αγγλικά" προκειμένου να ακολουθηθούν ευκολότερος τα επόμενα βήματα από το σεμινάριο.

»Το βήμα 7. το Joomla θα εκτελέσει έναν έλεγχο προ-εγκαταστάσεων για το περιβάλλον συστημάτων. Η αποτυχία να καλυφθεί μια απαίτηση ή μια σύσταση μπορεί να προκαλέσει λειτουργικά προβλήματα και προβλήματα ασφάλειας αργότερα.

Εδώ είναι ένα screenshot όλου του Joomla 1,5 απαιτήσεις που καλύπτονται σε έναν τυποποιημένο απολογισμό φιλοξενίας SiteGround:

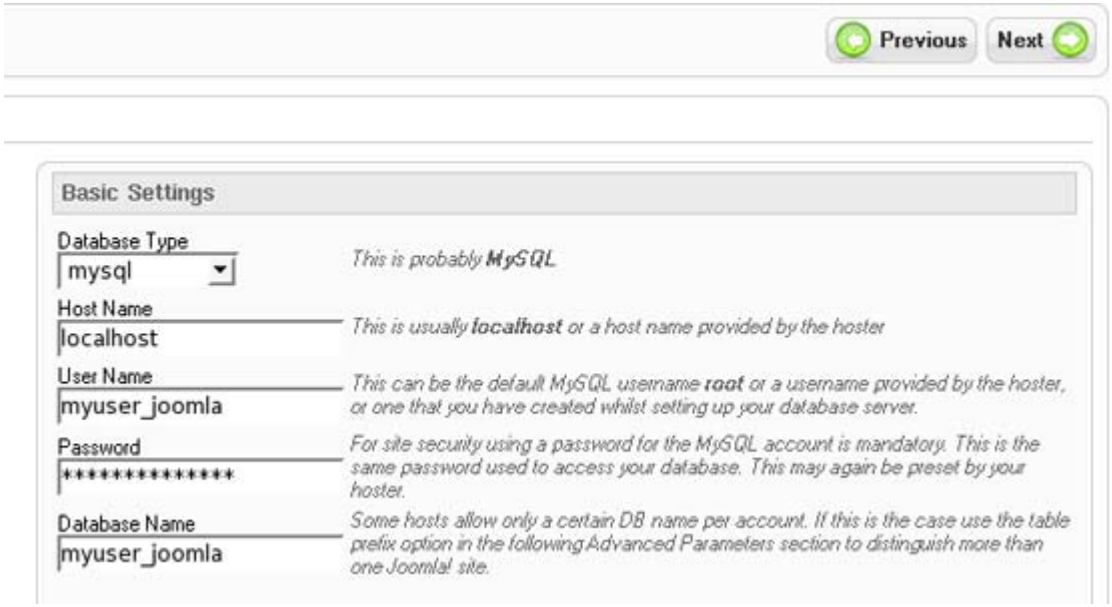


»Βήμα 8. Μόλις σιγουρευτείτε όλες οι απαιτήσεις καλύπτονται,κανετε κλίκ επάνω [**έπειτα**] από τις επιλογές κορυφαίου δικαιώματος.

»Το βήμα 9. έπειτα εσείς θα πρέπει να δεχτείτε την άδεια Joomla και να χτυπήσεται επάνω [**έπειτα**] για να συνεχιστεί.

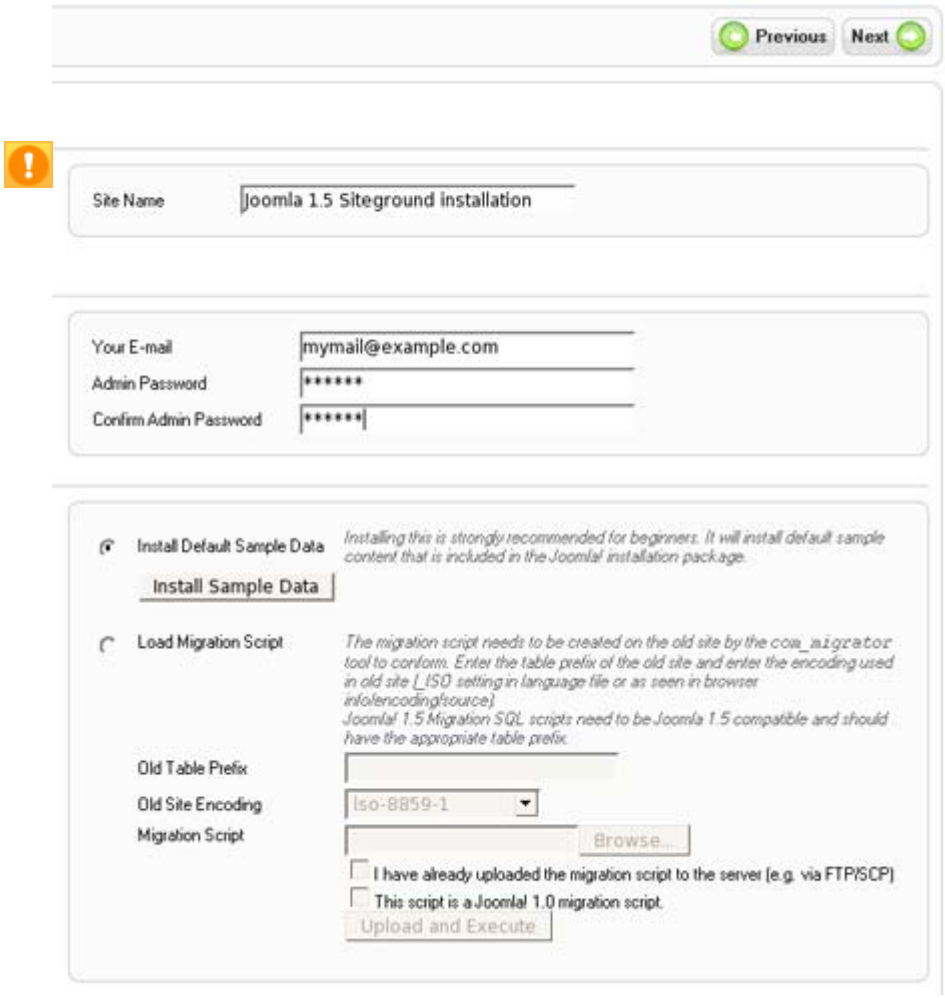
»Βήμα 10. Η ακόλουθη σελίδα θα ρωτήσει για τις λεπτομέρειες MySQL για το νέο Joomla 1,5 την εγκατάσταση.

Υπάρχουν εξηγήσεις για όλους τους τομείς σε περίπτωση που έχετε τις δυσκολίες με την παροχή των αναγκαίων πληροφοριών:



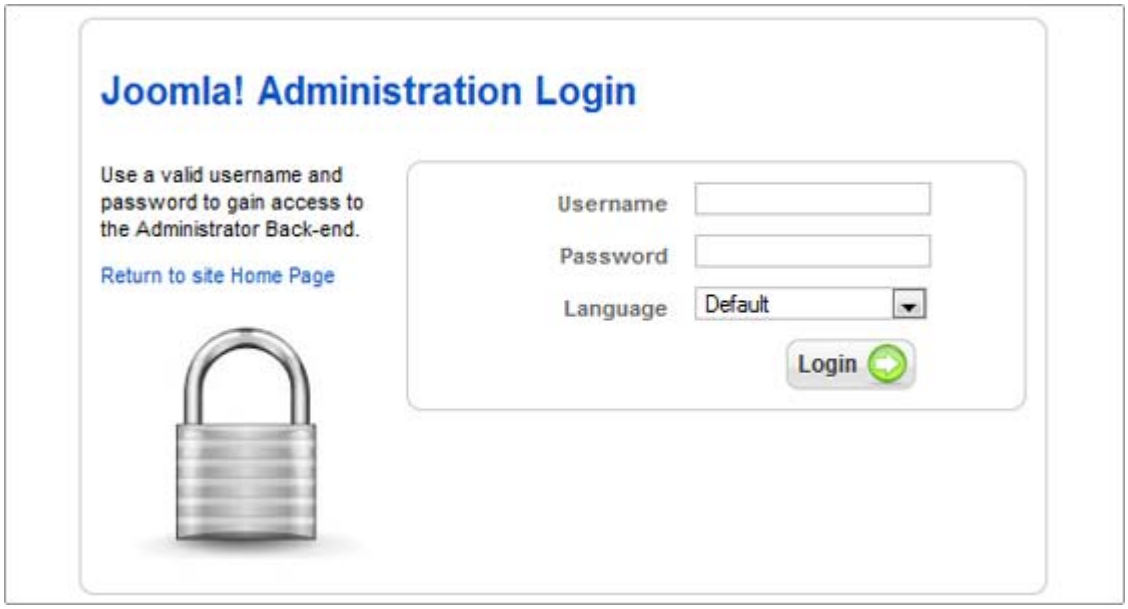
»Το βήμα 11, επόμενη οθόνη είναι για τη διαμόρφωση FTP.

»Βήμα 12. Από τη σελίδα που εμφανίζεται θα είστε σε θέση να ολοκληρώσετε το τελικό Joomla 1,5 τοποθετήσεις που διευκρινίζουν το ηλεκτρονικό ταχυδρομείο σας και που διευκρινίζουν τον κωδικό πρόσβασης admin. Χτυπήστε επάνω [**έπειτα**] για να σώσετε την πρόοδο.

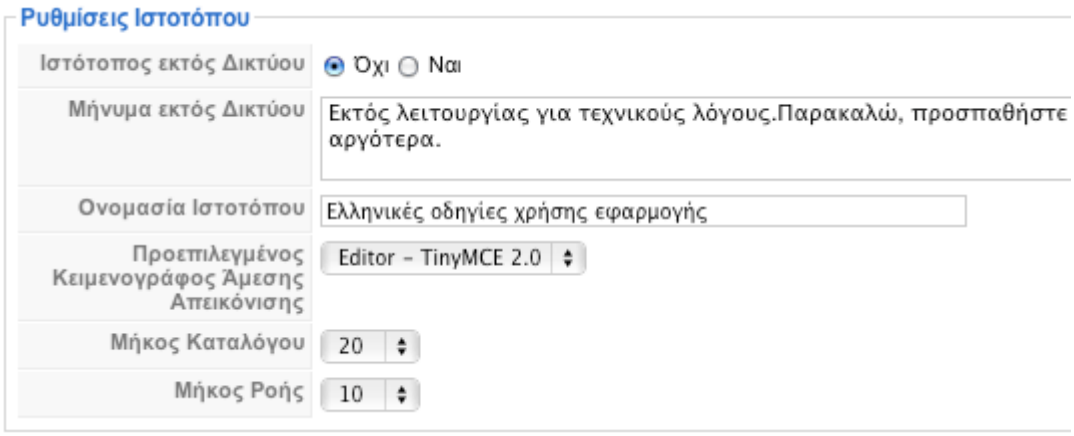


»Βήμα 13. Στην τελευταία σελίδα του wizard εγκαταστάσεων θα λάβετε μια επιβεβαίωση ότι Joomla έχει εγκατασταθεί επιτυχώς.

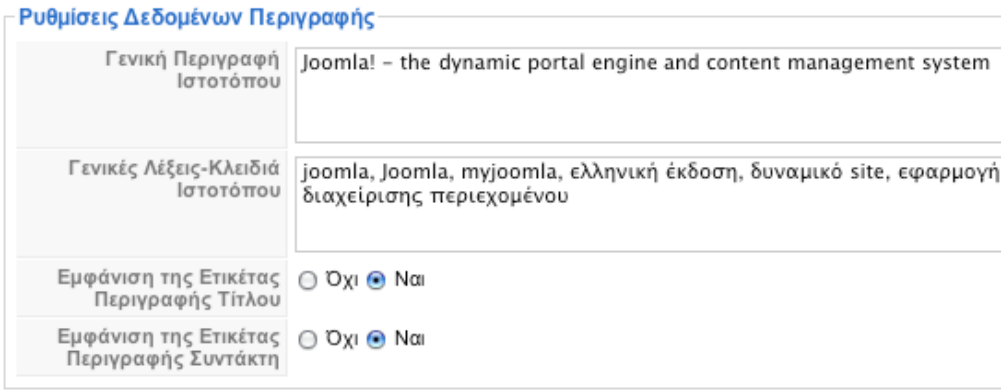
Πρίν είστε σε θέση να προσεγγιστεί το νέο Joomla σας 1,5 πρέπει να διαγράψετε τον κατάλογο **εγκαταστάσεων**.



Καλώς ηλθατε στη κεντρική σελίδα διαχείρισης του Joomla του.Μόλις κάνετε login θα βρεθείτε στη κεντρική διαχείρηση του Joomla Στη καρτέλα διαχείρισης Γενικών Ρυθμήσεων, υπάρχουν τρεις καρτέλες Ιστότοπος, όπου ρυθμήζεται η εμφάνιση και η διαθεσιμότητα του δικτυακού τόπου



Ρυθμίσεις Δεδομένων Περιγραφής

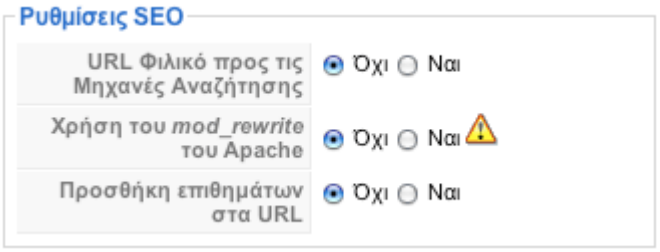


Γενική περιγραφή ιστοτόπου: αναζήτησης η περιγραφή που παssρνουν οι μηχανές

Γενικές Λέξεις-Κλειδιά Ιστοτόπου: (λέξεις κλειδιά) για αναζήτησης τις οι λέξεις-κλειδιά μηχανές

Εμφάνιση της Ετικέτας Περιγραφής Τίτλου: όταν προβάλλεται ένα κειμενο ετικεττών meta τίτλου εμφανίζει το όνομα της ετίκετας **Εμφάνιση της Ετικέτας Περιγραφής Συντάκτη:** όταν προβάλλεται ένα κείμενο ετικεττών meta συντακτών εμφανίζει το

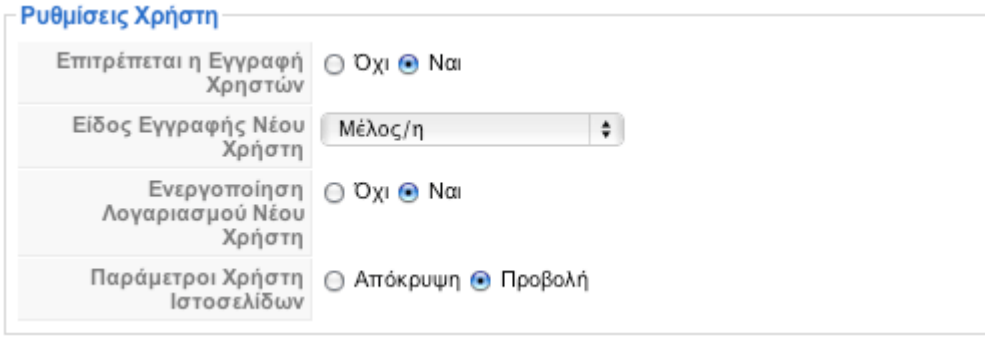
Ρυθμίσεις SEO

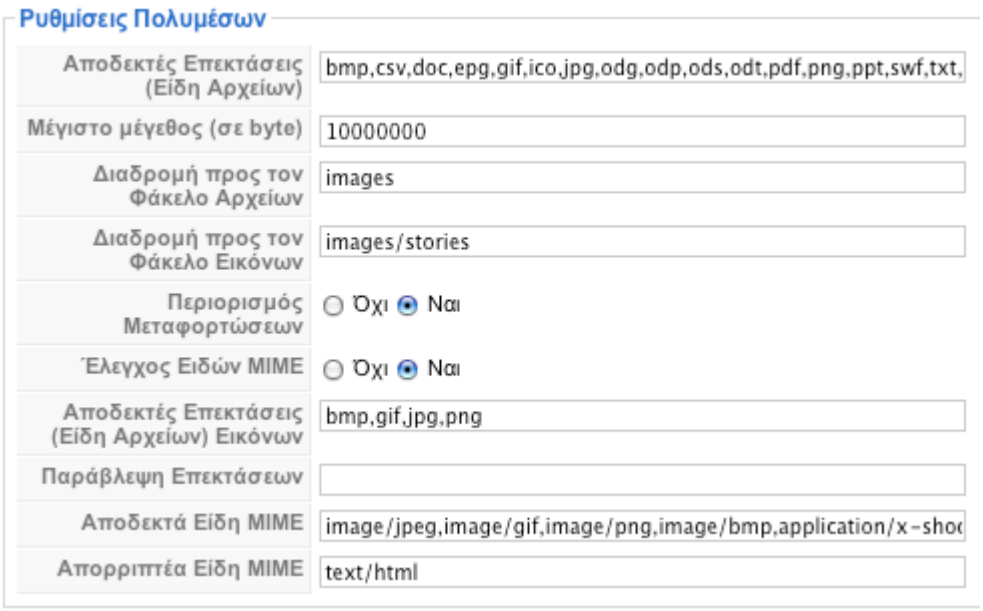


Τις Μηχανές Αναζήτησης προς URL Φιλικό: Αν επιλέξετε ναι, αλλάζει ο αναζήτησης μηχανών των κριτήρια βασικά τρόπος που παρουσιάζονται οι σύνδεσμοι στη μπάρα διεύθυνσης ενός φυλλομετρητή και οι διευθύνσεις βελτιστοποιούνται σύμφωνα με τα. Επσσσης, μορφή αριθμό του άρθρου, για παράδειγμα, εμφανσσζεται το ψευδώνυμο που έχουμε δώσει για τον Τσστλο τον γσσνεται φιλικότερη και αντσς για αύξοντα των η url.

Χρήση του mod_rewrite του Apache: Αναζήτησης διευθύνσεις τις μηχανές προς του δσσνει φιλικές κεντρικών υπολογιστών και προϋποθέτει τη μετονομασσσα του αρχεσσου htaccess.txt σε χταθθεσς Η ενεργοποσσησή μόνον δυνατότητα υπάρχει Αυτή η σε apache

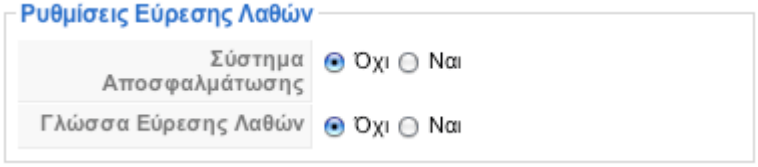
Προσθήκη επιθημάτων στα URL: Τυχόν ενεργοποσσηση, δσσνει κατάληξη χτμλ στις σελσσδες π οπυ παράγει το joomla!





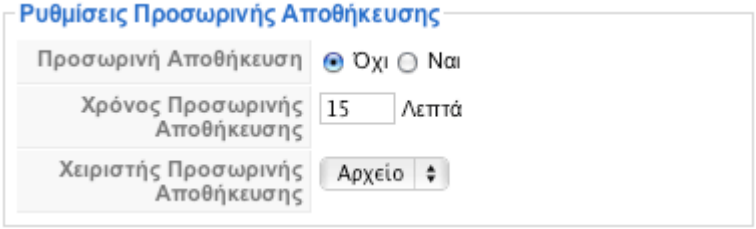
Αποδεκτές Επεκτάσεις (Είδη Αρχείων): επεκτάσεις αρχείων που γίνονται αποδεκτές για ανέβασμα στο joomla!
Μέγιστο μέγεθος (σε byte): το μέγιστο μέγεθος των αρχείων που μπορεί να μεταφορτωθεί.
Διαδρομή προς τον Φάκελο Αρχείων: ο φάκελος όπου αποθηκεύονται τα αρχεία (όχι οι φωτογραφίες) που ανεβάζετε στο server
Διαδρομή προς τον Φάκελο Εικόνων: ο φάκελος όπου αποθηκεύονται οι φωτογραφίες που ανεβάζετε στο server

Ρυθμίσεις Εύρεσης Λαθών



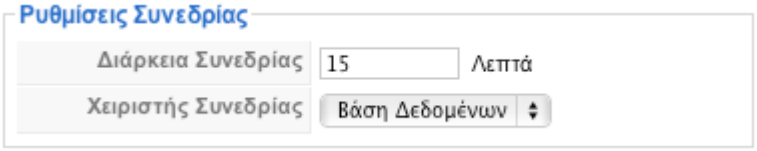
Χρησιμεύει όταν δημιουργείτε ένα δικτυακό ώστε να βλέπετε τα μηνύματα λάθους.

Ρυθμίσεις Προσωρινής Αποθήκευσης

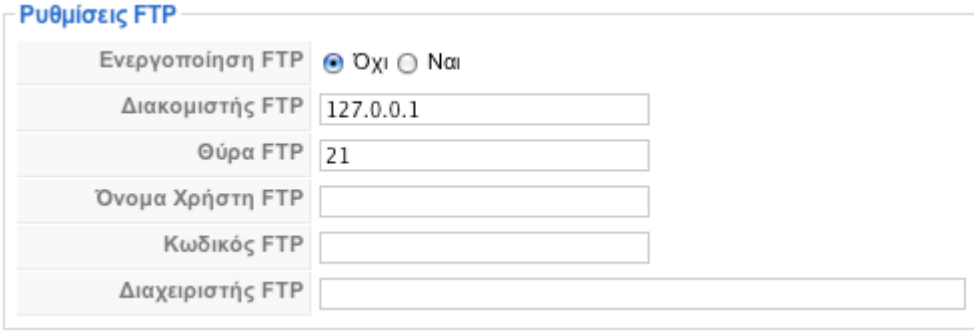


Ρυθμίσεις για την ενεργοποίηση ή όχι της προσωρινής αποθήκευσης των αρχείων, ώστε να εμφανίζονται ταχύτερα στον επισκέπτη. Στην πραγματικότητα αποθηκεύεται μια φωτογραφία της βάσης δεδομένων, η οποία και είναι διαθέσιμη στον επισκέπτη του δικτυακού σας τόπου.

Ρυθμίσεις Συνεδρίας



Ο χρόνος της συνεδρίας για κάθε χρήστη. Αν υπάρξει αδράνεια για διάστημα μεγαλύτερο του χρόνου που ορίζουμε, τότε ο χρήστης αυτόματα αποσυνδέεται.



Πρόκειται για πολύ χρήσιμη ρύθμιση. Δημιουργήστε έναν χρήστη ftp και δηλώστε τα στοιχεία του.

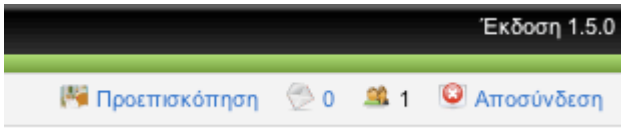
Πρόσβαση στη διαχείριση

Για να διαχειριστείτε την εγκατάσταση Joomla! πρέπει, μέσω ενός web browser, να επικεφθείτε τη διεύθυνση myjoomla_url_here/administrator (όπου myjoomla_url_here πληκτρολογείτε τη διεύθυνση όπου έχετε εγκαταστήσει το joomla!).

Στην οθόνη που θα σας εμφανισθεί χρειάζεται να δώσετε το **Ονομα Χρήστη** και τον **Κωδικό** σας, ώστε να συνδεθείτε. Είναι τα στοιχεία που πήρατε από την onScreen με την εγκατάσταση του Joomla! Μπορείτε επίσης να επιλέξετε και τη γλώσσα στην οποία θα εμφανίζονται τα μενού και οι λειτουργίες του πίνακα ελέγχου (στο παρόν κείμενο θεωρούμε ότι επιλέγεται η ελληνική γλώσσα).

Πίνακας Ελέγχου - η πρώτη εικόνα

Μετά από μια επιτυχή σύνδεση, έχετε στην οθόνη σας την αρχική σελίδα του πίνακα ελέγχου.



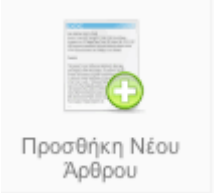
Στο πάνω δεξί μέρος της οθόνης, επιλέγοντας "**Προεπισκόπηση**",

μπορείτε να εμφανίσετε το δικτυακό σας τόπο σε ένα νέο παράθυρο του φυλομετρητή σας. Ακόμη πιο δεξιά, πατώντας "**Αποσύνδεση**", αποσυνδέεστε από το σύστημα διαχείρισης.

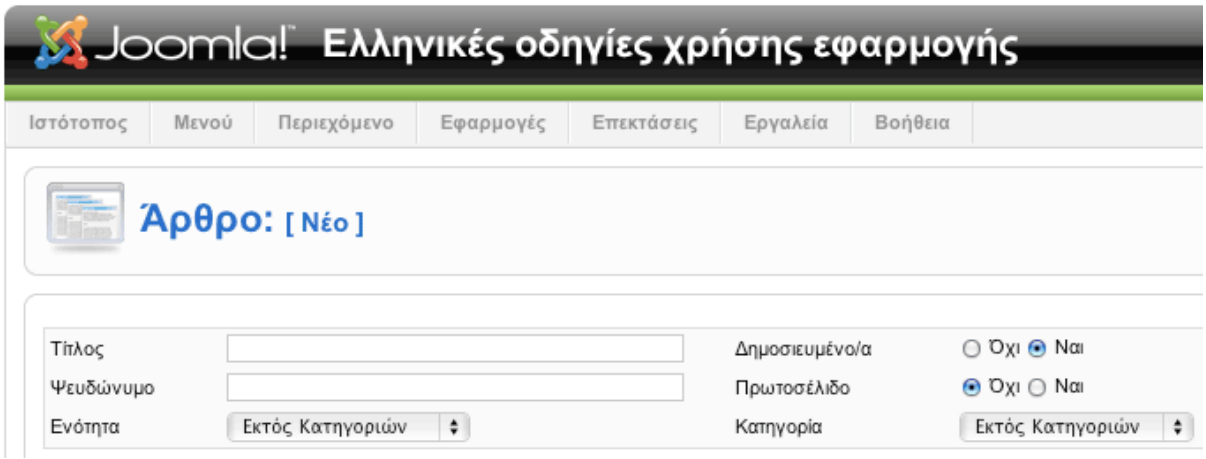
Οργάνωση του περιεχομένου

Το περιεχόμενο του δικτυακού σας τόπου αποτελείται, καταρχή, από κείμενα, που στο Joomla! ονομάζονται **άρθρα**. Τα άρθρα μπορούν είτε να ανήκουν σε μια συγκεκριμένη **κατηγορία**, η οποία με τη σειρά της ανήκει σε μια **ενότητα**, ή να είναι αυτόνομα, **εκτός κατηγοριών**.

Προσθήκη περιεχομένου



Ας δημιουργήσετε λοιπόν πρώτα άρθρο εκτός κατηγοριών. Στην κεντρική σελίδα της διαχείρισης, πατώντας του εικονίδιο **Προσθήκη Νέου Άρθρου**, εμφανίζεται η σχετική οθόνη.



Ας δείτε τα πεδία που πρέπει να συμπληρώσετε, προσεκτικά. **Τίτλος:** είναι ο τίτλος του άρθρου που θα δημιουργήσετε. Ο τίτλος αυτός θα φαίνεται στην αρχή του κειμένου στην ιστοσελίδα σας. **Ψευδώνυμο:** εδώ γράφετε ένα διακριτικό για τον τίτλο σας, κατά προτίμηση με λατινικούς χαρακτήρες. Το στοιχείο αυτό χρησιμεύει για

τη δημιουργία φιλικών για τις μηχανές αναζήτησης τίτλων στο δικτυακό σας τόπο.

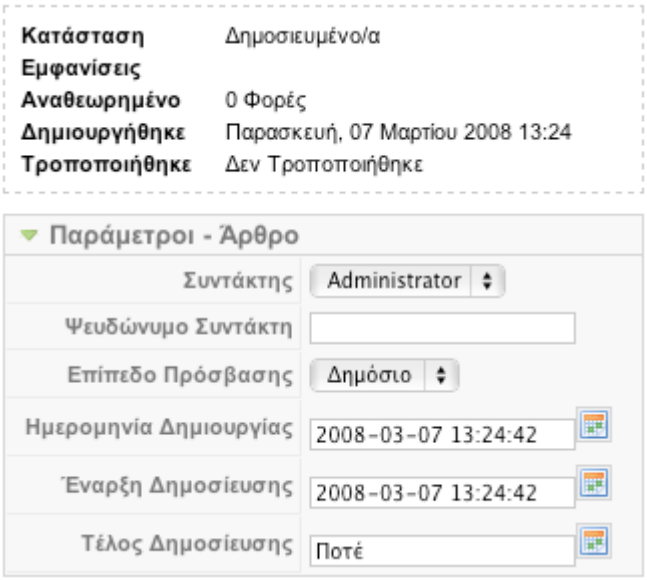
Ενότητα: στο σημείο αυτό ορίζετε σε ποια ενότητα θα ενταχθεί το άρθρο σας. Μόλις επιλέξετε την ενότητα, τότε δίπλα, στο πεδίο Κατηγορία εμφανίζονται οι κατηγορίες που ανήκουν στην ενότητα αυτή. Αν θέλετε να θα δημιουργήσετε ένα αυτόνομα κείμενο, επιλέγετε "Εκτός κατηγοριών".

Δημοσιευμένο/α: επιλέγετε αν το άρθρο που γράφετε είναι για δημοσίευση ή όχι.

Πρωτοσέλιδο: ορίζετε αν το άρθρο θα εμφανίζεται στο Πρωτοσέλιδο. Εδώ χρειάζετε η προσοχή σας: το Πρωτοσέλιδο δεν είναι αναγκαστικά η πρώτη σελίδα, αλλά είναι η σελίδα όπου χρησιμοποιείται το com_forntpage, όπου δηλαδή παρουσιάζονται περιεχόμενα με μορφή ιστολογίου.

Κατηγορία: επιλέγετε την κατηγορία στην οποία θα ενταχθεί το άρθρο. Στο συγκεκριμένο πεδίο εμφανίζονται μόνον οι διαθέσιμες κατηγορίες της ενότητας στην οποία έχετε εντάξει το άρθρο.

Κάτω από τα στοιχεία αυτά εμφανίζεται ο **επεξεργαστής κειμένου**, με τη βοήθεια του οποίου μπορείτε να συντάξετε το κείμενό σας. Οπως βλέπετε, αρκούν βασικές γνώσεις χρήσης κειμενογραφου.



Στο **δεξί τμήμα της οθόνης** εμφανίζονται κάποια στοχεία για το συγκεκριμένο άρθρο, καθώς και τρεις καρτέλες παραμετροποίησης. Δείτε προς το παρόν όσα στοιχεία αναφέρονται στην πρώτη καρτέλα:
Συντάκτης: είναι το μέλος της διαχείρισης που θα εμφανισθεί ως ο συντάκτης του άρθρου.
Ψευδώνυμο συντάκτη: εδώ γράφετε ό,τι θέλετε να εμφανισθεί, αν δεν σας καλύπτει το περιεχόμενο του μενού Συντάκτης
Επίπεδο Πρόσβασης: το πεδίο αυτό δέχεται τις παρακάτω τιμές:

- Δημόσιο, που σημαίνει πως το άρθρο είναι ορατό από κάθε επισκέπτη της ιστοσελίδας σας
- Μέλος/η, που σημαίνει ότι μπορούν να το διαβάσουν μόνον τα εγγεγραμμένα μέλη του δικτυακού σας τόπου
- Ειδικό, όταν θέλετε να είναι προσβάσιμο μόνον από τους διαχειριστές.

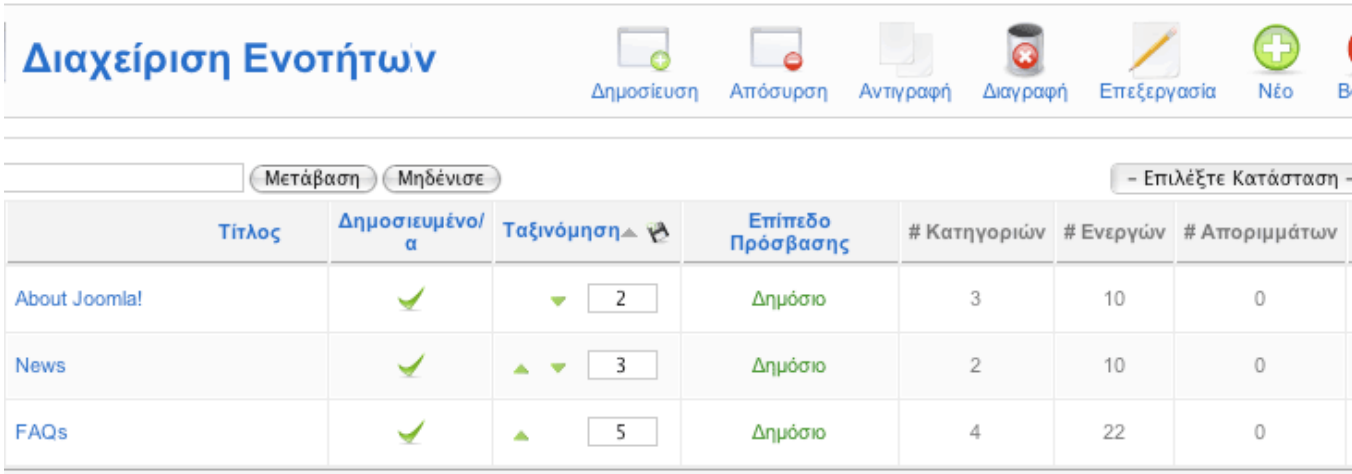
Ημερομηνία Δημιουργίας, είναι η ημερομηνία που συντάχθηκε το άρθρο.
Έναρξη Δημοσιεύσης: ορίζετε πότε θέλετε να ξεκινήσει η δημοσίευση του άρθρου
Τέλος Δημοσίευσης: ορίζετε πότε θα σταματήσει η δημοσίευση του άρθρου

Στο πάνω δεξί μέρος της οθόνης υπάρχει μια μπάρα εργαλείων, που σας επιτρέπει να διεκπεραιώσετε κάποιες εργασίες. Πιο συγκεκριμμένα:
Προεπισκόπηση: βλέπετε την εμφάνιση που θα έχει το άρθρο που συγγράφετε εκείνη τη στιγμή
Αποθήκευση: αποθηκεύετε τις αλλαγές και βγαίνετε από την οθόνη
Εφαρμογή: αποθηκεύετε τις αλλαγές και παραμένετε στην οθόνη
Ακύρωση: ακυρώνετε όσες αλλαγές δεν έχετε αποθηκεύσει
Βοήθεια: προσεγγίζετε τις οθόνες βοήθειας του joomla!

Ενότητες και Κατηγορίες

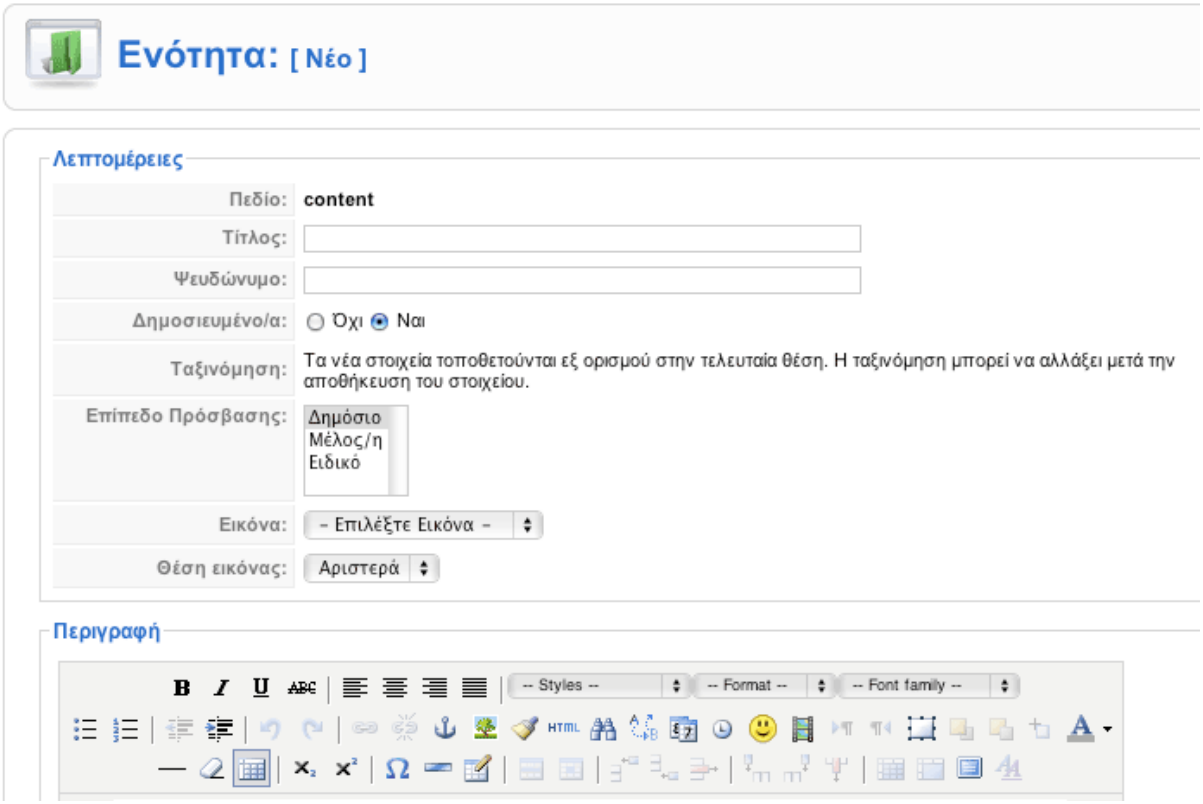
Η **δομή Ενότητα - Κατηγορία - Άρθρο** είναι ο τρόπος που το Joomla! οργανώνει το περιεχόμενο του δικτυακού τόπου. Το πλήθος των κατηγοριών δεν περιορίζεται, κάθε κατηγορία όμως πρέπει να ενήκει σε μια ενότητα. Και, αντίστοιχα, μπορούμε να έχετε όσες ενότητες χρειάζεστε. Από την άλλη πλευρά, όπως έχει ήδη αναφερθεί, τα άρθρα μπορούν είτε να ανήκουν στη δομή αυτή, σε μια κατηγορία δηλαδή, είτε να είναι αυτόνομα.

Για να δημιουργήσετε μια νέα Ενότητα, επιλέγετε, από την κεντρική σελίδα της διαχείρισης, το εικονίδιο **"Διαχείριση Ενοτήτων"**.



Στην οθόνη που εμφανίζεται παρουσιάζονται όλες οι ενότητες του

δικτυακού μας τόπου. Πατώντας το εικονίδιο **"Νέο"** στο πάνω δεξί μέρος της οθόνης, εμφανίζεται η οθόνη **δημιουργίας νέας ενότητας.**



Η εικόνα πρέπει να σας θυμίζει κάπως εκείνην της δημιουργίας νέου άρθρου.

Συμπληρώνετε με την ίδια λογική τα πεδία

Τίτλος

Ψευδώνυμο

Δημοσιευμένο/α

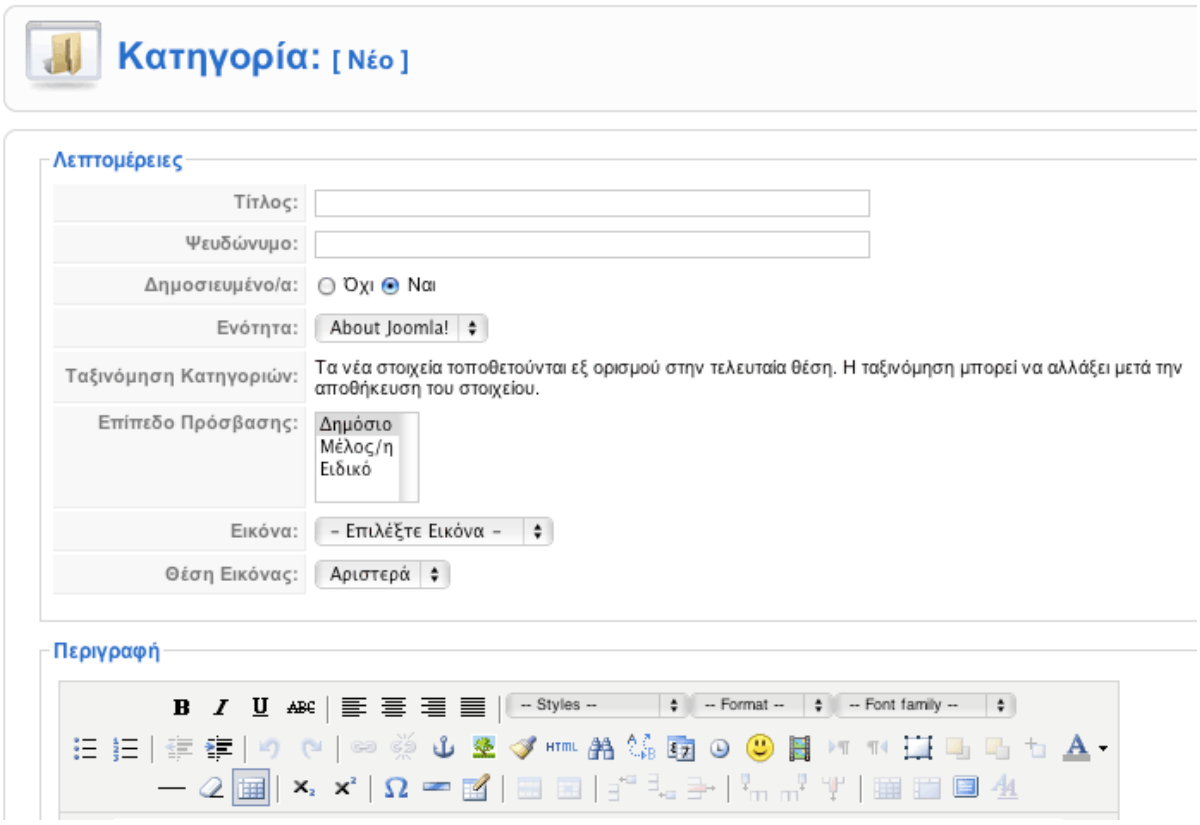
Επίπεδο πρόσβασης

Στο πεδίο **Εικόνα** προδιορίζετε, αν θέλετε, μια εικόνα που χαρακτηρίζει την ενότητα αυτή, και στο πεδίο **Θέση Εικόνας** ορίζετε τη θέση της.

Με τη βοήθεια του κειμενογράφου, δίνετε, αν θέλετε, την **περιγραφή** της ενότητας.

Πατώντας **Αποθήκευση**, ολοκληρώνετε και επιβεβαιώνετε τις αλλαγές αυτές. Μέσω του μενού Ιστότοπος > Πίνακας Ελέγχου, επιστρέφετε στη κεντρική σελίδα της διαχείρισης.

Μια ανάλογη διαδικασία ακολουθείτε **για να δημιουργήσετε μια νέα Κατηγορία.** Επιλέγετε, από την κεντρική σελίδα της διαχείρισης, το εικονίδιο **"Διαχείριση Κατηγοριών"**.
Στην οθόνη που εμφανίζεται παρουσιάζονται όλες οι κατηγορίες του δικτυακού μας τόπου. Πατώντας το εικονίδιο **"Νέο"** στο πάνω δεξί μέρος της οθόνης, εμφανίζεται η οθόνη **δημιουργίας νέας κατηγορίας.**



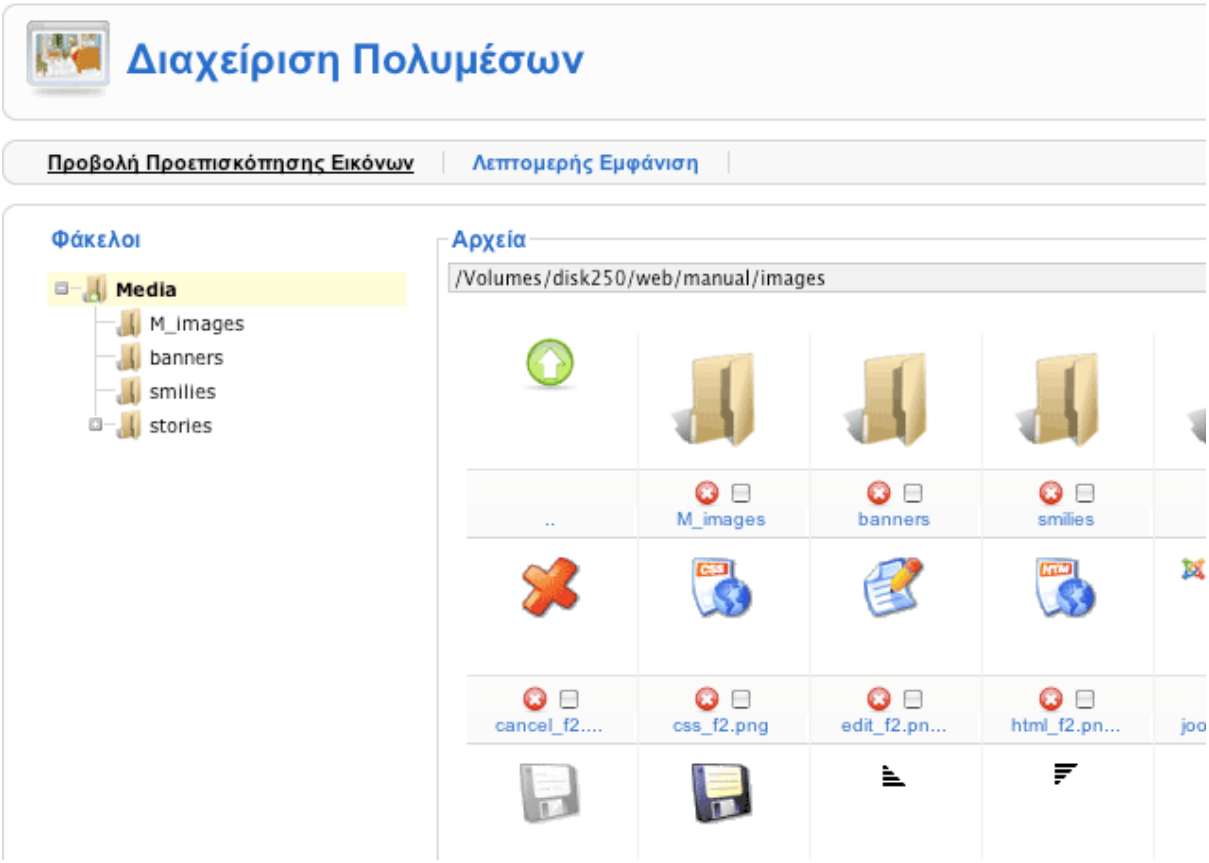
Η εικόνα πρέπει να σας θυμίζει πολύ εκείνην της δημιουργίας νέας ενότητας, που μόλις επισκεφθήκατε. Συμπληρώνετε με την ίδια λογική τα πεδία
Τίτλος
Ψευδώνυμο
Δημοσιευμένο/α
Ενότητα: είναι το επιπλέον πεδίο, όπου δηλώνετε την κατηγορία στην

οποία θα ενταχθεί η νέα κατηγορία.
Επίπεδο πρόσβασης
Στο πεδίο **Εικόνα** προδιορίζετε, αν θέλετε, μια εικόνα που χαρακτηρίζει την κατηγορία αυτή, και στο πεδίο **Θέση Εικόνας** ορίζετε τη θέση της.
Με τη βοήθεια του κειμενογράφου, δίνετε, αν θέλετε, την **περιγραφή** της κατηγορίας.
Πατώντας **Αποθήκευση**, ολοκληρώνετε και επιβεβαιώνετε τις αλλαγές αυτές. Μέσω του μενού Ιστότοπος > Πίνακας Ελέγχου, επιστρέφετε στη κεντρική σελίδα της διαχείρισης.

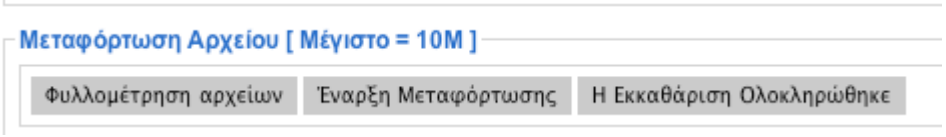
Εικόνες και άλλο υλικό

Οπως έχετε ασφαλώς παρατηρήσει, ο κειμένογραφος δίνει τη δυνατότητα να εντάξετε στο περιεχόμενο του δικτυακού σας τόπου εικόνες και άλλο υλικό (αρχεία flash animations, pdf, mov κλπ). Αυτό το υλικό βρίσκεται ταξινομημένο σε φακέλους μέσα στο φάκελο images/ της εγκατάστασης του joomla. **Οι εικόνες τοποθετούνται συνήθως μέσα στο φάκελο images/stories.**

Πώς θα ανεβάσετε και εσείς εικόνες στο δικτυακό σας τόπο μέσα από τη διαχείριση του joomla; Επιλέγετε, από την κεντρική σελίδα της διαχείρισης, το εικονίδιο **"Διαχείριση Πολυμέσων"**.



Στην οθόνη που εμφανίζεται, μπορείτε να δείτε όλο το υλικό που είναι διαθέσιμο για ένταξη στις σελίδες σας. **Υπάρχουν δυο ειδών απεικονίσεις:** η Προβολή Προεπισκόπησης Εικόνων, όπου μπορείτε να δείτε μια μικρογραφία της εικόνας, και η Λεπτομερής Εμφάνιση, όπου έχετε στη διάθεσή σας και άλλα στοιχεία όπως τις διαστάσεις της εικόνας, το μέγεθος του αρχείου κλπ.



Αφού δημιουργήσετε ένα νέο φάκελο,ή εντοπίσετε αυτόν που σας ενδιαφέρει, μπορείτε να ανεβάσετε ένα αρχείο στο μενού **Μεταφόρτωση Αρχείου**. Επιλέγετε το αρχείο μέσα από το μενού **"Φυλλομέτρηση Αρχείων"** και το ανεβάζετε πατώντας **"Έναρξη Μεταφόρτωσης"**.

Για πολλούς λόγους μπορεί καποιος να αποφασίσει τη μεταφορά του Joomla site σε ένα νέο server είναι βασικό να προσέξει κανείς τα

χαρακτηριστικά του νέου πριν καταλήξει στην απόφαση αυτή, ώστε να είναι πράγματι φιλικό το πακέτο προς το Joomla.

Η διαδικασία περιγράφεται με λίγα βήματα και έχει σκοπό να βοηθήσει τους απλούς χρήστες του Joomla να προχωρήσουν σε μια τέτοια ενέργεια.

Βήμα 1: Αντίγραφο ασφαλείας!
Το πρώτο πράγμα που πρέπει να κάνετε είναι ενα εφεδρικό αντίγραφο για όλα τα αρχεία απο τη Joomla εγκατάσταση. Δημιουργήστε έναν φάκελο (livesite) στο τοπικό σύστημά σας, και κατεβάστε όλα τα αρχεία σε εκείνο τον φάκελο χρησιμοποιώντας την FTP εφαρμογή σας .

Βήμα 2: Εξαγωγή της βάσης
Σ αυτό το βήμα πράγματι θα βοηθηθείς αρκετά αν ειναι εγακτεστημένο στο server σου το phpMyAdmin.
Βεβαιωθείτε ότι το αρχείο SQL περιέχει όλες τις απαραίτητες εντολές SQL για τη δημιουργία των πινάκων βάσεων δεδομένων σας και την πλήρωση τους με τα στοιχεία σας. Βεβαιωθείτε ότι εξάγετε την ολόκληρη βάση δεδομένων.
(Με ανοιχτή τη βάση μεσω phpMyAdmin επιλέγουμε εξαγωγή. Καλύτερα η εξαγωγή να γίνει σε sql. Ενεργοποιούμε την Αποστολή και επιλέγουμε τύπο συμπίεσης ή όχι αν είναι μικρή η βάση)

Βήμα 3: Ρύθμιση του configuration.php
Αυτό το βήμα είναι πολύ σημαντικό. Πηγαίνετε στο φάκελο στο τοπικό σύστημά σας στο οποίο κατεβάσατε τα αρχεία του Joomlasite σας!. Στον κύριο φάκελο που δημιουργήσατε (root), θα βρείτε το αρχείο με όνομα "configuration.php". Ανοίξτε αυτό το αρχείο με έναν κειμενογράφο και κάνετε τις απαραίτητες αλλαγές. Λογικά, θα πρέπει να αλλάξετε τις ακόλουθεςπαραμέτρους:

• *Config_absolute_path:* Αυτή είναι η απόλυτη διαδρομή του server στη νέο Joomla σας! εγκατάσταση. Θα μοιάζει πιθανώς κάτι σαν

"/path/to/joomla/installation" (Με Plesk εχει τη μορφή /home/httpd/vhosts/domain.gr/httpdocs) .

• *Config_cachepath:* Αυτή είναι η απόλυτη διαδρομή του server προς το Joomla/cache. Θα μοιάζει πιθανώς κάτι σαν "/path/to/joomla/installation/cache" (Με Plesk έχει τη μορφή /home/httpd/vhosts/domain.gr/httpdocs/cache).

• *Config_live_site:* Αυτό είναι url σας . Θα είναι κάτι σαν "http://www.myjoomla.gr".

• *Config_host:* Αυτή είναι η θέση του server που φιλοξενείται η MySQL βάση δεδομένων σας. Στις περισσότερες περιπτώσεις είναι "localhost".

• *Config_db:* Αυτό είναι το όνομα της MySQL βάσης δεδομένων σας.

• *Config_user:* Αυτό είναι το όνομα του χρήστη της βάσης (user name).

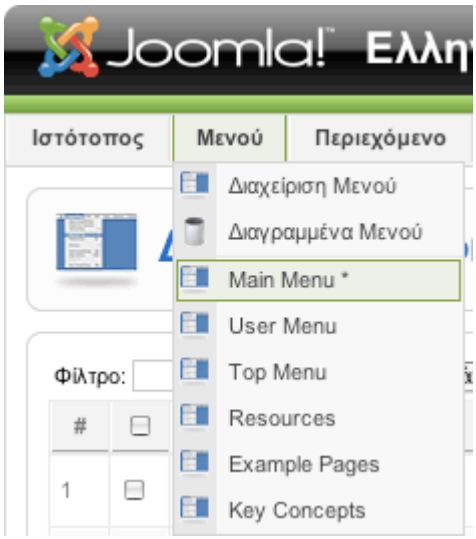
• *Config_password:* Αυτός είναι ο κωδικός της MySQL βάσης δεδομένων σας.

Βήμα 4: Ανεβάστε τα αρχεία στο νέο server Χρησιμοποιώντας μια ftp εφαρμογή (CuteFTP-FileZilla-WSftp),ανεβάστε όλα τα αρχεία στη θέση του νέου server που θέλετε να εγκαταστήσετε το Joomla!.

Βήμα 5: Δημιουργία νέας βάσης Μέσα απο το Control Panel του νέου σας server δημιουργήστε μια νέα βάση και ένα χρήστη. Πριν την εγκατάσταση, αλλάξτε τις ρυθμίσεις του collation σε utf8_general_ci μέσω του phpMyAdmin. (ALTER DATABASE nanedb DEFAULT CHARACTER SET utf8 DEFAULT COLLATE utf8_general_ci όπου namedb το όνομα της βάσης)

Βήμα 6: Είσοδος των στοιχείων στην νέα MySQL βάση
Απο το παράθυρο ερωτήματος > Εισαγωγή αρχείων. Χρησιμοποιώντας το phpMyAdmin και το το sql αρχείο που είχατε κάνει εξαγωγή στο 2ο βήμα κανετε εισαγωγή της παλιάς σας βασης στη νέα.

Μόλις εγκαταστήσατε το Joomla 1.5, δημιουργήσατε τα δικά σας κείμενα σε κατηγορίες και ενότητες, και θέλετε να αλλάξετε την εικόνα του πρωτοσέλιδου του ιστοτόπου σας. Ποιός είναι ο τίτλος που θα εμφανίζεται; Πόσα κείμενα, και με ποιόν τρόπο θα δημοσιεύονται; Ποιό θα είναι το όνομα του μενού που θα παραπέμπει στην αρχική σελίδα;



Στην κεντρική σελίδα διαχείρισης του joomla, επιλέγετε Μενού > Main Menu

και από τη λίστα των στοιχείων μενού που εμφανίζεται επιλέξτε Home

Ευρετήριο Άρθρων

Τρεις πρώτες αλλαγές που μπορείτε να κάνετε:

1. Να αλλάξετε το όνομα του στοιχείου μενού

Δώστε στο πεδίο **Τίτλος** το όνομα που θέλετε για το στοιχείο μενού, πχ. Αρχική Σελίδα, Κεντρική, Πρώτη κλπ.
Στο πεδίο **Ψευδώνυμο**, δώστε ένα μικρό χαρακτηρισμό με λατινικούς χαρακτήρες και χωρίς διαστήματα.

2. Να τροποποιήσετε την εμφάνιση των κειμένων

Εντοπιστε την καρτέλα **Βασικές Παράμετροι**. Εισάγετε τις τιμές που θέλετε στα πιο κάτω πεδία:
Επικεφαλής: δίνετε τον αριθμό των εισαγωγών των κειμένων που θα παρουσιάζονται σε πλήρες πλάτος, με μια ένδειξη "διαβάστε περισσότερα" για το υπόλοιπο κείμενο.
Εισαγωγής: δίνετε τον αριθμό των εισαγωγών των κειμένων που θα παρουσιάζονται σε πλάτος μιας στήλης, με μια ένδειξη "διαβάστε περισσότερα" για το υπόλοιπο κείμενο.
Στήλες: ορίζετε τον αριθμό των στηλών
Συνδέσμων: ορίζετε τον αριθμό των κειμένων που θα εμφανίζονται ως σύνδεσμοι, στο τέλος της σελίδας

Tip: αν ο αριθμός των στηλών είναι 1, τότε το # Επικεφαλής και # Εισαγωγής έχουν ίδια εμφάνιση.

3. Να αλλάξετε τον τίτλο της σελίδας

Εντοπιστε την καρτέλα **Παράμετροι Συστήματος**. Εισάγετε τις τιμές που θέλετε στο πεδίο **Τίτλος Σελίδας**. Επίσης ορίστε αν θα εμφανίζεται ο τίτλος πάνω από τα κείμενα ή όχι.

Στο tutorial αυτό περιγράφεται, με σύντομο τρόπο, το πώς δημιουργούμε και δημοσιεύουμε ένα νέο μπλοκ μενού σε ένα joomla site.

mosauthorxtd

Βήμα 1. Μέσα από το admin panel επιλέγουμε menu > menu manager

Βήμα 2. Επιλέγουμε "New", και δίνουμε το όνομα του menu, καθώς και το όνομα του module που θα αντιστοιχεί σε αυτό. Πατάμε "Save"

Βήμα 3. Μέσα από το menu > tomenumas (όπου tomenumas είναι το μενού που δημιουργήσαμε) μπορούμε να ορίσουμε ποια στοιχεία (menu items) θα υπάρχουν στο μενού αυτό.

Βήμα 4. Μέσα από το modules > site modules, επιλέγουμε το μενού που δημουργήσαμε και ορίζουμε τις παραμέτρους του: σε ποια θέση θα εμφανίζεται, σε ποιές σελίδες, με ποιο επίπεδο πρόσβασης, αν θα τυπώνεται ο τίτλος του κλπ.

VirtueMart Installation

Requirements

Server Requirements

VirtueMart has the following System Requirements:
• Apache 1.3.19 or above - http://www.apache.org, recommended: Apache 2.2.x
• PHP 4.2.x or above - http://www.php.net, recommended: PHP 5.2.x
• MySQL 3.23.x or above - http://www.mysql.com, recommended: MySQL 5.0.x

• Joomla! 1.0.x or Mambo (>= 4.6.2), recommended: Joomla! 1.0.x
You must ensure that you have MySQL-, XML- and Zlib-Support built into your PHP. Support for
https (openSSL) and **cURL** is recommended!

Important

The MySQL user, you access the database with in production use, must be able to create *temporary tables*.

Client Requirements

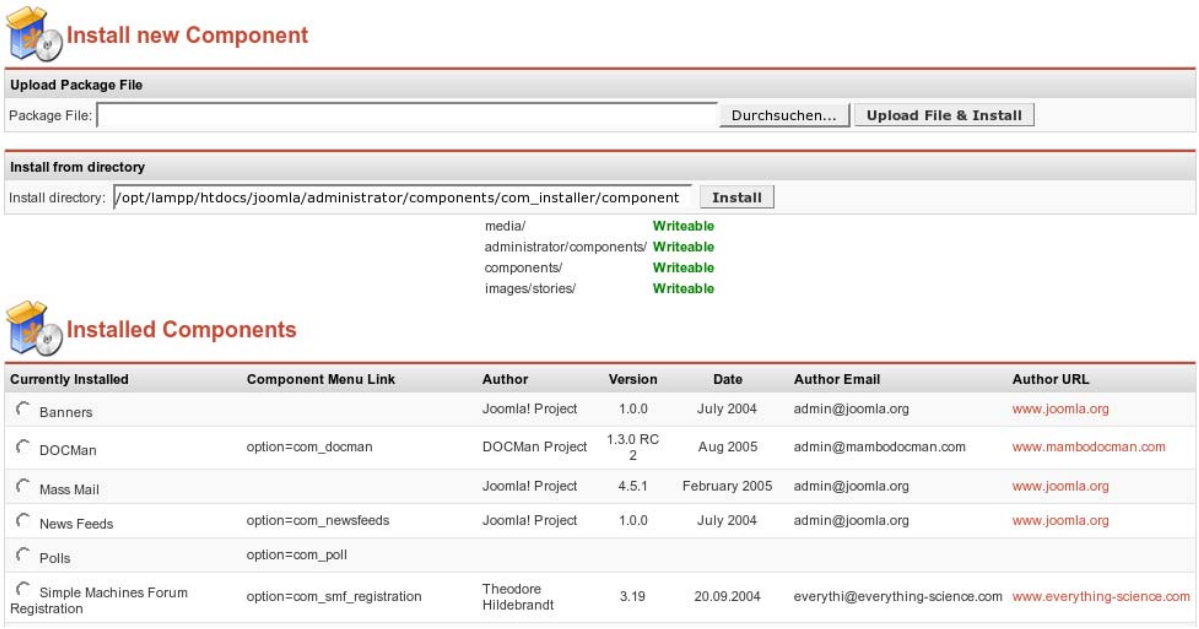
VirtueMart can be used with most major browsers including: Internet Explorer (version 5.5+), Firefox,
Opera 9+, Safari and Konqueror. Javascript doesn't need to be enabled when shopping and checking
out. The administration section requires Javascript to be enabled.
The browser needs to be capable of accepting Cookies and Cookies must be enabled.

Installation and Upgrade

New Installation

When having met all the requirements and when you are running Joomla! or Mambo you have two choices:

You need to have the priviliges of an Administrator / Super αdministrator to install Elements.
3. Click 'Installers' => 'Components' (or 'Components' => 'Install/Uninstall' when using an older
Mambo version) in the Top Menu.



Caution

You must check if the directories listed above the component list are writable! If the directories are not writable, use ftp or JoomlaXplorer to change the permissions. For proper installation, the directories should be set to 777, after that you can change back to 755.
In the part 'Upload new component' select the file 'com_virtuemart_x.x.tar.gz'. This is the package file which contains all files for the VirtueMart *Component*, located on your computer
(see Step 1).
Now click on 'Upload File & Install'. Since the tar.gz file is about 2 MB in size, you will have to
wait a moment while the file is being uploaded to your server and unpacked.

If the upload takes too long, try Step 4 or do the Manual Installation.
4. Alternative: You can unpack the contents of 'com_virtuemart_x.x.tar.gz' and upload

those files to a remote directory using a ftp connection. Now specify the directory on the server
from where you want to install the files and click 'Install'.

Note

Package Files are mostly a ZIP or tar.gz compressed file directory, which includes all information for the installation. The main file is an XML document which describes the
installation process. In order to use this function for your installation, your web server must support the zlib extension. You can check this in the Admin Section Menu
item, System > System Info > System Information.
5. The VirtueMart Component **should** be installed now. You'll see the Welcome Message Screen with
some options for the next steps:

Installation Welcome Screen
You can now choose whether you want to install Sample Data (18 products, with attributes, in 5
categories) to see how things have to be set up.
Or you can '**go directly to the Shop >>**' without installing Sample Data.
Caution
This step **again** takes some time & the VirtueMart installer is running a lot of Database
Queries now. So please be patient!
6. Click 'Installers' => 'Modules' (or 'Modules' -> 'Install/Uninstall' if you're using an older Mambo
version) in the Top Menu to proceed to the installation of the VirtueMart Main module.
Choose the file 'mod_virtuemart_x.x.tar.gz' in the File Dialog and click 'Upload File &
Install'.
Repeating this step you can install the additional modules for VirtueMart.
Publishing the Module:
Automatic Installation
10
Click 'Modules' -> 'Site Modules' in the Top Menu. Now browse through the list of installed
modules and find the one with the name 'VirtueMart Module'. Select it (click on the name) and
modify its settings/details. You can now choose where to put the Module on your Joomla! site.

For more information about modules please refer to the Joomla! documentation (help.joomla.org
[http://help.joomla.org]).

Important
Anywhere you place the module on your site, IT MUST BE PUBLISHED. If it is not, you
can't access or browse your shop.

Additional modules
mod_product_categories "Product Categories Module"
It can display the product categories you have set up.

mod_productscroller "Product Scroller Module"
It can scroll certain products somewhere on your site using a marquee tag.

mod_virtuemart_allinone "All-in-one module"
Can display the latest, featured, top-ten or random products in one module using tabs.

mod_virtuemart_cart "Mini-Cart Module"
Displays the mini-cart for the customer with a link to the cart page.

mod_virtuemart_featuredprod "Featured Products Module"
Can display featured products in your store. Featured products are those which are "on special".

mod_virtuemart_latestprod "Latest Products Module"
Displays the newest products in your store.

mod_virtuemart_manufacturers "Manufacturer Module"
Shows all manufacturers from your store with a link to find all products of the selected manufacturer.

mod_virtuemart_randomprod "Random Products Module"
Does what the name says: displays random products from your store or a certain category.

mod_virtuemart_search "Searchbox Module"
Displays the VirtueMart searchbox (which lets the customer search for products).

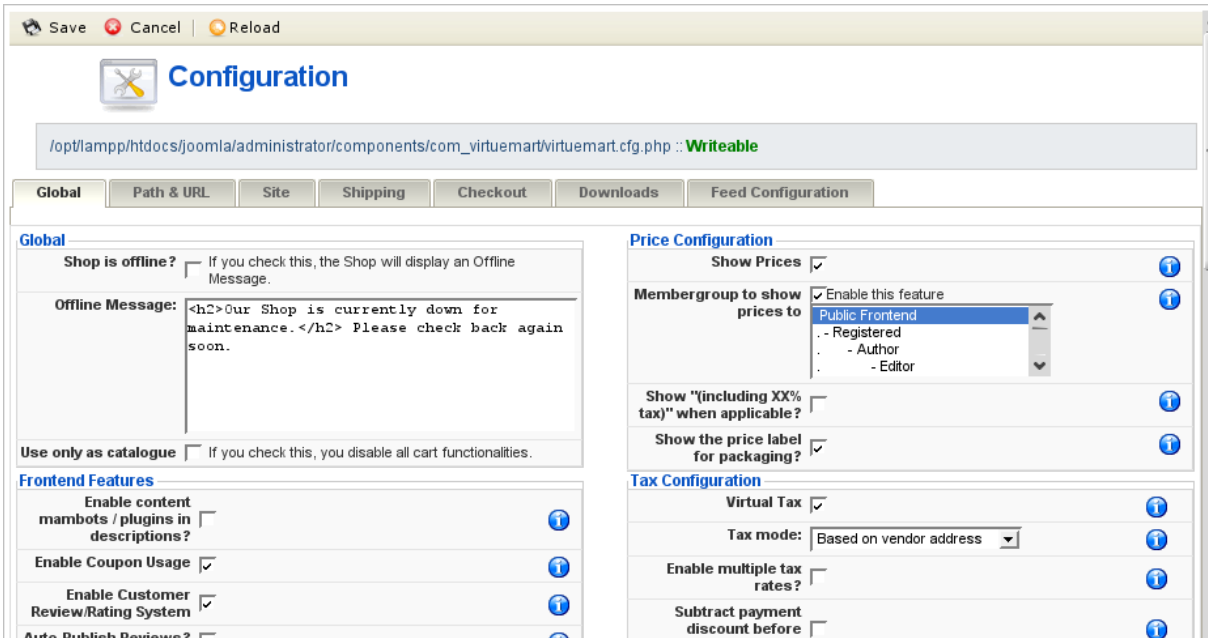
mod_virtuemart_topten "Top Ten Products Module"
Displays the bestsellers from your store.

2.2.4. Manual Installation

The installation has failed? You have safe_mode = On ?
You don't need to pull out your hair! You can still use the manual installation.
Manual Installation is a little bit harder than the automatic installation. It will need some file copying.
1. Download the Manual Installation Package. This is just another Package Form of VirtueMart.
2. Unpack the archive file VirtueMart_x.x_Manual-Installation-Package.tar.gz
you have downloaded in Step 1 to a local directory using Winzip or Winrar.
You should now see at least four directories. The directory structure in those directories is the same
as in your Joomla! / Mambo site:
/administrator
/components
/mambots
/modules
3. Open up an FTP Connection to your site (you should use an FTP Program like SmartFTP...) and
upload the directories to the root of your Joomla! site.
/site-root/administrator
/site-root/components
/site-root/mambots
/site-root/modules
4. Login in to the Backend (Administration) of your site (http://www.your_site.com/administrator/).
5. When having logged in, you see this URL in the address bar:
http://www.your_site.com/administrator/index2.php
6. Now just add "**?option=com_virtuemart**" after index2.php, so it looks like this in your
browser's address bar:

option=com_virtuemart
and submit (press Enter).

7. You should now see the "Installation was successful..." Screen. There you can click on "**GO TO**
THE SHOP >>" or "**INSTALL SAMPLE DATA >>**" (when you want to have some sample
Products and Categories in your Shop).
8. That's it.
9. To install the Modules and Mambots for VirtueMart, follow the instructions of the Automatic
Installation, Steps 6 and 7. If this doesn't help you, because NO automatic installations are possible,
you can manually upload the files (you have probably already done this in step 3).
Modules and Mambots require an entry in the table **jos_mambots** / **jos_modules.**
You can add these entries by uploading an SQL file (using phpMyAdmin) that contains all
necessary queries:
/administrator/components/com_virtuemart/sql/
virtuemart_modules.installation.sql
Now you should have installed VirtueMart correctly.



Note that the Configuration Panel can be accessed by Users with Permissions "admin" only (by default).
You can access the different parts of the Panel by clicking on the Tab Headings.

Global

Shop is offline? Here you can switch the shop from Online to Offline mode. In offline mode, the offline message is displayed instead of the product pages. This means the whole shop section isnt usable for customers. Administrators won't see the shop too.
Offline Message This message will be displayed to customers who try to access your store.
Global
18
Use only as catalogue Hides all "Add to Cart" buttons.
Show Prices When enabled, product prices are displayed. (useful when using "catalog-only" functionality. Note that you can't hide prices from unregistered users to show prices only to registered users. Either ON or OFF!
Membergroup to show prices to default:"Public Frontend"
Here you can decide which membergroups of your site are allowed to see product prices.
Show "(including XX% tax)" when applicable?
When checked, users will see the text "(including xx% tax)" when prices are shown incl. tax (which depends on shopper group settings!).
Show the price label for packaging?
Use "price per packaging" label?
Show Prices including tax? Sets the flag whether the shoppers sees prices including tax or excluding tax. When enabled prices are displayed like "X.XX (including XX% Tax)"
Enable content mambots/plugins in descriptions?
If enabled, you can use your mambots and plugins for dynamic content in the product or category descriptions.
Enable Coupon Usage If you enable the Coupon Usage, you allow customers to fill in Coupon Numbers to gain discounts on their purchase.
Customer Review/Rating System If enabled, you allow customers to rate products and write reviews about them. So customers can write down their experiences with the product for other customers.
Auto-Publish Reviews? If enabled, customer reviews are instantly shown after being submitted. Maybe not a good idea, because you want to check the product reviews before.
Comment Minimum Length This is the amount of characters a customer must write at least before a review can be submitted.

Comment Maximum Length This is the maximum amount of characters a customer can write
before a review can be submitted.
Enable Affiliate Program? This enables the affiliate tracking in the shop-frontend. Enable
if you have added affiliates in the backend.
Caution
The Affiliate Program doesn't fully work. It must be
completed in future versions.
Virtual Tax This determines whether items with zero weight are taxed or
not (only applies in Ship-To-Address based Tax Mode).
Tax mode This determines which tax rate is taken for calculating taxes.
It can be either the tax rate of the customer's shipping address
location, the tax rate of the store/vendor location or - in EU
Mode - the tax rate of the country, the store is located in,
regardless where the goods are shipped to.
Enable multiple tax rates? Check this, if you have products with different tax rates (e.g.
7% for books and food, 16% for other stuff).
Global
19
Discount before tax/shipping? Sets the flag whether to subtract the Discount for the selected
payment BEFORE (checked) or AFTER tax and shipping.
User Registration Type • Normal Account Creation:
This type of registration asks each customer for a username
and password and all other published registration details.
• Silent Account Creation:
In this mode, users don't need to fill in a username and
password for a new account. Instead the email address is used
for the new account and a random password is generated.
The registration details are mailed to the customer.
• Optional Account Creation:
The customer can select if a persistant account is created or
not. If the customers chooses to create an account, he is asked
for an username and password. If he chooses not to create an
account, a hidden account is created - so the customer can be
silently logged in and check out.
• No Account Creation possible
In this mode the customer can checkout without being able to
create an account for returning later on. Each time a dummy
user account is created to keep the data structure intact.
Show the "Remember me"
checkbox on login?
The "Remember me" feature allows to set a cookie in the
customer's browser, so the customer doesn't need to login each

time he returns to the site. This is done by default. But such cookies can be a security risk - especially when people are sharing a PC in an Internet Cafe. So check this checkbox to allow customers *not* to store a user cookie.

Customers can select a state/ region?

When enabled, your customers are presented a drop-down list with states where they can select one.

Must agree to Terms of Service? Check if you want a shopper to agree to your Terms of Service before registering to the shop.

Agree to T.o.S. on EVERY ORDER?

Check if you want a shopper to agree to your terms of service on EVERY ORDER (before placing the order).

Show information about "Return Policy" on the order confirmation page?

Store owners are required by law to inform their customers about return and order cancellation policies in most european countries. So this should be enabled in most cases.

Legal information text (short version)

This text instructs your customers in short about your return and order cancellation policy. It is shown on the last page of checkout, just above the "Confirm Order" button.

Long version of the return policy (link to a content item)

This is the long and detailled version of your returns policy. This text is linked in the short version and appended to each order confirmation email.

Check Stock? Sets whether to check the stock level when a user adds an item to the shopping cart. If set, this will not allow user to add more items to the cart than are available in stock.

Security

20

Show Products that are out of Stock?

Let's you decide wether Products that are out of Stock are displayed or hidden (only available when Check Stock is enabled).

Enable the Cookie Check? If enabled, VirtueMart checks wether the browser of the customer accepts cookies or not. This is user-friendly, but it can have negative consequences on the Search-Engine-Friendlyness of your shop.

Currency Converter Module This allows you to select a certain currency converter module.
Such modules fetch exchange rates from a server and convert
one currency into another.
Order-mail format: This determines how your order confirmation emails are set up:
• as a simple text email
• or as a html email with images.
DEBUG ? Turns on the debug output. This causes the DEBUGPAGE to be
displayed at the bottom of each VirtueMart page. Very helpful
during shop development since it shows the carts contents, form
field values, etc.

Security

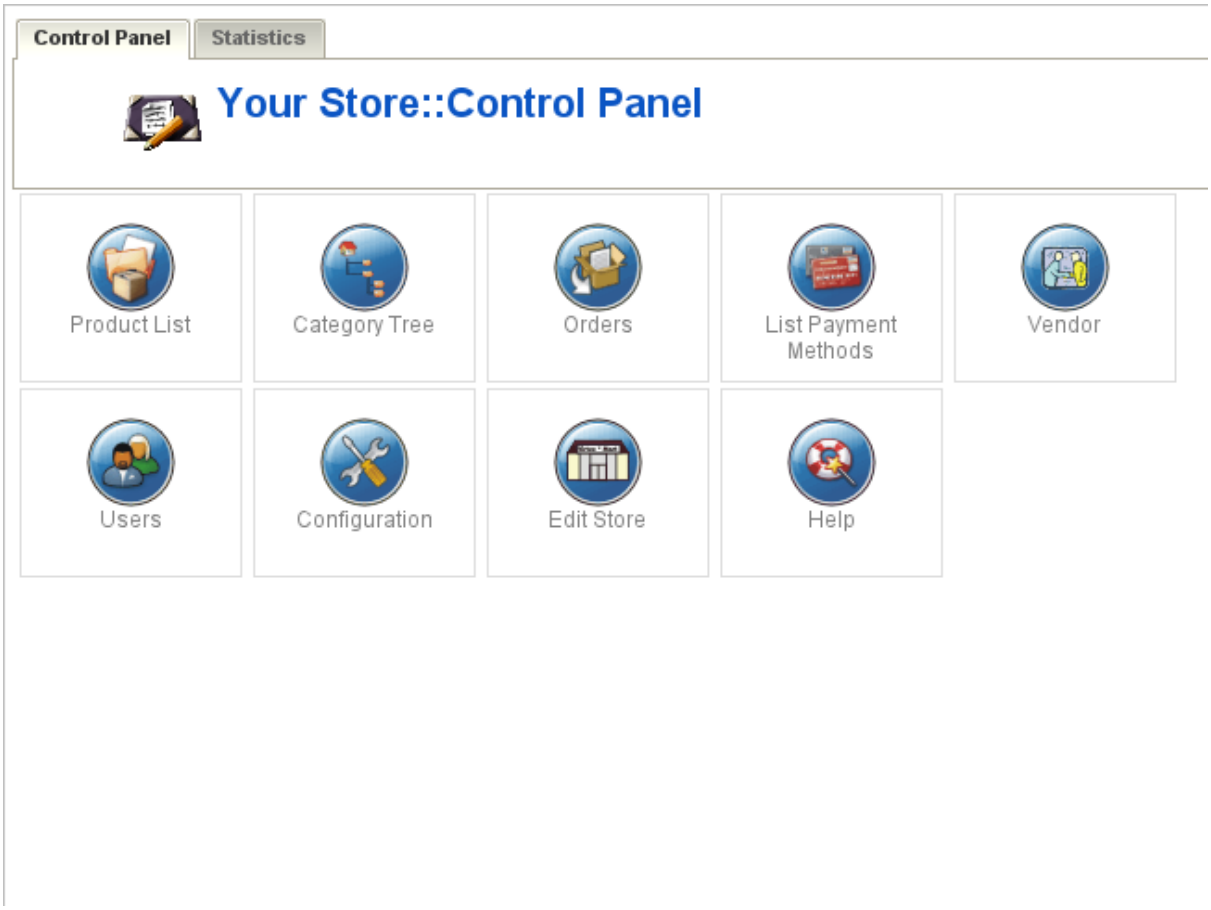
SECUREURL Example: https://www.mydomain.com
The secure URL to your site. (https - with trailing slash at the
end!)
Caution
Be careful what you fill in here - if the address doesn't
exist, customers would be redirected to a non-existing
location and receive a 404 error!
Shop Areas which must use https Some of the areas of your shop can be forced to use the SECUREURL connection. Here you can choose the
modules which must use this SECUREURL. By default this
is: "account" (Account Maintenance) and "checkout" (the
complete Checkout).
Generally prevent secure
connections?
When checked, the shopper is redirected to the **normal** URL
when not browsing in those shop areas, which are forced to use
the **SECUREURL**.
Encryption Key The secret key for encrypting payment account data like credit
card numbers and storing them encrypted in the database.
Store Credit Card Information? Allows to completely disable the storage of Credit Card data.
Allow Frontend-Administration... ...for non-Backend Users?
With this setting you can enable the Frontend Administration
for users who are storeadmins, but can't access the Mambo
Backend (e.g. Registered / Editor).
Table Prefix for VirtueMart Tables This is an experimental feature to allow multiple shops in one
Joomla! installation.
HOMEPAGE Example: shop.index
Site (Display & Layout)
21
This is the page which will be loaded **in the frontend** by

default.
ERRORPAGE Default: shop.error
This is the default page for displaying VirtueMart Error
Messages.
Proxy Server URL The URL of the Proxy Server you need to pass from the server for connections into the Internet.
Proxy Port The Port of the Proxy Server
Proxy Auth Username Only if needed: the username for authentication at the proxy server
Proxy Auth Password Only if needed:

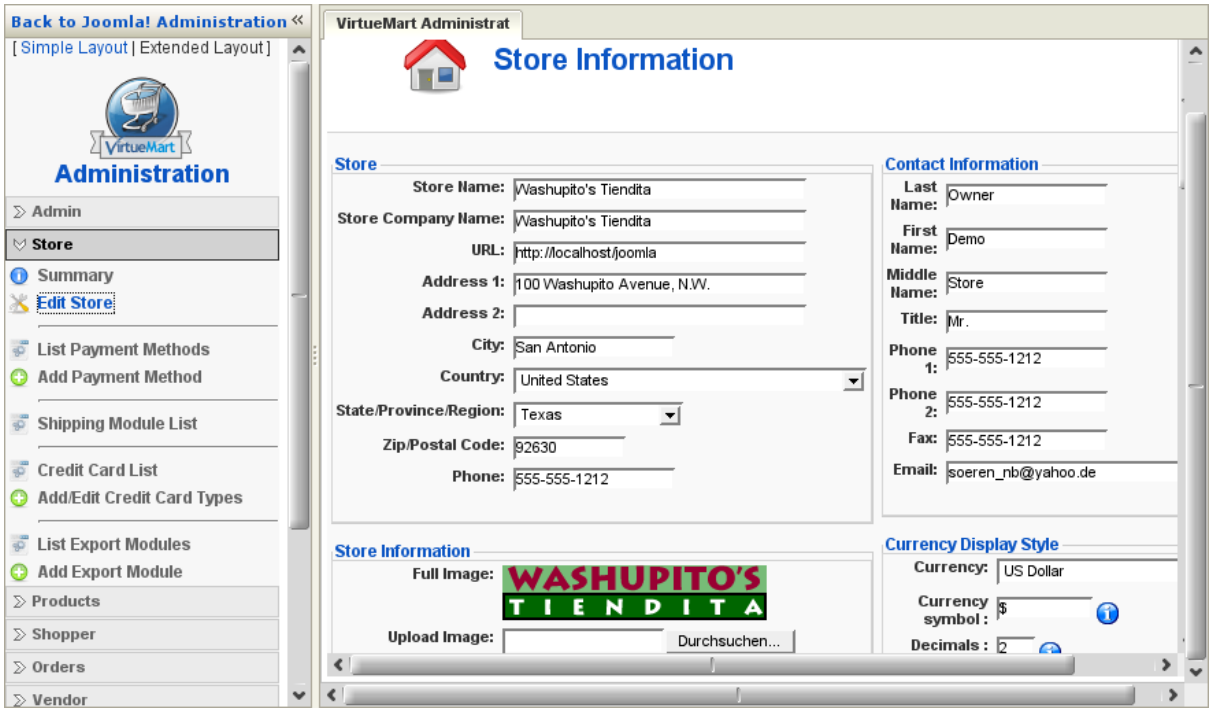
.2. Getting Started

To access the configuration of VirtueMart, select "Components | VirtueMart" in the Joomla! Administration Interface.


Joomla! Administrator
version 1.0
Home
Site
Menu
Content
Components
Modules
Mambots
Installers
Mes
VirtueMart 1.1.x Test / com_
Control Pan
Add New Content
Content Items Manager
Banners
Community Builder
Contacts
DocBook:Collab
JCE Admin
joomlaXplorer
Letterman
Mass Mail
News Feeds
Polls
Syndicate
Version Management
VirtueMart
VirtueMart Language Manager
Web Links
tor
tor
End >>
1 - 2 of 2



You may also access this page from within the VirtueMart interface under "Store | Summary"



The Information from the Store Information Form is displayed in various Locations on the Shopping Site. This is your Store's primary Identity - essentially a special "Master" Vendor.

Store Information Form Fields

Store Name Required
The name of the Store.
Store Company Name Required
The name of your company.
URL The Store's Internet Address.
Address 1 Address Line 1
Address 2 Address Line 2
City The City where your Store is located.
State/Province/Region The State / Region where your Store is located.
Country The Country where your Store is located.
Zip/Postal Code The ZIP of your Store's location.
Phone Your Store's Phone Number
Last, First & Middle Name The Name of your Contact Person.
Title The title of the Contact Person.
Phone 1 & 2 Your contact's Phone number.
Fax The Fax number for the Contact.
Email Address Primary store contact email address
Full Image Required
Displays the currently configured store logo.
Upload Image Optional
Browse to your company logo. This will be uploaded when you

click on the "Save" icon.
Minimum Purchase Order Value This is the amount which is the minimum Order Value for
Checkout.
Minimum Amount for Free
Shipping
This is the amount, from which on Shipping is free.
Currency The Store's global / default Currency
Currency symbol This is the currency symbol which will be used when displaying prices.
Decimals Number of decimals.
Decimal symbol Can be somethin like . , or empty.
Countries, Currencies,
Core Modules & Functions
27
Thousands separator
Positive format Display Order / Style for positive numbers.
Negative format Display Order / Style for negative numbers.
List of accepted currencies This list defines all those currencies you accept when people
are buying something in your store.
Note
All currencies selected here can be used at checkout! If
you don't want that, just select your country's currency
(=default).
Description This is your Store's Description which is shown on the page
shop.index.
Terms of Service This is the complete text for your Terms of Service that is displayed to the customer.
Click on the "Save" icon. Now you're ready to begin adding Categories, Products and Manufacturers.

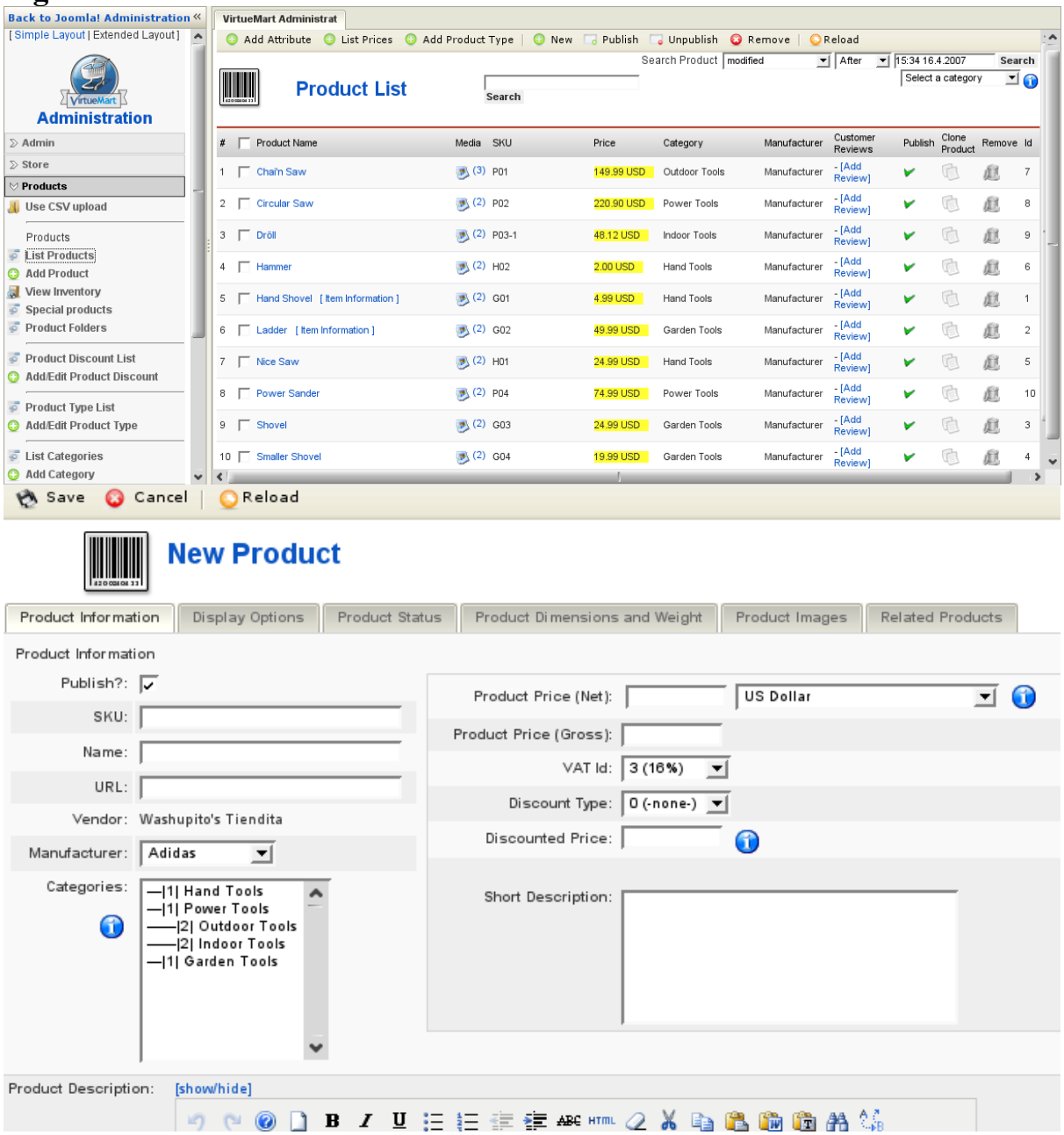
When creating your product records, it is important to make a distinction as to whether the product that
is being created can be uniquely identified by its nature or name (e.g. Compact Disks, Video Cassettes,
Books, etc.), or is one of many similar items that are uniquely identified by their attributes (e.g.
Apparel, Furniture, Automobiles, etc.). The reason this distinction needs to be made, is because the

methods for creating, editing and deleting differ for each. Items require the creation of Item Attributes,
but products do not.

Adding/Updating Products

To create a new product, click on "Products" # "Add Product" to display the product form. Complete
the product entry form and click the Save button in the top right corner to save the new product.
When Updating a product, just click on the Product Name in the Product List to display to Product
Form of that product.

Figure 4.15. VirtueMart Administration: Product List



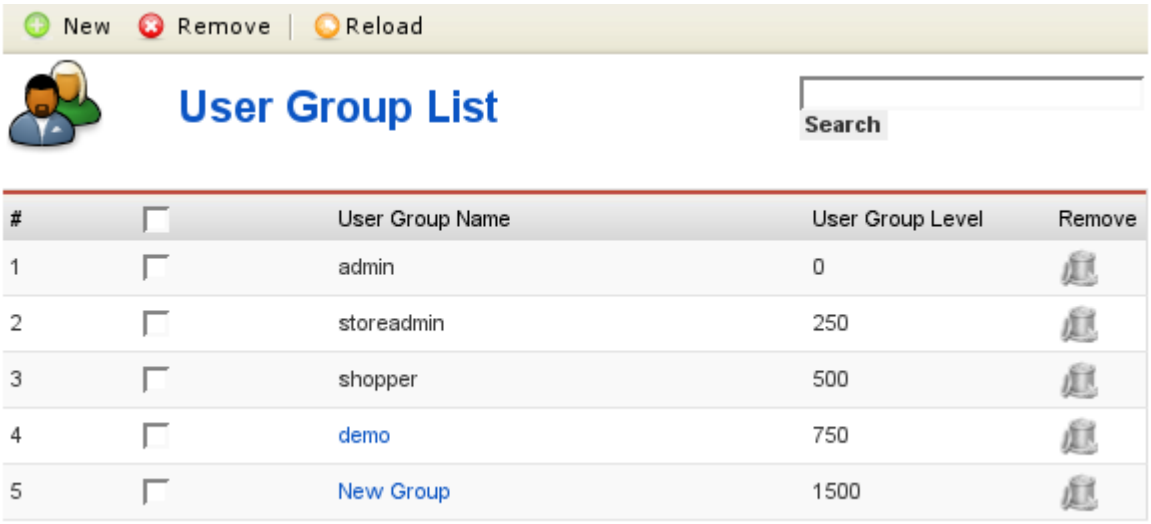
Name The name that will be used to identify the product.
URL A URL that can be displayed with a product. Usually used as a link to
the product vendor or manufacturer.
Category The product categories with which this product will be associated.
Vendor The vendor with which the product will be associated.

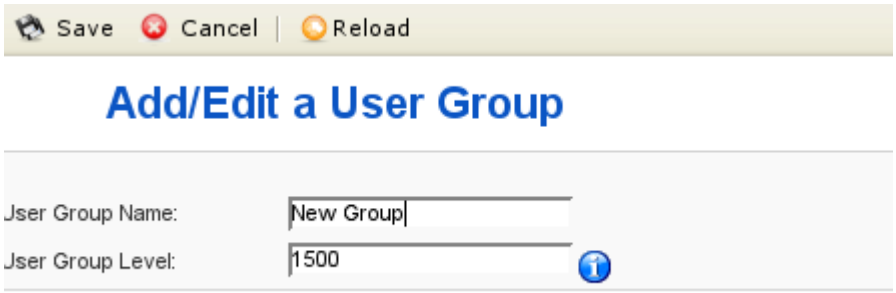
Manufacturer The manufacturer with which the product will be associated.
Retail Price The price for the default Shopper Group. Just fill in a decimal number.
Select the Product Currency from the drop-down list at the right.
VAT ID The ID of the tax rate that will be applied to this product. Here you
can select a specific tax rate for this product. If you don't want that this product is taxed, fill in a zero weight at "product weight" and Disable "Virtual Tax".
Short Description The short description that will be displayed on the browse (overview)
page for a category or search result.
Flypage Description This is the details description that will be displayed on the Flypage
(=details page) of this specific product.

USER GROUPS

User Groups are "Permission Groups" and used to restrict access to certain parts and functions of the
shop. Each user is assigned to a user group. By default registered customers are members of the group
"shopper".
When can this be useful? Imagine you have a user, who wants to access the "Report" section of
the store. Usually this is restricted to admins and stoeradmins. If you assign this user to the admin/
storeadmin group, he will also be able to access other sensible parts of the store, where he could change
or delete important data. The solution is to add a new User Group called "Report", which will have
the same permissions as shoppers PLUS access to the "report" core module. After the Group has been
added, you can assign this user to the new group.

User Groups can be added, modified and deleted from the User Group List ("Admin" # "User Groups").





Here you can choose a name for the group and the group level.

Note

The higher the group level, the less permissions are assumed: "admin" has higher permissions
than "storeadmin", because the group level number is lower.

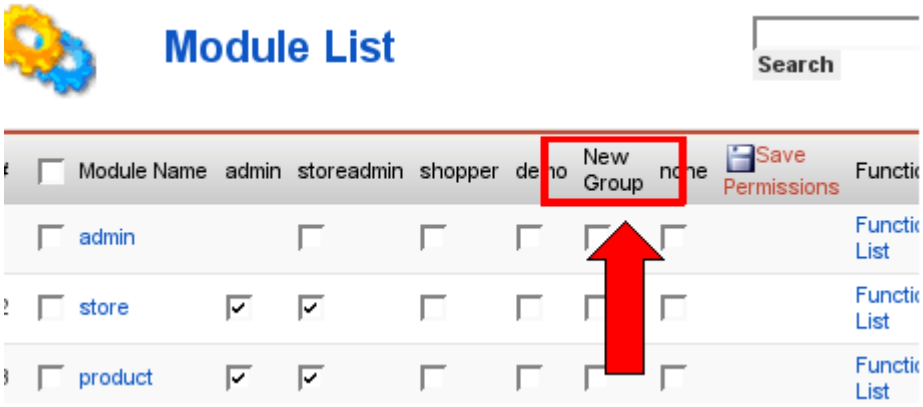
After you have saved the user group, it is available in the core module and function list/forms.

Figure 4.41. VirtueMart Administration: The New Group in the Module List

Now you can start to grant permissions to this new group by checking the boxes in this list for the
column of the "New Group".

Important

The same needs to be done for the function list of **each** module!



4.7.4. User Registration Fields

The "User Fields" Management allows you to freely modify the fields displayed on registration and
account maintenance. Such fields are for example: First Name, Last Name, Telephone,...

The User Field Management can be accessed via "Admin" # "Manage User Fields".

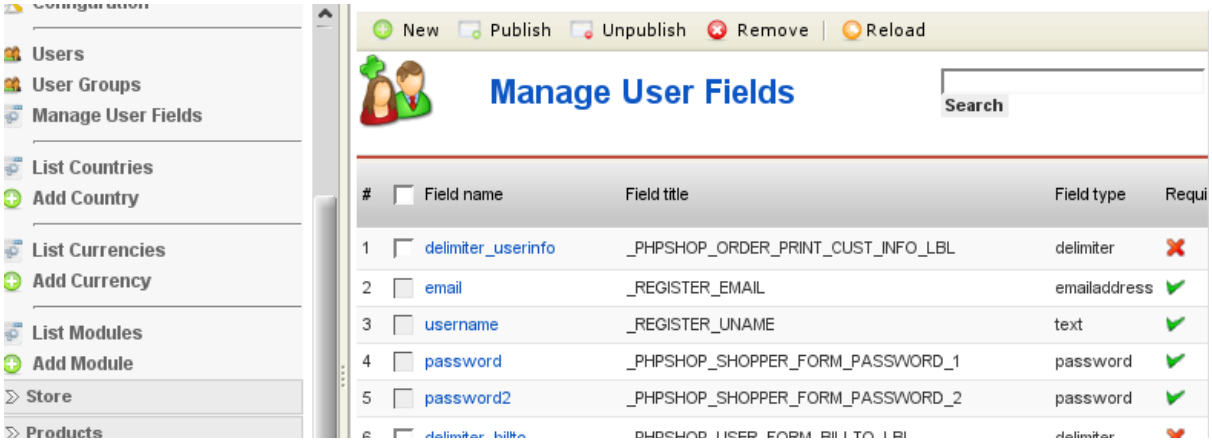


Figure 4.42. VirtueMart Administration: Manage User Fields

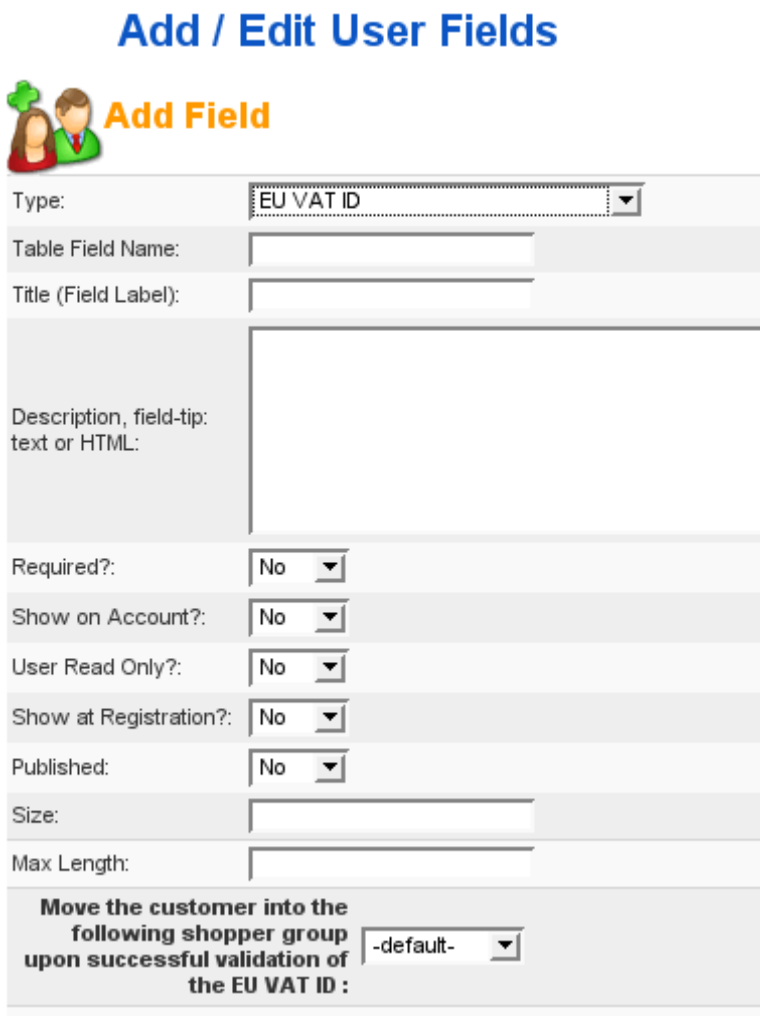


Figure 4.43. VirtueMart Administration: Add a new User Field

The Form Fields have the following meaning:
Type The type of this field. Can't be changed afterwards!
Table Field Name The name of the column that will be inserted into the table structure of the tables "jos_vm_user_info" and "jos_vm_order_user_info" in your database.
Title This is the Label of the Field in the Registration / Account Maintenance Form
User Registration Fields
58
Description This description will be shown to the customer in the frontend
in a small tooltip besides the field to explain the field.
Required? If this is set to yes, a value must be provided or chosen,

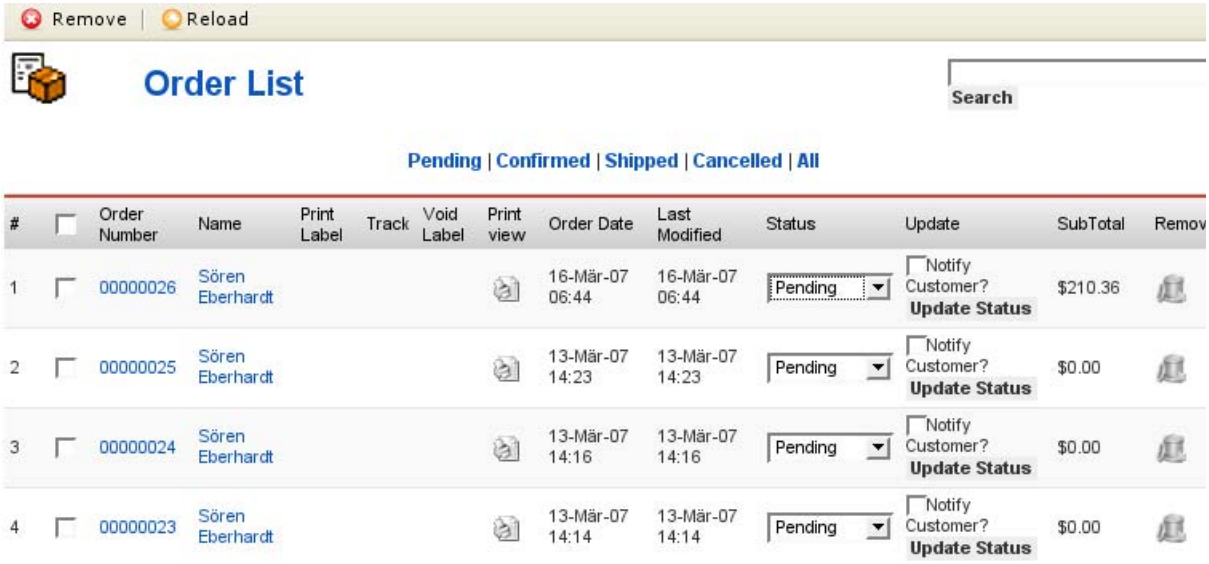
otherwise registration will not be possible.
Show on Account? This defines wether the field is shown in the account maintenance form or not.
User Read Only? If this is set to yes, the field is read-only and can't be changed
by the customer.
Show at Registration? If this is set to yes, the field will be shown in the registration
form.
Published Here you can unpublish the field completely, so it won't be shown in any form.
Size This defines the length of text input fields.
Max Length This is the maximum number of characters that can be filled into the text field.
Move the customer into the
following Shopper Group...
Here you can select into which shopper group the newly
registered customer is moved when the EU VAT ID has been
succesfully validated.
If you are finished filling in the necessary values, don't forget to Save your changes.
Here is a screenshot of the newly added field "EU Vat ID" in the registration form:

4.8.1. The Order List

Figure 4.47. VirtueMart Administration: Order List

When you click on an order number, you are given the full details of the order as shown in the next
figure.
When you click on the name of the customer, you will be taken to the user form for this user. The
Print View Link opens a new window that allows you to print out the order. In the status column you
can see the current status of this order. You can change this value and after that click on the "Update
Status" button to the right to update the order status. If you wish to notify the customer about this
action, check the option "Notify the customer?".
To delete an order, use the Trash Bin icon in the last column or select multiple orders using the

checkboxes in the first column and click on "remove" in the toolbar



4.8.2. The Order Details

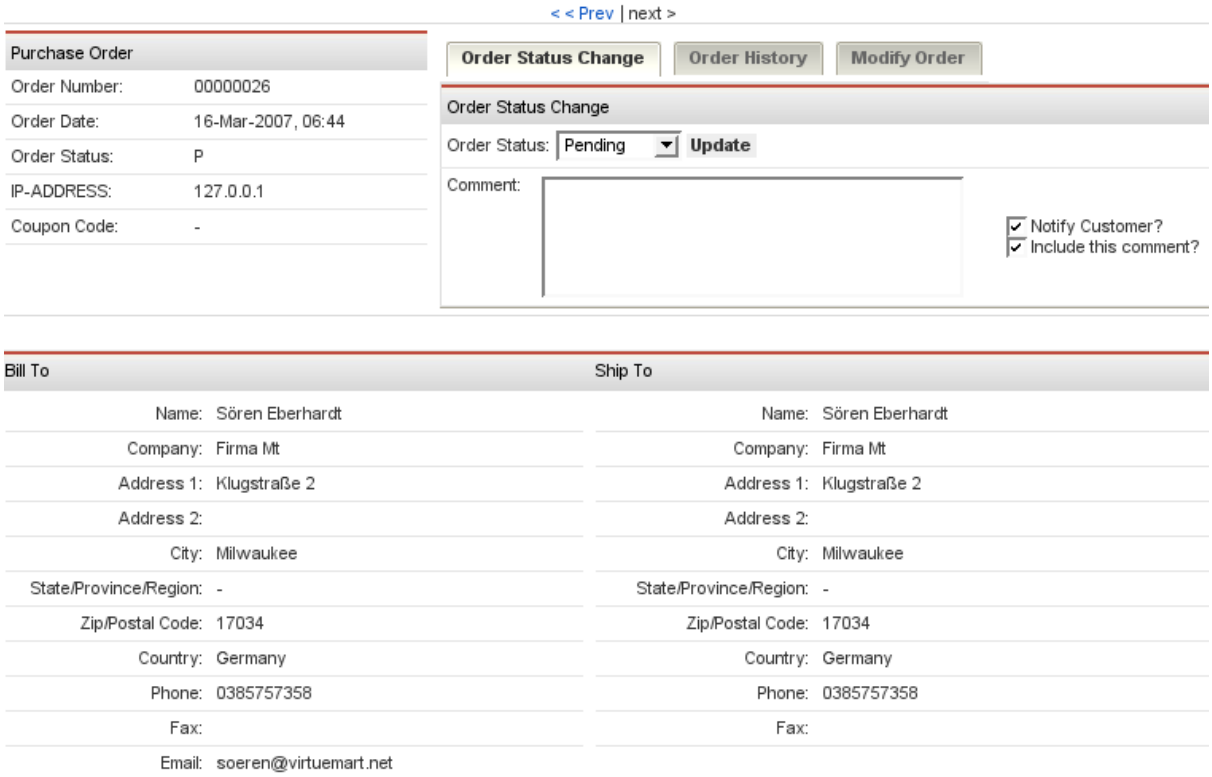
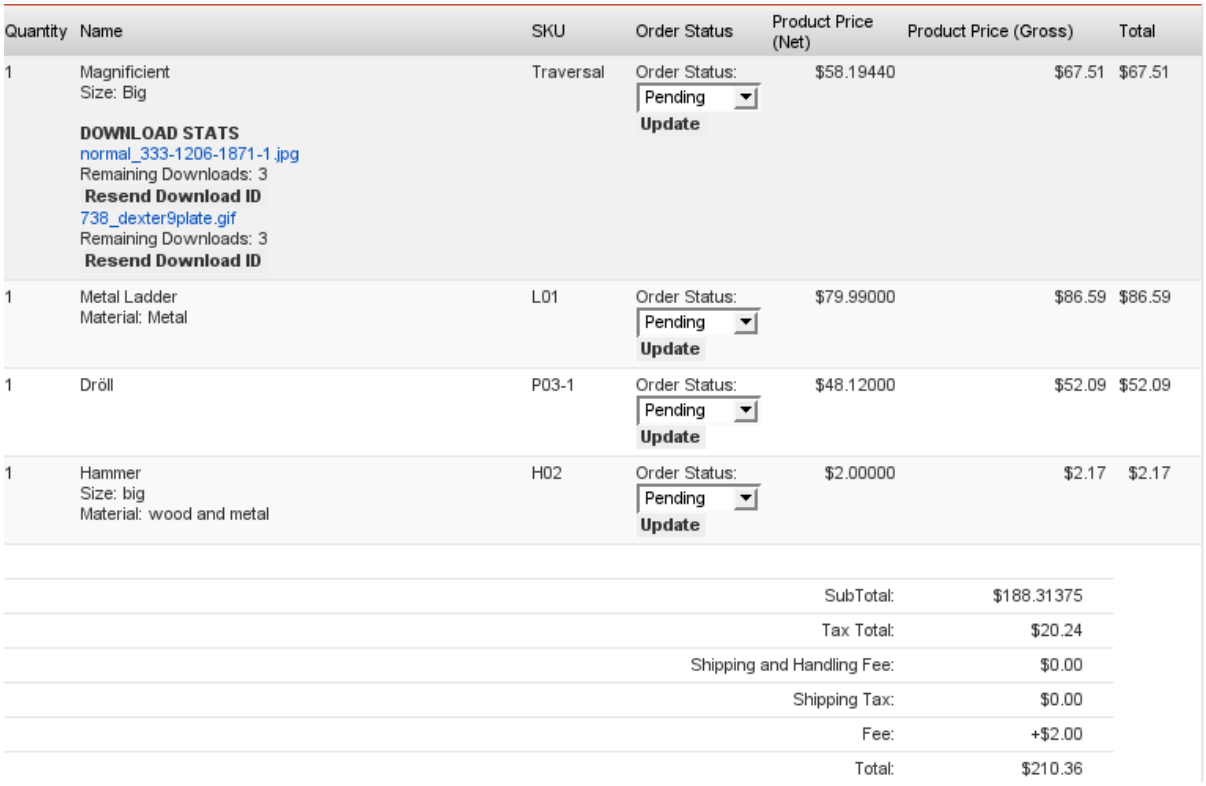


Figure 4.48. VirtueMart Administration: Upper Part of the Order Details

The Order Details View shows all details which are relevant to the store owner. You have three tabs in the upper part: Order Status Change, Order History and Modify Order.



Quantity	Name	SKU	Order Status	Product Price (Net)	Product Price (Gross)	Total
1	Magnificient Size: Big **DOWNLOAD STATS** normal_333-1206-1871-1.jpg Remaining Downloads: 3 **Resend Download ID** 738_dexter9plate.gif Remaining Downloads: 3 **Resend Download ID**	Traversal	Order Status: Pending **Update**	$58.19440	$67.51	$67.51
1	Metal Ladder Material: Metal	L01	Order Status: Pending **Update**	$79.99000	$86.59	$86.59
1	Dröll	P03-1	Order Status: Pending **Update**	$48.12000	$52.09	$52.09
1	Hammer Size: big Material: wood and metal	H02	Order Status: Pending **Update**	$2.00000	$2.17	$2.17

SubTotal:	$188.31375
Tax Total:	$20.24
Shipping and Handling Fee:	$0.00
Shipping Tax:	$0.00
Fee:	+$2.00
Total:	$210.36

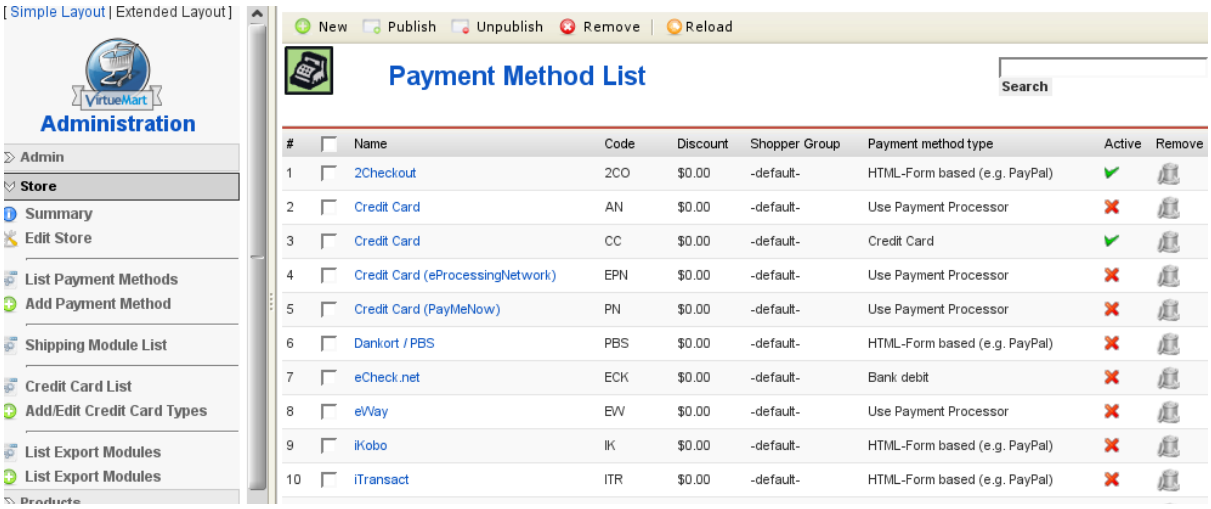
Figure 4.49. VirtueMart Administration: Bottom of the Order Details
In this part of the order details screen you see the list of all purchased products. If the products are downloadable products, you can re-send the Download Notification Email or re-initiate the downloads

4.12. Payment Methods

The area of *payment processing* can get a bit complicated, and it might be best to leave this to your
web designer to sort out if possible. If you are able to use one of the payment processing companies

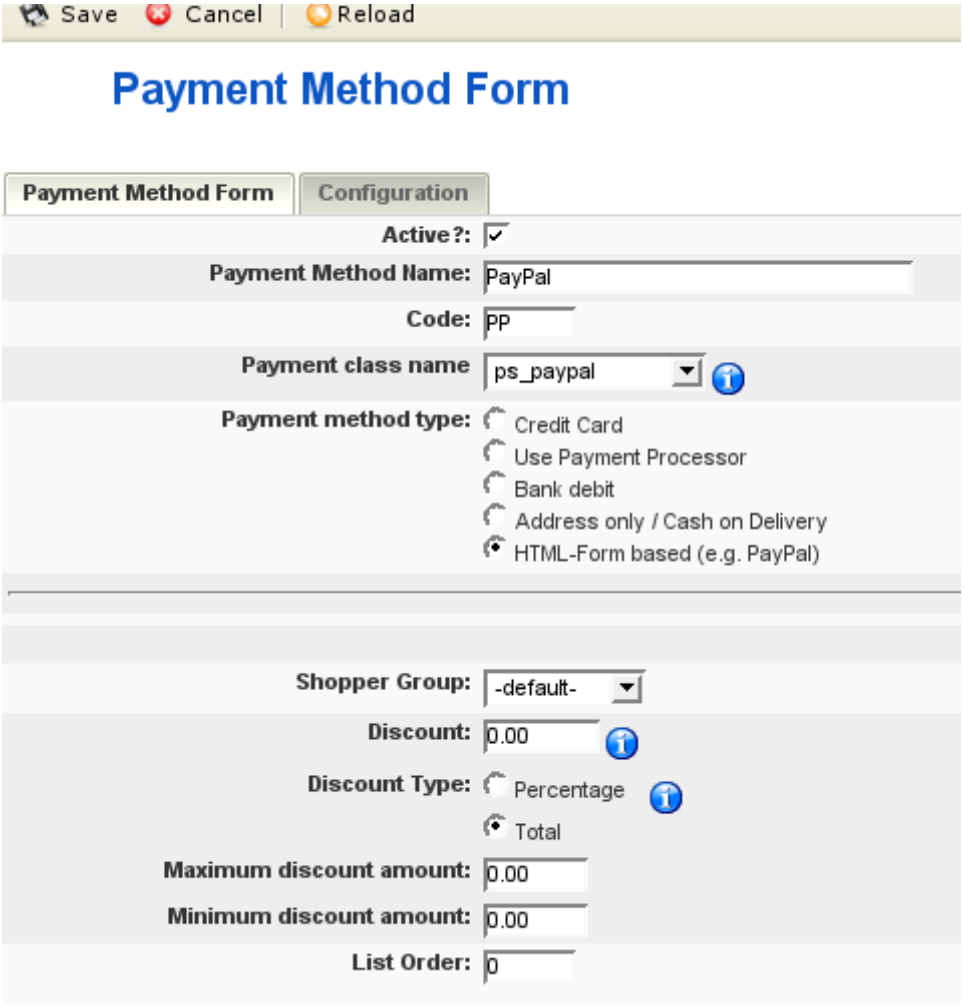
that are already supported by VirtueMart, it will make life a lot easier (you will need to sign-up with a
payment processor yourself – the program won't do that for you!). You can see the options available
by clicking on the *'List Payment Methods'* icon on the store summary, or by selecting 'List Payment
Methods' from the 'Store' menu.

4.12.1. Payment Method Management



It is possible to create a new payment method (there is a 'New' toolbar button), but you may to hack
the VirtueMart code in order to make use of it (not for the faint-hearted!)
Add and Edit Payment Methods
The configuration options for each payment method are different – depending on what is required
by that payment service provider. Usually your payment service provider will give you some kind of
code, key, or user name which needs to be entered in the *Payment Method Editor*.
The Payment Method Editor consists of 2 tabs – the first of which you will probably not need to touch.
The next Figure shows the 2nd tab ('Configuration'), which varies depending on the payment service
provider, and the example shown here is for WorldPay.

4.12.2. Add and Edit Payment Methods



Some payment processors will allow you to specify a script to be run on successful completion of a
payment. Such a script could be used to *automatically update the order status* in VirtueMart so that
you don't have to manually tie up all of your online receipts with your product orders. Another advantage of this process is that when you're selling downloadable files, you don't have to set
the Order Status that enables the Download (this sends out the Download-ID email) manually. This
is done automatically by the script.

See the Section "Pre-Configured Payment Methods" for more details on specific payment gateways.
Other payment service providers may use different methods of automatically notifying you when a

payment is received. Again, it is probably easiest to get your web designer to sort out the requirements
for this, but if you need to do it yourself, check with your payment service provider as to what
their requirements are. Often, automatic notification is referred to as *'IPN' or 'Instant Payment
Notification'*

PayPal

www.paypal.com [http://www.paypal.com]

PayPal η ολοκλήρωση γίνεται χρησιμοποιώντας ένα Webform που μεταφέρει τον πελάτη στην περιοχή PayPal.

Αυτή η μέθοδος πληρωμής επιτρέπει τις αυτόματες αναπροσαρμογές θέσης διαταγής. Εκεί αρχείων / διοικητής/

συστατικά/com_virtuemart/ που καλείται notify.php. Θα πρέπει να εισαγάγετε κατάλληλο URL (διεύθυνση Ιστού) για το αρχείο χειρογράφων στην επιτροπή ελέγχου PayPal's. Όταν ένας πελάτης τελειώνει η πληρωμή, ο κεντρικός υπολογιστής PayPal συνδέει με αυτό το εγγραφο στον κεντρικό υπολογιστή σας. Όταν η συναλλαγή και η πληρωμή είναι επιτυχής, η θέση διαταγής ενημερώνεται αυτόματα στη θέση που έχετε θέσει μέσα η μορφή διαμόρφωσης PayPal.

Επεξεργασία πληρωμής:

Δεχτείτε τις πληρωμές PayPal από τους πελάτες και όλες τις σημαντικές πιστωτικές κάρτες

Δεχτείτε τις δωρεές, τις συνδρομές, και τις επαναλαμβανόμενες πληρωμές

Αφήστε τη λαβή PayPal οι πληρωμές πελατών σας

Στείλετε τους πελάτες από τον ιστοχώρο σας στον παυΠαλ-φιλοξενημένο έλεγχο

Αφήστε τις πληροφορίες πιστωτικών καρτών καταστημάτων PayPal

Όφελος από το επαγγελματικό σύστημα επαλήθευσης απάτης PayPal

Εφαρμογή:

"Αγοράστε τώρα" τα κουμπιά διαθέσιμα για να κάνετε χωρίς ένα κάρρο αγορών

Ενσωματώνεται σε OScommerce, ZenCart, το κάρρο κύβων και άλλα κάρρα αγορών

Πώς χρησιμοποιώ το κλειδί ασφάλειας;

1. στην αρχική σελίδα PayPal, πληκτρολογέστε τη διεύθυνση ηλεκτρονικού ταχυδρομείου και τον προσωπικό κωδικό σας.
2. ελέγξτε το κλειδί ασφάλειας για τον τρέχοντα κώδικα ασφάλειας έξι-ψηφίων σας.
3. πληκτρολογέστε τον κωδικό δίπλα στον κωδικό πρόσβασής σας, κατόπιν π΄ατημα στο κουμπί **σύνδεσης**.

Το κλειδί ασφάλειας λειτουργεί με οποιοδήποτε browser λειτουργικών συστημάτων και Ιστού υπολογιστών που μπορεί να έχει πρόσβαση στον ιστοχώρο PayPal.

Το κλειδί ασφάλειας δημιουργεί τον κωδικό πρόσβασης μοναδικό με τη χρησιμοποίηση ενός σύνθετου αλγορίθμου που είναι μοναδικός στη συσκευή σας. Όταν πληκτρολογείτε εκείνο τον κωδικό Αυτό βοηθά να αποτρέψει τους αναρμόδιους χρήστες από την αναγραφή μέσα στον απολογισμό PayPal σας

ΠΡΟΤΟΚΟΛΛΑ ΚΑΙ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΠΟΥ ΧΡΥΣΙΜΟΠΟΙΗΣΑΜΕ ΓΙΑ ΝΑ ΓΙΝΕΙ ΤΟ E-SHOP ΠΙΟ ΑΣΦΑΛΕΣ ΓΙΑ ΣΥΝΑΛΛΑΓΕΣ

Πρωτόκολλο SSL

Το **πρωτόκολλο SSL (Secure Sockets Layer)** αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Η έκδοση 3.0 του πρωτοκόλλου κυκλοφόρησε από την Netscape το 1996 και αποτέλεσε την βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (Transport Layer Security), το οποίο πλέον τείνει να αντικαταστήσει το SSL. Τα δύο αυτά πρωτόκολλα χρησιμοποιούνται ευρέως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου.

Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών) εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP, το telnet κοκ.

Γενικά

Η μετάδοση πληροφοριών μέσω του διαδικτύου γίνεται ως επί το πλείστον χρησιμοποιώντας τα πρωτόκολλα TCP/IP (Transfer Control Protocol / Internet Protocol). Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου, όπως είναι για παράδειγμα το HTTP

(προβολή ιστοσελίδων), το FTP (μεταφορά αρχείων) και το IMAP (email). Άρα λοιπόν αυτό που ουσιαστικά κάνει το SSL είναι να παίρνει τις πληροφορίες από τις εφαρμογές υψηλότερων επιπέδων, να τις κρυπτογραφεί και στην συνέχεια να τις μεταδίδει στο Internet προς τον Η/Υ που βρίσκεται στην απέναντι πλευρά και τις ζήτησε.

Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου.

Το SSL προσφέρει συνοπτικά τις ακόλουθες υπηρεσίες:

- Πιστοποίηση του server από τον client.
- Πιστοποίηση του client από τον server.
- Εγκαθίδρυση ασφαλούς κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ των δύο μερών.

Οι κρυπτογραφικοί αλγόριθμοι που υποστηρίζονται από το πρωτόκολλο είναι οι εξής: DES - Data Encryption Standard, DSA - Digital Signature Algorithm, KEA - Key Exchange Algorithm, MD5 - Message Digest, RC2/RC4, RSA, SHA-1 - Secure Hash Algorithm, SKIPJACK, Triple-DES.

Τρόπος λειτουργίας

Το πρωτόκολλο SSL χρησιμοποιεί έναν συνδυασμό της κρυπτογράφησης δημοσίου και συμμετρικού κλειδιού. Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ πιο γρήγορη και αποδοτική σε σχέση με την κρυπτογράφηση δημοσίου κλειδιού, παρ' όλα αυτά όμως η δεύτερη προσφέρει καλύτερες τεχνικές πιστοποίησης. Κάθε σύνδεση SSL ξεκινά πάντα με την ανταλλαγή μηνυμάτων από τον server και τον client έως ότου επιτευχθεί η ασφαλής σύνδεση, πράγμα που ονομάζεται χειραψία (handshake). Η χειραψία επιτρέπει στον server να αποδείξει την ταυτότητά του στον client χρησιμοποιώντας τεχνικές κρυπτογράφησης δημοσίου κλειδιού και στην συνέχεια επιτρέπει στον client και τον server να συνεργαστούν για την δημιουργία ενός συμμετρικού κλειδιού που θα χρησιμοποιηθεί στην γρήγορη κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που ανταλλάσσονται μεταξύ τους. Προαιρετικά η χειραψία επιτρέπει επίσης στον client να αποδείξει την ταυτότητά του στον server. Αναλυτικότερα, η διαδικασία χειραψίας έχει ως εξής:

1. Αρχικά ο client στέλνει στον server την έκδοση του SSL που χρησιμοποιεί, τον επιθυμητό αλγόριθμο κρυπτογράφησης, μερικά δεδομένα που έχουν παραχθεί τυχαία και οποιαδήποτε άλλη πληροφορία χρειάζεται ο server για να ξεκινήσει μία σύνδεση SSL.
2. Ο server απαντά στέλνοντας παρόμοιες πληροφορίες με προηγουμένως συμπεριλαμβανομένου όμως και του ψηφιακού πιστοποιητικού του, το οποίο τον πιστοποιεί στον client. Προαιρετικά μπορεί να ζητήσει και το ψηφιακό πιστοποιητικό του client.
3. Ο client λαμβάνει το ψηφιακό πιστοποιητικό του server και το χρησιμοποιεί για να τον πιστοποιήσει. Εάν η πιστοποίηση αυτή δεν καταστεί δυνατή, τότε ο χρήστης ενημερώνεται με ένα μήνυμα σφάλματος και η σύνδεση SSL ακυρώνεται. Εάν η πιστοποίηση του server γίνει χωρίς προβλήματα, τότε η διαδικασία της χειραψίας συνεχίζεται στο επόμενο βήμα.
4. Ο client συνεργάζεται με τον server και αποφασίζουν τον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιηθεί στην ασφαλή σύνδεση SSL. Επίσης ο client δημιουργεί το συμμετρικό κλειδί που θα χρησιμοποιηθεί στον αλγόριθμο κρυπτογράφησης και το στέλνει στον server κρυπτογραφημένο, χρησιμοποιώντας την τεχνική κρυπτογράφησης δημοσίου κλειδιού. Δηλαδή χρησιμοποιεί το δημόσιο κλειδί του server που αναγράφεται πάνω στο ψηφιακό του πιστοποιητικό για να κρυπτογραφήσει το συμμετρικό κλειδί και να του το στείλει. Στην συνέχεια ο server χρησιμοποιώντας το ιδιωτικό του κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα και να αποκτήσει το συμμετρικό κλειδί που θα χρησιμοποιηθεί για την σύνδεση.
5. Ο client στέλνει ένα μήνυμα στον server ενημερώνοντάς τον ότι είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
6. Ο server στέλνει ένα μήνυμα στον client ενημερώνοντάς τον ότι και αυτός είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
7. Από εδώ και πέρα η χειραψία έχει ολοκληρωθεί και τα μηνύματα που ανταλλάσσουν τα δύο μηχανήματα (client - server) είναι κρυπτογραφημένα.

Επιβάρυνση από το SSL

Η χρήση του πρωτοκόλλου SSL αυξάνει τα διακινούμενα πακέτα μεταξύ των δύο μηχανών και καθυστερεί την μετάδοση των πληροφοριών επειδή

χρησιμοποιεί μεθόδους κρυπτογράφησης και αποκρυπτογράφησης. Ειδικότερα οι διάφορες καθυστερήσεις εντοπίζονται στα εξής σημεία:

- Στην αρχική διαδικασία χειραψίας όπου κανονίζονται οι λεπτομέρειες της σύνδεσης και ανταλλάσσονται τα κλειδιά της συνόδου.
- Στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης που γίνεται στους δύο υπολογιστές με αποτέλεσμα να δαπανώνται υπολογιστικοί πόροι και χρόνος.
- Στην καθυστέρηση μετάδοσης των κρυπτογραφημένων δεδομένων αφού αυτά αποτελούνται από περισσότερα bytes σε σχέση με την αρχική μη κρυπτογραφημένη πληροφορία.

Λόγω αυτών των επιβαρύνσεων που εισάγει το πρωτόκολλο SSL, χρησιμοποιείται πλέον μονάχα σε περιπτώσεις όπου πραγματικά χρειάζεται ασφαλής σύνδεση (πχ μετάδοση κωδικών χρήστη ή αριθμών πιστωτικών καρτών μέσω του διαδικτύου) και όχι σε περιπτώσεις απλής επίσκεψης σε μία ιστοσελίδα.

PASSWORD AUTHENTICATION PROTOCOL

Το **Password Authentication Protocol** (*PAP*) είναι ένα απλό πρωτόκολλο αυθεντικοποίησης που χρησιμοποιείται για την αυθεντικοποίηση ενός χρήστη σε κάποιο Διακομιστή Πρόσβασης Δικτύου (Network Access Server, NAS) που μπορεί να χρησιμοποιείται για παράδειγμα από παρόχους υπηρεσιών ίντερνετ. Το PAP χρησιμοποιείται από το πρωτόκολλο PPP. Το PAP μεταδίδει μη κρυπτογραφημένους ASCII κωδικούς μέσω δικτύου και γι αυτό θεωρείται μη ασφαλές. Χρησιμοποιείται ως έσχατη λύση όταν ο απομακρυσμένος διακομιστής δεν υποστηρίζει πιο ισχυρό πρωτόκολλο αυθεντικοποίησης, όπως το CHAP ή το EAP.

Κύκλος εργασιών πρωτοκόλλου

1. Ο πελάτης αποστέλλει όνομα χρήστη και κωδικό πρόσβασης

2. Ο διακομιστής αποστέλλει μήνυμα authentication-ack, εάν τα διαπιστευτήρια είναι αποδεκτά ή εναλλακτικά authentication-nak, εάν δεν είναι αποδεκτά.

Το πακέτο PAP ενθυλακώνεται σε ένα PPP frame. Το πεδίο του πρωτοκόλλου έχει τιμή C023 (hex).

Flag	Address	Control	Flag	Payload (table above)	FCS

Ο αλγόριθμος DES ως πρότυπο

Παρά τις επικρίσεις, ο DES εγκρίθηκε ως ένα ομοσπονδιακό πρότυπο, το Νοέμβριο του 1976 και δημοσιεύθηκε στις 15 Ιανουαρίου του 1977 ως FIPS PUB 46 και η χρήση του ήταν επιτρεπτή σε όλα τα μη απόρρητα δεδομένα. Στη συνέχεια, επιβεβαιώθηκε ως το πρότυπο το1983, το1988 (αναθεωρήθηκε ως FIPS-46-1), το 1993 (ως FIPS-46-2) και πάλι το 1999 (ως FIPS-46-3). Ο τελευταίος ορισμός ήταν ο Triple DES. Στις 26 Μαΐου του 2002, ο DES τελικά εκτοπίστηκε από τον Advanced Encryption Standard (AES) κατόπιν δημόσιου διαγωνισμού. Στις 19 Μαΐου του 2005, ο FIPS 46-3 είχε επισήμως αποσυρθεί, αλλά το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology - NIST) ενέκρινε τον Triple DES στο έτος 2003 για τις ευαίσθητες πληροφορίες της κυβέρνησης. Μια άλλη θεωρητική επίθεση, η γραμμική κρυπτανάλυση δημοσιεύθηκε το 1994, αλλά ήταν μια επίθεση brute force το 1998 που αναπαράστησε/απέδειξε ότι μπορεί κάποιος θα μπορούσε να επιτεθεί στον DES πολύ πρακτικά και τονίστηκε η ανάγκη για αντικατάσταση του αλγόριθμου. Αυτές και άλλες μέθοδοι κρυπτανάλυσης εξετάζονται λεπτομερώς. Η εισαγωγή του DES θεωρείται ότι ήταν ένας καταλύτης για την ακαδημαϊκή μελέτη της

κρυπτογραφίας, ιδιαίτερα των μεθόδων για να "σπάνε" block κρυπταλγόριθμους, σύμφωνα με μια αναδρομή στο NIST για τον DES.

Ο DES, μπορεί να ειπωθεί, ότι το "αρχικό άλμα" του ξεπέρασε τις στρατιωτικές μελέτες και την ανάπτυξη των αλγορίθμων κρυπτογράφησης. Στη δεκαετία του 1970 υπήρχαν πολύ λίγοι κρυπτογράφοι, εκτός εκείνων των στρατιωτικών ή των μυστικών οργανώσεων και ελάχιστη ακαδημαϊκή μελέτη της κρυπτογραφίας. Υπάρχουν τώρα πολλοί δραστικοί ακαδημαϊκοί κρυπτολόγοι και μαθηματικά τμήματα με ισχυρά προγράμματα στην κρυπτογραφία και την ασφάλεια των πληροφοριών και των εμπορικών εταιρειών και συμβούλων. Μια γενιά κρυπταναλυτών έχει αναλύσει εξονυχιστικά τον αλγόριθμο DES προσπαθώντας να τον "σπάσουν". Ανέφεραν πως ο DES έκανε περισσότερα για να γαλβανίσει τον τομέα της κρυπτανάλυσης από οτιδήποτε άλλο και έτσι υπήρχε ένας αλγόριθμος για τη μελέτη. Ένα εκπληκτικό μερίδιο της ανοιχτής λογοτεχνίας στην κρυπτογραφία κατά τη δεκαετία του 1970 και του 1980 ασχολήθηκε με τον DES και ο DES είναι το πρότυπο ενάντια σε όλους τους αλγόριθμους συμμετρικού κλειδιού μετά από σύγκριση.

ΠΕΡΙΓΡΑΦΗ ΤΟΥ DES

Ο DES είναι ο αρχετυπικός block cipher, δηλαδή, ένας πρωτότυπος κρυπταλγόριθμος συμμετρικού κλειδιού, που λαμβάνει μια σειρά από plaintext bits (bits απλού κειμένου) σταθερού μήκους και την μετατρέπει μέσω μιας σειράς πολύπλοκων ενεργειών σε μια άλλη σειρά bit, το chiphertext (κρυπτοκείμενο) με το ίδιο μήκος. Στην περίπτωση του DES, το μέγεθος μπλοκ (block size: Η σειρά των bits σταθερού μήκους) είναι 64 bits. Ο DES χρησιμοποιεί επίσης ένα κλειδί για να προσαρμόσει τη μετατροπή, ώστε η αποκρυπτογρά-φηση να μπορεί, υποθετικά, να

πραγματοποιηθεί μόνο από εκείνους που γνωρίζουν το συγκεκριμένο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση. Το κλειδί φαινομενικά αποτελείται από 64 bits. Ωστόσο, στην πραγματικότητα, μόνο 56 από αυτά χρησιμοποιήθηκαν από τον αλγόριθμο. Τα υπόλοιπα 8 bits χρησιμοποιούνται αποκλειστικά για τον έλεγχο της ισοτιμίας (αρτιότητα) και στη συνέχεια απορρίπτονται. Αυτά τα 8 bits ονομάζονται parity bits. Εξ' ου και αναφέρεται συνήθως ως κλειδί μήκους των 56 bits. Όπως οι άλλοι block αλγόριθμοι κρυπτογράφησης, έτσι και ο DES από μόνος του δεν είναι ένας ασφαλής τρόπος κρυπτογράφησης, αλλά αντίθετα, πρέπει να χρησιμοποιηθεί με ένα ειδικό τρόπο λειτουργίας (mode of operation). Ο FIPS-81 ορίζει πολλούς τρόπους χρήσης με DES. Περαιτέρω παρατηρήσεις σχετικά με τη χρήση του DES περιέχονται στο FIPS-74.

Επίθεσεις brute-force (ωμής βίας) ο φόβος κάθε κρυπταλγόριθμου

Για οποιοδήποτε κρυπταλγόριθμο, η πιο βασική μέθοδος επίθεσης είναι η brute force — δοκιμάζοντας συνεχόμενα κάθε πιθανό κλειδί - Το μήκος του κλειδιού καθορίζει το πλήθος των πιθανών κλειδιών και ως εκ τούτου τη δυνατότητα πραγματοποίησης αυτής της προσέγγισης. Ερωτήσεις τέθηκαν από νωρίς για την επάρκεια του μήκους κλειδιού του DES πριν ακόμα υιοθετηθεί ως πρότυπο. Το μικρό μήκος κλειδιού ήταν αυτό που στην ουσία διέταξε την ανάγκη για την αντικατάσταση του αλγόριθμου, παρά η θεωρητική κρυπτανάλυση. Είναι γνωστό ότι η NSA ενθάρρυνε, αν δεν έπεισε, την IBM για να μειώσει το μήκος του κλειδιού από τα 128 bits στα 64 bits και από εκεί σε 56 bits. Αυτό λαμβάνεται συχνά ως ένδειξη ότι η NSA σκέφτηκε ότι θα ήταν σε θέση να “σπάσει” τα κλειδιά αυτού του μήκους ακόμη και στα μέσα της δεκαετίας του '70. Στον ακαδημαϊκό κόσμο, έγιναν διάφορες προηγμένες προτάσεις για μια μηχανή που θα αποσκοπούσε στο να “σπάει” τον DES. Το 1977, οι Diffie και Hellman πρότειναν μια μηχανή που κοστίζει κατ' εκτίμηση 20 εκατομμύρια δολάρια η οποία θα μπορούσε να βρει ένα κλειδί DES σε μία και μόνο ημέρα. Μέχρι το 1993, ο Wiener είχε προτείνει μια μηχανή

αναζήτησης κλειδιού με κοστολόγηση 1 εκατομμύριο δολάρια που θα έβρισκε ένα κλειδί μέσα σε 7 ώρες. Εντούτοις, καμία από αυτές τις πρόωρες προτάσεις δεν εφαρμόστηκε ˙ τουλάχιστον καμία εφαρμογή δεν αναγνωρίστηκε δημόσια. Η ευπάθεια του DES επιδείχθηκε πρακτικά προς το τέλος της δεκαετίας του '90. Το 1997, η εταιρεία RSA Security υποστήριξε μια σειρά διαγωνισμών, που προσέφερε ένα βραβείο $10.000 στην πρώτη ομάδα που θα "έσπαγε" ένα μήνυμα το οποίο κρυπτογραφήθηκε με τον DES για το διαγωνισμό. Εκείνος ο διαγωνισμός κερδήθηκε από το πρόγραμμα DESCHALL, που οδηγήθηκε από Rocke Verser, τον Matt Curtin, και τον Justin Dolske, χρησιμοποιώντας ιδανικούς κύκλους χιλιάδων υπολογιστών σε ολόκληρο το Διαδίκτυο. Η δυνατότητα πραγματοποίησης του "σπάσιμου" του DES γρήγορα καταδείχθηκε το 1998 όταν φτιάχτηκε μια "DES-σπάστης" συνήθειας από την EFF (Electronic Frontier Foundation), μια ομάδα αστικών δικαιωμάτων κυβερνοχώρου, με κόστος περίπου $250,000 (Εικόνα 4). Το κίνητρό τους ήταν να δείξουν ότι ο DES ήταν το ίδιο εύθραυστος στην πράξη όπως και στην θεωρία:

"Υπάρχουν πολλοί άνθρωποι που δεν θα πιστέψουν μια αλήθεια έως ότου μπορούν να τη δουν με τα μάτια τους. Δείχνοντάς τους μία φυσική μηχανή που μπορεί να "σπάσει" τον DES σε μερικές ημέρες είναι ο μόνος τρόπος να πειστούν μερικοί άνθρωποι ότι δεν μπορούν να εμπιστευθούν την ασφάλειά τους στον DES."

Η μηχανή εμφάνισε ένα κλειδί με χρήση brute force σε κάτι περισσότερο από 2 ημέρες. Περόπου στον ίδιο χρόνο ένας πληρεξούσιος από το αμερικανικό Υπουργείο Δικαιοσύνης ανήγγελλε ότι ο DES ήταν άθραυστος.

Η μόνη άλλη επιβεβαιωμένη μηχανή που "έσπαγε" τον DES ήταν η μηχανή COPACOBANA (σύντμηση του βέλτιστου κόστους και παράλληλα ενός code breaker) που χτίστηκε πιο πρόσφατα από τις ομάδες των πανεπιστημίων του Μπόχουν και του Κίελου της Γερμανίας.

Αντίθετα από τη μηχανή της EFF, η COPACOBANA αποτελείται από τα εμπορικά διαθέσιμα, ανασχηματισμένα ολοκληρωμένα κυκλώματα. 120 αυτών των FPGAs του τύπου XILINX Spartan3-1000 τρέχουν σε παράλληλη σύνδεση. Ομαδοποιούνται σε 20 DIMM ενότητες, που κάθε μια περιέχει 6 FPGAs. Η χρήση των ανασχηματισμένων hardware κάνει την μηχανή εφαρμόσιμη και σε άλλες λειτουργίες για "σπάσιμο" κωδικών. Η Εικόνα 5 δείχνει μία πλήρη μηχανή COPACOBANA. Μια από τις πιό ενδιαφέρουσες πτυχές COPACOBANA είναι ο παράγοντας του κόστους της. Μια μηχανή μπορεί να φτιαχτεί για περίπου $10.000. Η μείωση κόστους από έναν κατά προσέγγιση παράγοντα της τάξης των 25% από αυτή της μηχανής της EFF είναι ένα εντυπωσιακό παράδειγμα για τη συνεχή βελτίωση του ψηφιακού υλικού. Κατά ενδιαφέροντα τρόπο ο νόμος του Moore προβλέπει μια βελτίωση της τάξης περίπου 32%, δεδομένου ότι περίπου 8 έτη έχουν μεσολαβήσει μεταξύ του σχεδιασμού των δύο μηχανών, πράγμα το οποίο επιτρέπει περίπου πέντε διπλασιασμούς της δύναμης υπολογιστών (ή 5 μειώσεις τις τάξεως του 50% του κόστους για τον ίδιο υπολογισμό).

Επιθέσεις γρηγορότερες από την brute - force

Υπάρχουν τριων ειδών επιθέσεις που είναι γνωστό οτι μπορούν να "σπάσουν" ΚΑΙ τους δέκα έξι γύρους του DES με λιγότερη πολυπλοκότητα από μια αναζήτηση brute force:

Η Διαφορική Κρυπτανάλυση (Differential Cryptanalysis – DC)

Η Γραμμική Κρυπτανάλυση (Linear Cryptanalysis - LC) και τέλος

Η επίθεση του Davie (Davies' Attack)
Εντούτοις, οι επιθέσεις είναι θεωρητικές και είναι αδύνατο να τοποθετηθούν στην πράξη. Τέτοιου είδους επιθέσεις καλούνται μερικές φορές Certificational Weaknesses.

Όλα τα τα παραπάνω πρωτοκολλα και πρότυπα ασφάλειας και λειτουργίες του Virtual Mart υπάρχουν στο site της πτυχιακής μας

http://www.archwnmedia.com

2. ΒΙΒΛΙΟΓΡΑΦΙΑ

1. COMPUTER SECURITY AND CRYPTOGRAPHY by ALAN G. KONHEIM

2. Applied cryptography by Bruce Shneier

3. W. DIFFIE AND M. E. HELLMAN, "Multiuser Cryptographic Techniques," National Computer Conference

4. R. B. FOUGNER, "Public Key Standards and Licenses", RFC 1170, January 1991.

5. M. E. HELLMAN AND R. C. MERKLE, U.S. Patent No. 4,218,582, "Public Key Cryptographic Apparatus and

Method",

6. M. E. HELLMAN B. W. DIFFIE, AND R. C. MERKLE, U.S. Patent No. 4,200,770, "Cryptographic Apparatus and

Method",

7. R. L. RIVEST, A. SHAMIR, AND M. ADLEMAN, U.S. Patent No. 4,405,829, "Cryptographic Communications

System and Method",

8. U.S. Patent No. 4,218,582, “Public Key Cryptographic Apparatus and Method”, Martin E. Hellman and

Ralph C. Merkle

9. U.S. Patent No. 4,405,829, “Cryptographic Communications System and Method”, Ronald L. Rivest, Adi

Shamir and Leonard M. Adleman

10..Ghosh A. K., *E–Commerce Security*, John Wiley & Sons, 1998.

11.Gollmann D., *Computer Security*, J. Wiley & Sons, 1999.

12.Higgins R. & Woods R., ≪The business of the Internet≫, *Telecommunications.*

13.April 1998, pp. 39–47.

14..Howard J. D., *An analysis of security incidents on the Internet 1989–1995*, Ph.

15.D. Thesis, Carnegie Mellon University, Pittsburgh, 1997.

16.ISO 7498–2, *OSI/RM Security Architecture*.

17. Kou W., *Networking Security and Standards*, Kluwer Academic Publishers, 1997.

18. Loeb L., *Secure Electronic Transactions*, Artech House, 1998.

19. Meinel C. P., ≪How Hackers Break In … and How They Are Caught≫, *Scientific*

20. *American*, October 1998, pp. 70–77.

21. Muftic S., *Security Mechanisms for Computer Networks*, Ellis Horwood, 1989.

22. Purser M., *Secure Data Networking*, Norwood, MA, Artech House, 1993.

23. Rubin A. D. and Geer D. E., ≪A Survey of Web Security≫, *IEEE Computer*, 1998

24. Stallings W., *Cryptography and Network Security. Principles and Practice.*

25. Prentice–Hall Inc., 1999.

26. Stallings W., *Network and Internetwork Security: Principles and Practice*.

27. Prentice–Hall, Englewood Cliffs, 1995.

Η Ορολογία (Γλωσσάριο) της Κρυπτογραφίας

(AES) Advanced Encryption Standard - Το Advanced Encryption Standard, δηλ. το *Προηγμένο Πρότυπο Κρυπτογράφησης*, θα αποτελεί τον νέο στάνταρτ αλγόριθμο κρυπτογράφησης για χρήση από τις κυβερνητικές υπηρεσίες των ΗΠΑ. Επιλέχθηκε ο αλγόριθμος Rijndael από μια ομάδα υποψηφίων αλγορίθμων. Στοχεύεινα γίνει ο διάδοχος του DES και οι νεώτερες εκδόσεις των PGP και GPG περιλαμβάνουν υποστήριξη για το AES.

Algorithm - Αναφέρεται στον αλγόριθμο κρυπτογράφησης, που είναι μια μαθηματική διαδικασία (μέθοδος) κρυπτογράφησης (κωδικοποίησης) και αποκρυπτογράφησης (αποκωδικοποίησης) μηνυμάτων και κειμένων, τα οποία μετατρέπονται σε μια μη αναγνώσιμη μορφή.

Asymmetric Encryption - Αποδίδεται στα ελληνικά ως *Ασύμμετρη Κρυπτογράφηση* και είναι ένα σύγχρονο σύστημα κρυπτογράφησης, το οποίο με τη χρήση δύο κλειδιών (δημόσιο και ιδιωτικό) επιτυγχάνει σχεδόν απόλυτη προστασία των ευαίσθητων (απόρρητων) πληροφοριών (δεδομένων).

Authentication - Αποδίδεται στα ελληνικά με τον όρο *Ταυτοποίηση* ή *Πιστοποίηση* και είναι η διαδικασία ή μέθοδος επιβεβαίωσης (εξακρίβωσης) με τη χρήση ψηφιακών ταυτοτήτων ή πιστοποιητικών της ταυτότητας ενός ατόμου ώστε να έχει δικαίωμα για πρόσβαση σε διάφορα συστήματα. Στην ουσία αυτό που ζητάμε να μάθουμε είναι αν το άτομο ή η εταιρεία που ζητάει μια συναλλαγή είναι όντως αυτός ή αυτή που ισχυρίζεται ότι είναι. Ο ίδιος όρος αναφέρεται και στη διαδικασία επαλήθευσης ότι κάποιο αρχείο ή μήνυμα δεν έχει υποστεί κάποια τροποποίηση κατά τη μεταφορά του από τον αποστολέα ως τον παραλήπτη και ότι έχει παραληφθεί ακέραιο.

Authorization - Αποδίδεται στα ελληνικά με τον όρο *Εξουσιοδότηση* και είναι η διαδικασία σύμφωνα με την οποία γίνεται ο απαραίτητος έλεγχος από την τράπεζα του πελάτη (πληρωτή) ως προς το υπόλοιπο του λογαριασμού του, έτσι ώστε να εγκριθεί η εισαγωγή του σ' ένα δίκτυο και να δοθεί η σχετική εντολή πληρωμής στην τράπεζα του αποδέκτη. Το authorization επιτρέπει σ' έναν χρήστη την πρόσβαση σε περιοχές ή στο σύνολο ενός δικτύου βάσει της ταυτότητάς του.

Back Door - Αποδίδεται στα ελληνικά με τον όρο *Πίσω Πόρτα* ή και *Κερκόπορτα* και αναφέρεται σε ορισμένες αδυναμίες των λειτουργικών συστημάτων των υπολογιστών, τις οποίες μπορούν να εκμεταλλευτούν κάποιο επίδοξοι hackers ή crackers και να προκαλέσουν ζημιά ή απλά να καταγράφουν (παρακολουθούν) τις κινήσεις και τις επιλογές μας στο Internet ή και να υποκλέπτουν μυστικούς κωδικούς εν αγνοία μας.

Certification Authority (CA/TTP) - Αποδίδεται στα ελληνικά μ' έναν από τους όρους *Οργανισμός Πιστοποίησης* ή *Έμπιστη Τρίτη Οντότητα* ή και *Πάροχος Υπηρεσιών Πιστοποίησης* και αναφέρεται στους Οργανισμούς ή Εταιρείες που έχουν το δικαίωμα (άδεια) να εκδίδουν ψηφιακές ταυτότητες και να εγγυώνται μ' αυτόν τον τρόπο τη διασφάλιση (απόρρητο) των επικοινωνιών.

Chosen Plain Text Attack - Αποτελεί το επόμενο βήμα από την *Known Plain Text Attack*, όπου ο κρυπταναλυτής (cryptanalyst) μπορεί να επιλέξει ποιο μήνυμα plain text επιθυμεί να κρυπτογραφήσει και να δει το αποτέλεσμα, σ' αντίθεση από το πάρει απλά ένα παλιό plain text. Αν μπορέσει να ανακτήσει το κλειδί, μπορεί να το χρησιμοποιήσει για να αποκωδικοποιήσει όλα τα δεδομένα που είναι κρυπτογραφημένα κάτω απ' αυτό το κλειδί. Είναι μια πολύ πιο δυνατή μορφή επίθεσης σε σχέση με την known plain text. Τα καλύτερα συστήματα κρυπτογράφησης μπορούν να αντισταθούν σ' αυτή τη μορφή επίθεσης.

Cipher - Όρος που αναφέρεται στην κρυπτογράφηση (κωδικοποίηση) μηνυμάτων. Εϊναι συνώνυμος με τους όρους *Encryption* και *Encode*.

CipherText - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτογράφημα* και είναι το κρυπτογραφημένο (κωδικοποιημένο) αρχείο, κείμενο ή μήνυμα που στέλνει ο αποστολέας στον παραλήπτη. Το αρχικό (αυθεντικό), δηλ. το μη κρυπτογραφημένο μήνυμα, αποκαλείται *PlainText*.

Code - Αποδίδεται στα ελληνικά με τον όρο *Κώδικας* και αναφέρεται στη χρήση χαρακτήρων ή λέξεων για την αναπαράσταση άλλων λέξεων ή προτάσεων. Κλασικό παράδειγμα αποτελεί ο Κώδικας Morse, όπου με τον κατάλληλο συνδυασμό από τελείες και πάυλες μπορούμε να παραστήσουμε όλα τα γραμματα και τα ψηφία αλλά και μερικές τυποποιημένες προτάσεις.

Cracker - Χρήστης ο οποίος εισβάλει σε σύστημα στο οποίο δεν έχει νόμιμη πρόσβαση, με σκοπό να παραποιήσει ή ακόμη και να καταστρέψει δεδομένα και πληροφορίες ή και να δημιουργήσει παράνομα αντίγραφα νόμιμων προγραμμάτων.

Cryptography - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτογραφία* και είναι η προστασία των ευαίσθητων (απόρρητων) πληροφοριών (δεδομένων) με την μετατροπή τους από την απλή μορφή κειμένου, που αποκαλείται plain text, σε μια μη αναγνώσιμη μορφή, που αποκαλείται cipher text. Το κρυπτογραφημένο μήνυμα μπορεί να αποκρυπτογραφηθεί (decrypted) μόνο από τον κάτοχο ενός απόρρητου αλγορίθμου (encryption algorithm), που αποκαλείται κλειδί ή κλείδα (key).

Cryptoanalysis - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτανάλυση* και αναφέρεται στην τέχνη της παραβίασης, δηλ. της αποκρυπτογράφησης, των κρυπτοσυστημάτων. Μπορεί να αναφέρεται επίσης και στην εύρεση λαθών ή και ελλείψεων κατά την εφαρμογή ενός αλγορίθμου κρυπτογράφησης.

Cryptology - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτολογία* και αναφέρεται στη μελέτη (έρευνα) της κρυπτογραφίας και της κρυπτανάλυσης.

Cryptosystem - Αποδίδεται στα ελληνικά με τον όρο *Σύστημα Κρύπτο* και αναφέρεται στην όλη διαδικασία χρησιμοποίησης της κρυπτογραφίας, δηλ. στις μεθόδους κρυπτογράφησης και αποκρυπτογράφησης καθώς και στις μεθόδους διαπίστωσης της ταυτότητας του αποστολέα ενός μηνύματος.

Data Enrcyption - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτογράφηση Δεδομένων* και αναφέρεται στη χρήση μαθηματικών εργαλείων για την καθιέρωση της εμπιστοσύνης ανάμεσα στον αποστολέα και τον παραλήπτη (αποδέκτη) ενός μηνύματος. Η κύρια χρήση της κρυπτογραφίας είναι αυτή της κωδικοποίησης της πληροφορίας με τέτοιο τρόπο ώστε η αποκωδικοποίηση της να είναι δυνατή μόνο από τον τελικό αποδέκτη του μηνύματος. Για να γίνει αυτό ο τελικός αποδέκτης του μηνύματος αναγνωρίζεται από ένα ειδικό identifier, ευρύτερα γνωστό ως κλειδί αποκωδικοποίησης. Οι δύο σημαντικότερες μορφές (μέθοδοι) κρυπτογράφησης δεδομένων είναι η *Συμμετρική Κρυπτογράφηση* και η *Κρυπτογράφηση Δημόσιου Κλειδιού*, στην οποία ο κάθε χρήστης έχει τη δυνατότητα να δημιουργήσει ένα ζεύγος κλειδιών, δηλ. ένα γνωστό ή δημόσιο κλειδί (public key) και ένα κρυφό κλειδί (secret key) ή ιδιωτικό κλειδί (private key). Το δημόσιο κλειδί μπροεί να το δημοσιοποιήσει (κοινοποιήσει) σ' όλον τον κόσμο. Στη συμμετρική κρυπτογραφία, υπάρχει μόνο ένα κλειδί το οποίο χρησιμοποιείται τόσο για την κωδικοποίηση όσο και για αποκωδικοποίηση του μηνύματος, το οποίο κλειδί πρέπει να παραμένει κρυφό σ' όλους εκτός από τον αποστολέα και τον αποδέκτη του μηνύματος, πράγμα βέβαια δύσκολο σήμερα με τις εκπληκτικές δυνατότητες των hackers και των crackers. Η κρυπτογραφία με χρήση δημόσιου κλειδιού χρησιμοποιεί ένα πιο ευέλικτο και πιο ασφαλή σχήμα πιστοποίησης για την αποκωδικοποίηση των δεδομένων και ως εκ τούτου έχει επικρατήσει (με δημοφιλέστερες μορφές δεδομένων το PKI και το PGP).

Decryption - Αποδίδεται στα ελληνικά με τον όρο *Αποκρυπτογράφηση* και είναι η μέθοδος (διαδικασία) επαναφοράς ενός μηνύματος, που έχει κρυπτογραφηθεί σε μη αναγνώσιμη μορφή (cipher text), στην κανονική ή αρχική του του μορφή (plain text). Η αποκρυπτογράφηση μπορεί να γίνει μ' ένα απόρρητο ή μ' ένα δημόσιο (public key) ή και μ' έναν κωδικό πρόσβασης (password).

Data Encryption Standard (DES) - Αποδίδεται στα ελληνικά με τον όρο *Πρότυπο Κρυπτογράφησης Πληροφοριών* και είναι ένας είδος κρυπτογράφησης που δημιουργήθηκε από την κυβέρνηση των ΗΠΑ τη δεκαετία του 1970 ως ο επίσημος αλγόριθμος κρυπτογράφησης σε χρήση στις ΗΠΑ. Αναπτύχθηκε από την IBM υπό την αιγίδα της κυβέρνησης των ΗΠΑ. Αναπτύχθηκαν ανησυχίες ότι ίσως υπάρχουν κρυμμένες παγίδες στη λογική του αλγορίθμου που θα επέτρεπαν στην κυβέρνηση να σπάσει τον κωδικό μιας οποιασδήποτε επικοινωνίας. Το DES χρησιμοποιεί ένα κλειδί των 56 bit για να κάνει μια σειρά από μη γραμμικούς μετασχηματισμούς σ' έναν μπλοκ δεδομένων των 64 bit. Όμως, σήμερα με την ολοένα αυξανόμενη ταχύτητα του hardware και το χαμηλό του κόστος, είναι εφικτό να κατασκευασθεί ένα μηχάνημα που αν μπορεί να σπάισε ένα κλειδί των 56 bit σε μία μόνο ημέρα. Γι' αυτόν τον λόγο, έχει αναπτυχθεί το τριπλό-DES ή *3DES*, το οποίο χρησιμοποιεί το απλό-DES για να κρυπτογραφήσει τα δεδομένα, μετά τα αποκρυπτογραφεί μ' ένα άλλο κλειδί και κρυπτογραφεί ξανά το αποτέλεσμα μ' ένα άλλο κλειδί. Η κρυπτογράφηση που επιτυγχάνεται μ' αυτόν τον τρόπο είναι ισοδύναμη μ' ένα υποθετικό 112-bit DES.

Digital ID/Certificate - Αποδίδεται στα ελληνικά με τον όρο *Ψηφιακή Ταυτότητα* ή *Ψηφιακή Βεβαίωση* ή και *Ψηφιακό Πιστοποιητικό* και πρόκειται για μια κρυπτογραφημένη ταυτότητα που την εκδίδουν ειδικά εξουσιοδοτημένοι Οργανισμοί Παροχής Υπηρεσιών Πιστοποίησης, με την οποία επιβεβαιώνεται η γνησιότητα των στοιχείων του κατόχου, το ότι αυτός που στέλνει το μήνυμα είναι όντως αυτός που ισχυρίζεται ότι είναι και ότι δεν γίνεται ηλεκτρονική απάτη ή πλαστοπροσωπία. Μπορεί να την χρησιμοποιήσει ο κάτοχός της για να κάνει ασφαλείς ηλεκτρονικές συναλλαγές και επικοινωνία μέσω του Internet. Η ψηφιακή ταυτότητα περιλαμβάνει την ψηφιακή υπογραφή του κατόχου της (digital signature) και το δημόσιο κλειδί του (public key). Το πρότυπο που χρησιμοποιείται κυρίως στα ψηφιακά πιστοποιητικά είναι το X.509.

Digital Signature - Αποδίδεται στα ελληνικά με τον όρο *Ψηφιακή Υπογραφή* και πρόκειται για ειδικό αρχείο το οποίο δημιουργείται από κείμενο που το υπογράφει και το κρυπτογραφεί (κωδικοποιεί) ο κάτοχός του. Ο παραλήπτης

του μηνύματος θα πρέπει να κάνει αποκρυπτογράφηση του κειμένου, σύγκριση της ψηφιακής υπογραφής και πιστοποίηση (επιβεβαίωση) της ταυτότητας του αποστολέα του μηνύματος. Με την ψηφιακή υπογραφή μπορεί να γίνει η ηλεκτρονική πιστοποίηση (επιβεβαίωση) στοιχείων, όπως είναι η ταυτότητα ενός χρήστη, η ικανότητα πληρωμής ή και η γνησιότητα ενός ηλεκτρονικού εγγράφου.

Encryption - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτογράφηση* και είναι η μέθοδος (διαδικασία) μετατροπής κάποιων πληροφοριών (δεδομένων) σε απόρρητο (μη αναγνώσιμο) κώδικα, που είναι γνωστό και ως κρυπτογράφημα (cipher text). Αποτελεί την αποτελεσματικότερη μέθοδο για την επίτευξη της ασφάλειας στις επικοινωνίες. Για την ανάγνωση ενός κρυπτογραφημένου αρχείου είναι απαραίτητη η κατοχή του απόρρητου (ιδιωτικού) κλειδιού ή του κωδικού πρόσβασης, με τα οποία μπορεί να γίνει η αποκρυπτογράφηση των δεδομένων. Τα μη κρυπτογραφημένα δεδομένα ονομάζονται plain text, ενώ τα κρυπτογραφημένα δεδομένα ονομάζονται cipher text. Υπάρχουν δύο είδη κρυπτογράφησης : η *Ασύμμετρη Κρυπτογράφηση*, που είναι γνωστή και ως *Κρυπτογράφηση Δημόσιου Κλειδιού* και η *Συμμετρική Κρυπτογράφηση*.

Encryption Algorithm - Είναι ένας αλγόριθμος (μαθηματική μέθοδος) κρυπτογράφησης δεδομένων, με τη βοήθεια του οποίου μπορούμε να μετατρέψουμε κανονικό κείμενο (πληροφορία) σε μη αναγνώσιμη μορφή (cipher text). Για την επαναφορά των δεδομένων στην αρχική τους μορφή απαιτείται η ύπαρξη ειδικού κλειδιού.

Firewall - Ειδικό Πρόγραμμα (λογισμικό) ή και υλικό (hardware) που έχει τη δυνατότητα να ελέγχει ή και να απαγορεύει την απομακρυσμένη πρόσβαση σ' έναν υπολογιστή ή και να περιορίζει τις διαθέσιμες ιστοσελίδες σ' έναν προσωπικό υπολογιστή ή και σ' ένα δίκτυο υπολογιστών. Το firewall κάνει έλεγχο στα εισερχόμενα και εξερχόμενα δεδομένα από και προς τον υπολογιστή ή το δίκτυο από τη μια μεριά και το Internet από την άλλη.

Hacker - Χρήστης ο οποίος εισβάλει σε σύστημα στο οποίο δεν έχει νόμιμη πρόσβαση, αλλά μόνο για πειραματισμό και ευχάριστη απασχόληση καθώς και για να εντοπίσει και να υποδείξει κενά στα συστήματα ασφαλείας των υπολογιστικών συστημάτων. Διακρίνονται από τους λεγόμενους *Crackers*, οι οποίοι προκαλούν ζημιές ή κάνουν μη νόμιμες ενέργειες.

Hashing Algorithm - Ειδικός αλγόριθμος κρυπτογράφησης, με τη βοήθεια του οποίου δημιουργείται μια σύνοψη (περίληψη) ενός κειμένου (εγγράφου) σ' έναν αριθμό σταθερού μήκους, π.χ. 128 bits. Από δύο διαφορετικά έγγραφα είναι αστρονομικά αδύνατο να προκύψουν δύο ίδιοι κωδικοί των 128 bits. Η μέθοδος αυτή χρησιμοποιείται για να διαπιστωθεί η ακεραιότητα (integrity) ενός αποσταλέντος μηνύματος και όχι τόσο για την κρυπτογράφηση απόρρητων μηνυμάτων. Η διαδικασία που ακολουθείται είναι η εξής : ο αποστολέας του μηνύματος στέλνει το κανονικό μήνυμα σε απλή (όχι κωδικοποιημένη) μορφή μαζί με τον αριθμό που έχει προκύψει από την κρυπτογράφηση με τον αλγόριθμο hashing. Ο παραλήπτης εφαρμόζει στο ίδιο μήνυμα τον ίδιο αλγόριθμο hashing και συγκρίνει τους δύο αριθμούς των 128 bits που έχουν προκύψει, δηλ. αυτόν που έχει λάβει και αυτόν που έχει δημιουργήσει ο ίδιος και αν προκύψει διαφορά αυτό σημαίνει όυι το μήνυμα έχει αλλοιωθεί στην πορεία και θα πρέπει να ξανασταλεί.

HTTPS (Secure Hypertext Transfer Protocol) - Ασφαλές πρωτόκολλο για την ανταλλαγή κρυπτογραφημένων ιστοσελίδων ανάμεσα στον Web server και τον φυλλομετρητή (browser). Οι δικτυακοί τόποι που υποστηρίζουν το συγκεκριμένο πρωτόκολλο, στο πεδίο διευθύνσεων του φυλλομετρητή εμφανίζεται το https:// αντί του γνωστού http:// και στη γραμμή κατάστασης το σύμβολο μιας κλειδαριάς. Το πρωτόκολλο αυτό παρέχει ασφαλή διαχείριση των προσωπικών δεδομένων των χρηστών και χρησιμοποιείται συνήθως σε online συναλλαγές ή σε αποστολή στοιχείων πιστωτικής κάρτας κ.ά. Πρόκειται στην ουσία για μια ασφαλή μορφή του γνωστού πρωτοκόλλου μεταφοράς υπερκειμένου HTTP, ώστε να είναι εξασφαλισμένη η ανταλλαγή πληροφοριών ανάμεσα στον φυλλομετρητή και τον Web server.

(IDEA) International Data Encryption Algorithm - Αναπτύχθηκε στην Ελβετία και χρησιμοποιείται στο PGP 2.x ως ο συμμετρικός αλγόριθμος κρυπτογράφησης. Χρησιμοποιεί ένα κλειδί των 128 bit για να κάνει μια σειρά από μη γραμμικούς μαθηματικούς μετασχηματισμούς σ' ένα μπλοκ δεδομένων (data block) των 64 bit.

Key - Αποδίδεται στα ελληνικά με τον όρο *Κλειδί* ή και *Κλείδα* και είναι μια συλλογή από δυαδικά ψηφία που είναι αποθηκευμένα σ' ένα αρχείο που χρησιμοποιείται για την κρυπτογράφηφη ή αποκρυπτογράφηση ενός μηνύματος.

Key Escrow - Σε γενικές γραμμές, η διαδικασία key escrow σημαίνει ότι ένα αντίγραφο του μυστικού κλειδιού που είναι απαραίτητο στην αποκρυπτογράφηση αποθηκεύεται (φυλάσσεται) από κάποιον τρίτο, που μπορεί να είναι ένας συμβολαιογράφος ή μια τράπεζα, και οι οποίοι το κρατούν σε ασφάλεια σε περιπτωση απώλειας του κλειδιού ή θανάτου του

κατόχου του. Η χρήση του είναι κοινή και στις επιχειρήσεις, όπως όταν ένας υπάλληλος κατέχει κρυπτογραφημένο υλικό στον υπολογιστή της εταιρείας του και σε περίπτωση που συμβεί κάτι με τον υπάλληλο ή με τον υπολογιστή, η εταιρεία δεν θα μπορέσει να αποκρυπτογραφήσει τα μηνύματα. Γι' αυτόν τον λόγο, ένα αντίγραφο του μυστικού κλειδιού φυλάσσεται από έναν ή περισσότερους προϊσταμένους. Για να υπάρχει η εξασφάλιση ότι ένας προϊστάμενος δνε θα κάνει κατάχρηση της θέσης του, το κλειδί μπορεί να διαχωρισθεί και να μοιρασθεί σε πολλά άτομα, οι οποίοι θα πρέπει να συνεργασθούν για την ανάκτηση του κλειδιού.

Known Plain Text Attack - Είναι μια μέθοδος επίθεσης σ' ένα σύστημα κρυπτογράφησης όπου ο κρυπταναλυτής κατέχει αντίγραφα του plain text και του αντίστοιχου κρυτπογραφημένου κειμένου. Με τα ασθενέστερα συστήματα κρυτπογράφησης, η μέθοδος αυτή μπορεί να βελτιώσει τις πιθανότητες σπασίματος του κωδικού και απόκτησης του plain text των άλλων μηνυμάτων όπου το plain text δεν είναι γνωστό.

Message Digest Algorithm #5 (MD5) - Ο MD5 Message Digest Algorithm είναι ο αλγόριθμος σύνοψης μηνύματος που χρησιμοποιείται στο PGP. Υπολογίζεται ότι η πιθανότητα να έχουν δύο μηνύματα την ίδια σύνοψη είναι μετά από 2^{64} περιπτώσεις και ότι η πιθανότητα να έχει ένα οποιοδήποτε μήνυμα μια δεδομένη σύνοψη μηνύματος είναι είναι μετά από 2^{128} περιπτώσεις. Ο αλγόριθμος MD5 είναι ένας καινούργιος αλγόριθμος αλλά το επίπεδο ασφαλείας που παρέχει είναι αρκετό για την υλοποίηση ψηφιακών υπογαρφών υψηλών απαιτήσεων που βασίζονται στο MD5 και το RSA.

One Time Pad (OTP) - Το one time pad είναι το μόνο σχήμα κρυπτογράφησης (encryption scheme) που μπορεί να αποδειχθεί ότι είναι απολύτως απαραβίαστο. Χρησιμοποιείται πολύ από τους κατασκόπους καθώς δεν απιατεί κάποιον μηχανισμό (hardware) για να υλοποιηθεί και λόγω της απόλυτης ασφάλειας που παρέχει. Αυτός ο αλγόριθμος απαιτεί τη δημιουργία πολλών συνόλων από keys pads, όπου το κάθε pad αποτελείται από έναν αριθμό από τυχαίους χαρακτήρες κλειδιών. Each party involved receives matching sets of pads. Ο κάθε χαρακτήρας κλειδιού στο pad χρησιμοποιείται για να κρυπτογραφήσει έναν μόνο χαρακτήρα plain text και μετά δεν χρησιμοποιείται ποτέ ξανά. Ο λόγος που δεν χρησιμοποιείται ευρέως αυτό το σχήμα κρυπτογράφησης είναι ότι λόγω της πολυπλοκότητάς του δεν είναι κατάλληλο για τα σύγχρονα συστήματα επικοινωνιών που έχουν μεγάλες απαιτήσεις σε ταχύτητα. Ένα από τα διασημότερα links επικοινωνίας που χρησιμοποιούν αυτό το σχήμα είναι η κόκκινη γραμμή Ουάσινγκτον - Μόσχας.

Passphrase - Αποδίδεται στα ελληνικά με τον όρο *Συνθηματική Λέξη* ή και *Κωδική Φράση* και είναι ουσιαστικά το ίδιο πράγμα με το Password με τη διαφορά ότι είναι πιο περίπλοκο και συνεπώς πιο δύσκολο να εντοπισθεί.

Password - Αποδίδεται στα ελληνικά με τον όρο *Συνθηματικό* ή και *Κωδικός Πρόσβασης* και είναι μια μοναδική και απόρρητη λέξη κλειδί με την οποία σε συνδυασμό με το όνομα χρήστη (username) μπορούμε να αποδείξουμε την ταυτότητά μας όταν εισερχόμαστε σε περιορισμένης πρόσβασης σελίδες ή εφαρμογές ή σε πύλες (portals) ή και αλλού. Αποτελεί καλή τακτική να αλλάζουμε συχνά το password μας και να μην χρησιμοποιούμε κωδικούς που να μπορεί εύκολα να τους μαντέψει κάποιος αλλά περίεργους συνδυασμούς από γράμματα, ψηφία και σύμβολα.

PGP (Pretty Good Privacy) - Αποτελεί ένα από τα πιο δημοφιλή προγράμματα που χρησιμοποιούνται για την κρυπτογράφηση μηνυμάτων και την αποστολή τους μέσω του Internet. Χρησιμοποιεί την κρυπτογράφηση με συνδυασμό δημόσιου και ιδιωτικού κλειδιού (public key - private key). Θεωρείται απόλυτα ασφαλές. Το δημόσιο κλειδί είναι γνωστό σ' όλους και μπορούμε να το κατεβάσουμε (download) από κάποια ιστοσελίδα, ενώ το ιδιωτικό κλειδί είναι αυστηρά προσωπικό για τον κάθε χρήστη. Ό,τι κωδικοποιείται με το ένα κλειδί μπορεί να αποκωδικοποιηθεί με το άλλο και αντίστροφα. Όμως, είναι εξαιρετικά δύσκολη, αν όχι αδύνατη, η εύρεση του ιδιωτικού κλειδιού όταν γνωρίζουμε το δημόσιο κλειδί ενός χρήστη. Όταν ένα μήνυμα κωδικοποιείται με το ιδιωτικό κλειδί ενός χρήστη, μπορεί να αποκωδικοποιηθεί από οποιονδήποτε τρίτο με το γνωστό δημόσιο κλειδί του ίδιου χρήστη, αλλά αυτό αποτελεί μια επιβεβαίωση της ταυτότητας του χρήστη. Επίσης, η κωδικοποίηση ενός μηνύματος με το δημόσιο κλειδί ενός χρήστη εξασφαλίζει το ότι μόνο ο συγκεκριμένος χρήστης θα μπορέσει να το αποκωδικοποιήσει.

PlainText - Είναι το αυθεντικό (αρχικό) αρχείο, κείμενο ή μήνυμα, το οποίο πρέπει να λάβει κανονικά ο παραλήπτης. Το κρυπτογραφημένο μήνυμα που αποστέλνεται αποκαλείται *CipherText (Κρυπτογράφημα)*.

Private Key - Αποδίδεται στα ελληνικά με τον όρο *Ιδιωτικό Κλειδί* και είναι το μυστικό (κρυφό) κλειδί ενός κρυπτογραφικού συστήματος. Μπορεί να το χρησιμοποιεί ο κάτοχός του για να υπογράφει ηλεκτρονικά τα εξερχόμενα μηνύματά του καθώς και για να αποκρυπτογραφεί τα εισερχόμενα μηνύματά του.

Public Key - Αποδίδεται στα ελληνικά με τον όρο *Δημόσιο Κλειδί* και είναι το κοινό κλειδί ενός κρυπτογραφικού συστήματος. Μπορεί να το χρησιμοποιεί ένας οποιοσδήποτε τρίτος για να κρυπτογραφεί τα εξερχόμενα μηνύματά του προς τον κάτοχο του αντίστοιχου ιδιωτικού κλειδιού καθώς και για να αποκρυπτογραφεί τα εισερχόμενα μηνύματα που έχουν κωδικοποιηθεί με το ιδιωτικό κλειδί του αποστολέα.

Public Key Encryption - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτογράφηση με Δημόσιο Κλειδί* και πρόκειται για ένα σύστημα (τεχνική) κρυπτογράφησης που χρησιμοποιεί έναν συνδυασμό από ένα δημόσιο και ένα ιδιωτικό κλειδί για την κρυπτογράφηση των μηνυμάτων. Με τον τρόπο αυτό αποφεύγουμε την αποστολή του κλειδιού από τον αποστολέα στον παραλήπτη, κάτι που είναι πολύ επικίνδυνο για υποκλοπή. Η τεχνική αυτή κρυπτογράφησης λειτουργεί μ' έναν εμπιστευτικό κωδικό του νόμιμου χρήστη, που είναι το γνωστό ιδιωτικό κλειδί (private key), και μ' έναν δημόσιο κωδικό, που είναι το γνωστό δημόσιο κλειδί (public key), και το οποίο διανέμεται (δίνεται) ελεύθερα μέσω του Internet ή και ως συνημμένο σ' ένα e-mail. Οι δύο αυτοί κωδικοί αποτελούν από κοινού ένα μοναδικό ζεύγος κλειδιού με το οποίο επιτυγχάνεται η αποκρυπτογράφηση των δεδομένων.

Registered User - Όρος που αναφέρεται σ' έναν εγγεγραμμένο χρήστη μιας online υπηρεσίας, ο οποίος προσδιορίζεται από το όνομα χρήστη και τον προσωπικό (απόρρητο) κωδικό πρόσβασης και ενδεχομένως από κάποια επιπλέον στοιχεία.

RSA - Μια μέθοδος κρυπτογράφησης δημόσιου κλειδιού που μπορεί να χρησιμοποιηθεί και για την κρυπτογράφηση μηνυμάτων και για τη δημιουργία ψηφιακών υπογραφών, δηλ. για την επιβεβαίωση της ταυτότητας του αποστολέα ενός μηνύματος. Το RSA είναι η μέθοδος κρυπτογράφησης δημοσίου κλειδιού που χρησιμοποιείται στο PGP. Τα αρχικά του RSA αναφέρονται στους δημιουργούς του αλγορίθμου *(Rivest-Shamir-Adleman)*. Η βασική ασφάλεια στο RSA προέρχεται από το γεγονός ότι, ενώ είναι σχετικά εύκολο να πολλαπλασιάσουμε δύο μεγάλους πρώτους αριθμούς και να πάρουμε το γινόμενό τους, είναι υπολογιστικά δύσκολο να κάνουμε το αντίστροφο, δηλ. το να βρούμε τους δύο πρώτους παράγοντες ενός δεδομένου σύνθετου αριθμού. Είναι αυτή η φύση του RSA που επιτρέπει τη δημιουργία και την αποκάλυψη στον κόσμο ενός κλειδιού κρυπτογράφησης, ενώ από την άλλη μεριά δεν επιτρέπει την αποκρυπτογράφηση ενός μνηνύματος.

Secret Key Encryption - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτογράφηση με Κρυφό Κλειδί* και πρόκειται για ένα σύστημα κρυπτογράφησης με το οποίο αποστέλλεται στον παραλήπτη το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ενός μηνύματος.

Secure Web Server - Ένας Web server που εργάζεται με πιστοποιητικά (πρωτόκολλα) ασφαλείας. Οι συνδέσεις που γίνονται μ' έναν τέτοιο Web server είναι ασφαλείς και όλα τα μηνύματα (δεδομένα) που ανταλλάσσονται με τους πελάτες (clients) του είναι κρυπτογραφημένα.

SET (Secure Electronic Transaction) - Πρόκειται για ένα σύστημα ασφαλών τραπεζικών πληρωμών που έχει δημιουργηθεί από γνωστές εταιρείες πιστωτικών καρτών. Χρησιμοποιεί τη λεγόμενη *Έμπιστη Τρίτη Οντότητα (Third Trusted Party)* στις συναλλαγές εμπόρου-πελάτη, δηλ. μια ιδιωτική εταιρεία εμπιστοσύνης που παρεμβάλλεται ως τρίτος στις συνδιαλλαγές και εκδίδει τα ψηφιακά πιστοποιητικά ταυτότητας των συναλλασσομένων. Τα κρυπτογραφικά αυτά πρωτόκολλα σχεδιάστηκαν και αναπτύχθηκαν από κοινού από τις εταιρείες Visa, MasterCard, Netscape & Microsoft προκειμένου να παρέχουν ασφαλείς συναλλαγές με πιστωτικές κάρτες στο Διαδίκτυο για τους καταναλωτές (επλάτες) και τους πωλητές.

Spam e-mail - Έτσι αποκαλούνται τα e-mails που έχουν ενοχλητικό και συνήθως διαφημιστικό περιεχόμενο και που έχουν κατακλείσει το Internet τελευταία. Αποτελούν μια πολύ φθηνή μέθοδο διαφήμισης και προώθησης προϊόντων αλλά και marketing. Στα spam e-mails συγκαταλέγονται ανεπιθύμητες διαφημίσεις για προϊόντα, υπηρεσίες και sites καθώς επίσης και διάφοροι άλλοι τύποι e-mail (newsletters, chain mails κ.ά.).

SSL (Secure Sockets Layer)- Πρόκειται για ένα σύστημα (πρωτόκολλο) κρυπτογράφησης που έχει δημιουργήσει η γνωστή εταιρεία Netscape, με σκοπό την ασφαλή σύνδεση (επικοινωνία) ενός φυλλομετρητή με τον Web server. Τα δεδομένα που στέλνονται ανάμεσα στους δύο είναι κρυπτογραφημένα αλλά το σύστημα δεν εξασφαλίζει την ταυτότητα ούτε του αποστολέα ούτε του παραλήπτη. Είναι ειδικό πρωτόκολλο επικοινωνίας ανάμεσα σε browsers και servers και το οποίο κρυπτογραφεί κάθε online επικοινωνία. Το πρωτόκολλο αυτό διασφαλίζει συναλλαγές με διαφάνεια στους τελικούς χρήστες.

Steganography - Αποδίδεται στα ελληνικά με τον όρο *Στεγανογραφία* και είναι η διαδικασία απόκρυψης πληροφοριών μέσα σ' ένα άλλο πακέτο πληροφοριών και δεδομένων. Με τον τρόπο αυτό μπορούμε να αποκρύψουμε ένα αρχείο κειμένου μέσα σε κάποιο αρχείο εικόνας ή και ήχου, ώστε να μην γίνεται κατανοητό από τον παραλήπτη του αρχείου εικόνας ή ήχου.

Symmetric Encryption - Αποδίδεται στα ελληνικά με τον όρο *Συμμετρική Κρυπτογράφηση* και είναι μια από τις πρώτες μορφές κρυπτογραφίας που χρησιμοποιεί το ίδιο κλειδί τόσο για την κωδικοποίηση όσο και για την αποκωδικοποίηση του μηνύματος. Υπάρχει και η *Ασύμμετρη Κρυπτογράφηση (Asymmetric Encryption)*, η οποία χρησιμοποιεί δύο διαφορετικά κλειδιά (δημόσιο και ιδιωτικό).

Symmetric Key - Αποδίδεται στα ελληνικά με τον όρο *Συμμετρικό Κλειδί* και είναι η παλιά μέθοδος κρυπτογράφησης που χρησιμοποιεί το ίδιο κλειδί τόσο για την κωδικοποίηση όσο και για την αποκωδικοποίηση του μηνύματος. Δεν χρησιμοποιείται σήμερα καθώς δεν είναι ασφαλής μέθοδος επικοινωνίας.

TripleDES - Είναι μια μέθοδος βελτίωσης των δυνατοτήτων του αλγορίθμου DES, η οποία χρησιμοποιεί τον ίδιο αλγόριθμο τρεις φορές σε αλληλουχία με διαφορετικά κλειδιά, για μεγαλύτερη ασφάλεια.

User Identification - Αναφέρεται στην πιστοποίηση, δηλ. στον έλεγχο της ταυτότητας ή του δικαιώματος πρόσβασης σ' έναν δικτυακό τόπο, που γίνεται με το όνομα χρήστη και τον κωδικό πρόσβασης.

Username - Αποδίδεται στα ελληνικά με τον όρο *Όνομα Χρήστη* ή και *Αναγνωριστικό* και χρησιμοποιείται συνήθως σε συνδυασμό μ' έναν Κωδικό Πρόσβασης (Password) για την εισαγωγή σ' ένα σύστημα ή δίκτυο πολλαπλών χρηστών. Συνήθως ο χρήστης μπορεί να επιλέξει ο ίδιος το δικό του username (που πρέπει να είναι μοναδικό, στο πλαίσιο ενός δικτύου ή συστήματος) και το password, το οποίο δεν είναι απαραίτητο να είναι μοναδικό αλλά θα πρέπει να είναι απόρρητο και δύσκολο στο να μπορέσει να το εντοπίσει κάποιος.

Verisign - Μια από τις πιο γνωστές διεθνώς εταιρείες που λειτουργεί ως Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ) και εκδίδει ψηφιακές ταυτότητες (digital ID's) σε τρίτους (ιδιώτες ή και εταρείες). Οι εταιρείες αυτές αποκαλούνται και Έμπιστες Τρίτες Οντότητες (ΕΤΟ), δηλ. Trusted Third Parties (TTP), ή και Αρχές Πιστοποίησης (CA, Certification Authorities). Μια εταιρεία Παροχής Υπηρεσιών Πιστοποίησης μπορεί να εξουσιοδοτήσει άλλες εταιρείες σ' άλλες χώρες ή και σ' άλλες πόλεις για να κάνουν πιστοποίηση και να σχηματιστεί έτσι ένα δένδρο από τους Οργανισμούς Πιστοποίησης.

X.509 - Ένα από τα πιο διαδεδομένα πρότυπα για τη δημιουργία ψηφιακών πιστοποιητικών.

Η Ορολογία (Γλωσσάριο) του e-commerce

Acceptable Use Policy (AUP) - Είναι η *Αποδεκτή Πολιτική Χρήσης* ενός δικτυακού τόπου από τους επισκέπτες του. Μεγάλες εταιρείες, σχολικές μονάδες και παροχείς υπηρεσιών Internet (ISPs) μπορούν να δημιουργήσουν δικά τους AUPs με στόχο την πρόληψη του spamming ή της πειρατείας ή και άλλων παράνομων ενεργειών.

Acquiring Bank - Αποδίδεται στα ελληνικά με τον όρο *Τράπεζα Υποδοχής* και είναι η τράπεζα στην οποία μπορεί να ανοίξει λογαριασμό ένας επιχειρηματίας ώστε να δέχεται τις πληρωμές για τις ηλεκτρονικές του συναλλαγές.

Ad Click - Είναι το κλικ που κάνουμε με το ποντίκι σε μια διαφήμιση που υπάρχει σε μια ιστοσελίδα, από την οποία μεταβαίνουμε σε μια άλλη ιστοσελίδα, συνήθως του διαφημιζόμενου. Τα Ad Clicks μετριούνται από ειδικούς servers, τους Ad Servers.

Ad Impression - Η ολοκληρωμένη εμφάνιση μιας online διαφήμισης, όπως μπορεί να είναι ένα Banner, μέσα σε μια ιστοσελίδα.

Ad Management - Όρος που αναφέρεται στη διαχείριση των online διαφημίσεων (Banners, Buttons) μέσω κάποιου ειδικού προγράμματος διαχείρισης.

Ad Server - Ειδικό πρόγραμμα για τη διαχείριση των διαφημιστικών εκστρατειών, το οποίο είναι εγκατεστημένο σε κάποιον server και που η δουλειά του είναι ο προγραμματισμός και η εμφάνιση των online διαφημιστικών εκστρατειών. Παρέχει χρήσιμα στατιστικά στοιχεία για την απόδοση της διαφημιστικής εκστρατείας.

Ad Units - Τρόπος ταξινόμησης τύπων διαφήμισης. Στο Διαδίκτυο ad units είναι τα *banners*, τα *buttons*, τα *micro buttons*, τα *pop-ups*, οι *ουρανοξύστες (skyscrapers)*, οι *σύνδεσμοι (links)*, τα *interstitials*, τα *superstitials* κ.ά.

ADSL (Asymmetric Digital Subscriber Line) - Καινούργια τεχνολογία για τη μετάδοση ψηφιακών πληροφοριών μέσα από τα ήδη υπάρχοντα τηλεφωνικά καλώδια. Πλεονεκτεί έναντι της τεχνολογίας ISDN στο ότι παρέχει συνεχή σύνδεση με το Internet επί 24ωρου βάσεως, χωρίς να χρειάζεται να κάνουμε κλήση (dial up) κάθε φορά που θέλουμε να συνδεθούμε. Ο συνδρομητής δεν χρεώνεται με το κόστος της κάθε κλήσης που κάνει για σύνδεση στο Internet αλλά μ' ένα σταθερό μηνιαίο πάγιο, ανάλογα με την ταχύτητα σύνδεσης που έχει επιλέξει απ' αυτές που του προσφέρει ο Παροχέας (ISP). Με την ADSL σύνδεση έχουμε και τη δυνατότητα για ταυτόχρονη χρήση δύο τηλεφωνικών γραμμών και το modem της ADSL γραμμής μπορεί να παίξει και τον ρόλο του δρομολογητή (router) σ' ένα τοπικό δίκτυο υπολογιστών (LAN). Η τεχνολογία ADSL παρέχει ασυμμετρικό εύρος δεδομένων (bandwidth) μέσω ενός ζεύγους καλωδίων, το οποίο πρακτικά σημαίνει ότι το εισερχόμενο bandwidth (από το δίκτυο προς τον χρήστη) είναι μεγαλύτερο από το εξερχόμενο (από τον χρήστη προς το δίκτυο).

Affiliate Marketing - Διαφημιστικό σύστημα σύμφωνα με το οποίο ένας δικτυακός τόπος μπορεί να προβάλλει δωρεάν τα banners των διαφημιζομένων και να λαμβάνει ποσοστά κάθε φορά που γίνεται κάποια πώληση ή εγγραφή από τους επισκέπτες του συγκεκριμένου banner.

Affinity Marketing - Μια προσπάθεια προβολής και διαφήμισης ενός δικτυακού τόπου που περιλαμβάνει e-mail marketing, banner ή και συμβατικά μέσα και προσπαθεί να εντοπίσει τις καταναλωτικές (αγοραστικές) συνήθειες των χρηστών του Διαδικτύου. Για παράδειγμα ένα βιβλιοπωλείο που εξειδικεύεται σε νομικά βιβλία, μπορεί να στείλει ένα διαφημιστικό μήνυμα ηλεκτρονικού ταχυδρομείου σ' όλους τους πελάτες του που έχουν αγοράσει στο παρελθόν βιβλία πληροφορικής, με θέμα μηνύματος "Δίκαιο και Internet" και να αναφέρεται σε καινούργιες κυκλοφορίες σχετικών βιβλίων.

Aggregator - Όρος που αναφέρεται σε ειδικά προγράμματα που προσπαθούν να εξυπηρετήσουν τους χρήστες που κάνουν αγορές με ηλεκτρονικό εμπόριο, βοηθώντας τους να επιλέξουν ανάμεσα σε ανταγωνιστικές εταιρίες. Τα προγράμματα αυτά συγκεντρώνουν πληροφορίες για την αγορά και τους προμηθευτές και παρέχουν αυτά τα στοιχεία σ' έναν δικτυακό τόπο.

Authentication - Αποδίδεται στα ελληνικά με τον όρο *Ταυτοποίηση* ή *Πιστοποίηση* και είναι η διαδικασία επιβεβαίωσης με τη χρήση ψηφιακών ταυτοτήτων ή πιστοποιητικών, τού ότι το άτομο ή η εταιρεία που ζητάει μια συναλλαγή είναι όντως αυτός ή αυτή που ισχυρίζεται ότι είναι.

Authorization - Αποδίδεται στα ελληνικά με τον όρο *Εξουσιοδότηση* και είναι η διαδικασία σύμφωνα με την οποία γίνεται ο απαραίτητος έλεγχος από την τράπεζα του πελάτη (πληρωτή) ως προς το υπόλοιπο του λογαριασμού του, έτσι ώστε να δοθεί η σχετική εντολή πληρωμής στην τράπεζα του αποδέκτη.

B2B (Business-to-Business) - Όρος που αναφέρεται στο Ηλεκτρονικό Εμπόριο ανάμεσα σε εταιρείες, επιχειρήσεις ή και οργανισμούς (χονδρική πώληση).

B2C (Business-to-Consumer) - Όρος που αναφέρεται στο Ηλεκτρονικό Εμπόριο ανάμεσα σε επιχειρήσεις και στο ευρύτερο καταναλωτικό κοινό (λιανική πώληση).

B2G (Business-to-Government) - Όρος που αναφέρεται στο Ηλεκτρονικό Εμπόριο ανάμεσα σε επιχειρήσεις και κυβερνητικούς ή δημόσιους οργανισμούς.

Banner - Όρος που αναφέρεται σε μια διαφημιστική εικόνα που χρησιμοποιείται σε μια online διαφήμιση. Τα banners διακρίνονται σε στατικά, που είναι ακίνητα δισδιάστατα γραφικά, και σε κινούμενα (animated), που είναι κινούμενα γραφικά. Τα interactive banners έχουν κι έναν σύνδεσμο (link) προς την ιστοσελίδα του διαφημιζόμενου.

Brochureware - Ένας είδος δικτυακού τόπου που έχει την εμφάνιση μιας ηλεκτρονικής μπροσούρας, μπορεί να περιέχει δηλαδή τα στοιχεία επικοινωνίας της εταιρείας, μια σύντομη περιγραφή των προϊόντων ή/και των υπηρεσιών της, γενικότερες πληροφορίες για την επιχείρηση, συχνές ερωτήσεις-απαντήσεις (FAQs) κ.ά.

Burnout - Έκφραση που αναφέρεται στο «κάψιμο» μιας online διαφημιστικής εκστρατείας λόγω του ότι έμεινε για μεγάλο χρονικό διάστημα με τα ίδια διαφημιστικά στοιχεία (banners, buttons). Η διαφήμιση δεν αποδίδει τα αναμενόμενα και το Click Through Rate μειώνεται καθώς οι χρήστες έχουν βαρεθεί να βλέπουν το ίδιο banner με το ίδιο διαφημιστικό μήνυμα. Υπολογίζεται ότι ένα banner έχει πετύχει τον σκοπό του μετά από τρεις εμφανίσεις ανά χρήστη και τότε θα πρέπει να αλλαχθεί. Οι Ad Servers χρησιμοποιούν ειδικά φίλτρα και Cookies ώστε να αντιμετωπίσουν αυτό το πρόβλημα και έτσι μόλις ο ίδιος χρήστης δει τρεις φορές ένα συγκεκριμένο banner, τότε τού εμφανίζεται ένα άλλο.

Business Intelligence (BI) - Αποδίδεται στα ελληνικά ως *Επιχειρηματική Ευφυΐα/Νοημοσύνη* και αναφέρεται στην αμφίδρομη διαδικασία ανάλυσης και αξιοποίησης κάποιων καλά οργανωμένων και δομημένων πληροφοριών, με τη βοήθεια των οποίων η διοίκηση μιας επιχείρησης παρακολουθεί αποτελεσματικότερα τις νέες τάσεις και τα νέα καταναλωτικά πρότυπα, εξάγει χρήσιμα συμπεράσματα και μπορεί να λάβει έτσι σωστότερες αποφάσεις. Η Επιχειρηματική Ευφυΐα αφορά σε πελάτες, προϊόντα, υπηρεσίες ή και ανταγωνιστές.

Certification Authority (CA/TTP) - Αποδίδεται στα ελληνικά μ' έναν από τους όρους *Οργανισμός Πιστοποίησης* ή *Έμπιστη Τρίτη Οντότητα* ή και *Πάροχος Υπηρεσιών Πιστοποίησης* και αναφέρεται στους Οργανισμούς ή Εταιρείες που έχουν το δικαίωμα (άδεια) να εκδίδουν ψηφιακές ταυτότητες και να εγγυώνται μ' αυτόν τον τρόπο τη διασφάλιση (απόρρητο) των επικοινωνιών.

Click Through Rate - Όρος που αναφέρεται στον λόγο (αναλογία) μεταξύ των εμφανίσεων (Ad Impressions) μιας online διαφήμισης σε μια ιστοσελίδα και των κλικ (Ad Clicks) που έκαναν σ' αυτήν οι χρήστες. Μ' άλλα λόγια, το Click Through Rate φανερώνει το ποσοστό των χρηστών που έκαναν κλικ σε μια online διαφήμιση σε σχέση μ' αυτούς που την είδαν. Υπολογίζεται ως το πηλίκο των συνολικών Ad Clicks ανά εκατό εμφανίσεις (Ad Impressions). Για παράδειγμα ένα 5% Click Through Rate σημαίνει ότι στους 100 χρήστες που θεωρητικά είδαν ένα banner, έκαναν κλικ οι 5. Το Click Through Rate υπολογίζεται αυτόματα από τους Ad Servers και κυμαίνεται συνήθως μεταξύ 0,5% - 2%.

Commerce Service Provider (CSP) - Εταιρεία Παροχής Υπηρεσιών Διαδικτύου (ISP) που εξειδικεύεται σε υπηρεσίες ηλεκτρονικού εμπορίου αλλά και όσοι προσφέρουν ειδικό λογισμικό ή υποστήριξη γι' αυτές τις υπηρεσίες.

Conversion Rate - Ποσοστό χρηστών που αφού είδαν και έκαναν κλικ σε μια διαφήμιση, επισκέφτηκαν το site του διαφημιζόμενου και τελικά αγόρασαν μια υπηρεσία ή ένα προϊόν. Αποτελεί συνήθως το 1% - 5% των επισκεπτών που προέρχονται από μια διαφήμιση.

CPO (Cost per Order) - Όρος που αναφέρεται στο κόστος της αγοράς ενός προϊόντος ή μιας υπηρεσίας από έναν χρήστη, η οποία αγορά έγινε μέσα από μια online διαφήμιση. Υπολογίζεται αν διαιρέσουμε το κόστος της διαφημιστικής εκστρατείας με τις συνολικές αγορές που τελικά έγιναν.

CRM (Customer Relationship Management) - Όρος που αναφέρεται στη διαχείριση των σχέσεων μιας επιχείρησης με τους πελάτες της. Ο όρος

περιλαμβάνει όλα τα μέτρα που πρέπει να πάρει η επιχείρηση ώστε να προσελκύσει και να εξυπηρετήσει όλους τους πελάτες της.

Cybercash - Όρος που αναφέρεται στο εικονικό χρήμα ή στο μέσο πληρωμής που μπορεί να φορτωθεί μέσω ενός ανοικτού δικτύου, όπως είναι το Internet.

Data Mining - Αποδίδεται στα ελληνικά με τον όρο *Εξόρυξη Δεδομένων* και αναφέρεται στην επεξεργασία και την αξιολόγηση των δεδομένων με βάση τη συμπεριφορά των χρηστών (επισκεπτών) του δικτυακού τόπου μιας εταιρείας. Η εταιρεία μπορεί να εκμεταλλευτεί (αξιοποιήσει) αυτά τα δεδομένα για να βελτιώσει την εικόνα της στην αγορά και να αυξήσει έτσι σημαντικά τις πωλήσεις της.

Deep linking - Αναφέρεται σ' έναν σύνδεσμο (link) ο οποίος μας κατευθύνει σε μια εσωτερική ιστοσελίδα ενός δικτυακού τόπου και όχι στην αρχική του σελίδα (home page). Μερικές εταιρείες είναι αντίθετες μ' αυτήν την πρακτική καθώς, όπως ισχυρίζονται, οι χρήστες (επισκέπτες του δικτυακού τόπου) δεν είναι σε θέση να δουν τα διαφημιστικά banners που υπάρχουν στην αρχική σελίδα του Web site.

Demand Aggregators - Αναφέρεται σε ειδικούς οργανισμούς (εταιρείες) οι οποίες απασχολούνται με το να καταμετρούν και να συγκεντρώνουν την καταναλωτική ζήτηση που υπάρχει για ένα συγκεκριμένο προϊόν. Με τον τρόπο αυτό μπορούν και οι καταναλωτές να επιτυγχάνουν μεγαλύτερες εκπτώσεις (καλύτερες τιμές) στις αγορές που κάνουν μέσω του Internet, αλλά και οι ίδιες οι εταιρείες έχουν τη δυνατότητα να πωλούν προϊόντα που διαφορετικά θα έπρεπε να είχαν μείνει στο στοκ.

Digital ID/Certificate - Αποδίδεται στα ελληνικά με τον όρο *Ψηφιακή Ταυτότητα* ή *Ψηφιακή Βεβαίωση* ή και *Ψηφιακό Πιστοποιητικό* και πρόκειται για μια κρυπτογραφημένη ταυτότητα που την εκδίδουν ειδικά εξουσιοδοτημένοι Οργανισμοί Παροχής Υπηρεσιών Πιστοποίησης, με την οποία επιβεβαιώνεται η γνησιότητα των στοιχείων του κατόχου, το ότι αυτός που στέλνει το μήνυμα είναι όντως αυτός που ισχυρίζεται ότι είναι και ότι δεν γίνεται ηλεκτρονική απάτη ή πλαστοπροσωπία. Μπορεί να την χρησιμοποιήσει ο κάτοχός της για να κάνει ασφαλείς ηλεκτρονικές συναλλαγές και επικοινωνία μέσω του Internet. Η ψηφιακή ταυτότητα περιλαμβάνει την ψηφιακή υπογραφή του κατόχου της (digital signature) και το δημόσιο κλειδί του (public key).

Digital Money - Αποδίδεται στα ελληνικά με τον όρο *Ψηφιακό Χρήμα* και αναφέρεται στο εικονικό (άυλο) χρήμα που διακινείται μέσω του Internet, είτε με πιστωτικές κάρτες είτε με ειδικούς ψηφιακούς λογαριασμούς. Οι καταθέσεις και οι αναλήψεις γίνονται κανονικά στις τράπεζες των συναλλασσομένων και φαίνονται κατά την ενημέρωση των βιβλιαρίων τους.

Digital Signature - Αποδίδεται στα ελληνικά με τον όρο *Ψηφιακή Υπογραφή* και πρόκειται για ειδικό αρχείο το οποίο δημιουργείται από κείμενο που το υπογράφει και το κρυπτογραφεί (κωδικοποιεί) ο κάτοχός του. Ο παραλήπτης του μηνύματος θα πρέπει να κάνει αποκρυπτογράφηση του κειμένου, σύγκριση της ψηφιακής υπογραφής και πιστοποίηση (επιβεβαίωση) της ταυτότητας του αποστολέα του μηνύματος.

Digital Wallet- Αποδίδεται στα ελληνικά με τον όρο *Ψηφιακό Πορτοφόλι* και αναφέρεται σ' έναν εικονικό πορτοφόλι που μπορεί να δημιουργήσει ένας χρήστης και να αποθηκεύσει στον υπολογιστή του ενώ πραγματοποιεί τις αγορές του στο Internet. Με τη βοήθεια του ψηφιακού πορτοφολιού μπορεί να δημιουργηθεί το προφίλ του online καταναλωτή που να περιέχει τα στοιχεία της πιστωτικής του κάρτας, τη διεύθυνση κατοικίας κ.ά., αλλά και ένα αρχείο με τα στοιχεία της κάθε συναλλαγής που κάνει στο Διαδίκτυο. Με το ψηφιακό πορτοφόλι, οι καταναλωτές μπορούν να αποφεύγουν την συνεχή συμπλήρωση των στοιχείων τους κάθε φορά που επισκέπτονται και συναλλάσσονται μ' ένα ηλεκτρονικό κατάστημα. Επίσης, σ' ένα ψηφιακό πορτοφόλι μπορούν να αποθηκευθούν οι προτιμήσεις του καταναλωτή, τυχόν ενημερώσεις (ειδοποιήσεις) για καινούργια προϊόντα που τον ενδιαφέρουν κ.ά.

Direct Marketing - Έτσι αποκαλείται η διαδικασία κατά την οποία μια εταιρεία στέλνει διαφημιστικά μηνύματα απευθείας στους πιθανούς της πελάτες. Το direct marketing μέσω ηλεκτρονικού ταχυδρομείου κερδίζει συνεχώς έδαφος τελευταία, ενώ είναι πολύ ενοχλητικό για τον περισσότερο κόσμο το λεγόμενο *spamming* ή στα ελληνικά η *μη ζητηθείσα εμπορική επικοινωνία*, με πιο απλά λόγια ο βομβαρδισμός των e-mails των χρηστών του Internet με συνεχή διαφημιστικά μηνύματα.

Domain Name Service (DNS) - Αποδίδεται στα ελληνικά με τον όρο *Υπηρεσία Ονομάτων Περιοχής* ή και *Υπηρεσία Ονομάτων Χώρου* (σύμφωνα με τον Ν. 2867/2000) και πρόκειται για μια διαδικασία όπου αντιστοιχίζεται το όνομα περιοχής (domain name) μιας διεύθυνσης URL με την πραγματική IP διεύθυνση του υπολογιστή που περιέχει την ιστοσελίδα που επιθυμούμε να προσπελάσουμε. Η Υπηρεσία DNS πραγματοποιείται με ειδικές βάσεις

δεδομένων που βρίσκονται εγκατεστημένες στους λεγόμενους DNS Servers, οι οποίοι βρίσκονται διάσπαρτοι σ' όλον τον κόσμο σε κομβικά σημεία (ISPs, Πανεπιστήμια, Ερευνητικά Κέντρα και αλλού) και ενημερώνονται συνεχώς με τις αλλαγές (προσθήκες, διαγραφές, μεταβολές) των ονομάτων περιοχής (domain names).

Dotcom - Με τον όρο αυτό χαρακτηρίζονται οι εταιρείες που κάνουν τις συναλλαγές τους αποκλειστικά μέσω του Internet. Χαρακτηριστικό παράδειγμα αποτελεί η Amazon, ένα από τα πρώτα και πιο πετυχημένα διεθνή διαδικτυακά βιβλιοπωλεία, με παραρτήματα σε πολλές χώρες. Πολλές επιχειρήσεις dotcom ενώ ξεκίνησαν με ενθουσιασμό και προοπτικές, δεν βρήκαν την ανάλογη ανταπόκριση από το καταναλωτικό κοινό και οδηγήθηκαν σε πτώχευση.

E-Auction - Δημοπρασία που γίνεται online στο Διαδίκτυο.

E-Banking - Με τον όρο αυτό είναι γνωστές οι τραπεζικές συναλλαγές, όπως για παράδειγμα οι καταθέσεις και οι αναλήψεις, που γίνονται μέσω του Internet.

E-Business - Αποδίδεται στα ελληνικά με τον όρο *Ηλεκτρονικό Επιχειρείν* και αναφέρεται στην πραγματοποίηση των επιχειρηματικών συναλλαγών μέσω του Internet, δηλ. στην ανάπτυξη του νέου επιχειρηματικού μοντέλου με αντικείμενο μόνο το Internet.

E-Cash - Γενικός όρος που αναφέρεται στις ηλεκτρονικές χρηματικές συναλλαγές που πραγματοποιούνται μέσω του Internet.

E-Commerce - Αποδίδεται στα ελληνικά με τον όρο *Ηλεκτρονικό Εμπόριο* και αναφέρεται στην πραγματοποίηση όλων των ειδών των συναλλαγών με ηλεκτρονικά μέσα και κυρίως μέσω του Internet. Το ηλεκτρονικό εμπόριο διακρίνεται σε B2B (Business To Business), δηλ. ανάμεσα σε επιχειρήσεις, B2C (Business To Consumer), δηλ. ανάμεσα σε επιχειρήσεις και καταναλωτές κ.ά.

EDI (Electronic Data Interchange) - Αποδίδεται στα ελληνικά με τον όρο *Ηλεκτρονική Ανταλλαγή Δεδομένων* και αναφέρεται στη νόμιμη έκδοση τιμολογίων και άλλων εμπορικών παραστατικών μέσω του Internet.

EDIFACT (Electronic Data Interchange For Administration, Commerce and Transport) - Σύστημα Ανταλλαγής Ηλεκτρονικών Δεδομένων Διοίκησης, Εμπορίου και Μεταφορών.

EFT (Electronic Funds Transfer) - Όρος που αναφέρεται στην ηλεκτρονική μεταφορά κεφαλαίου (χρημάτων) από λογαριασμό σε λογαριασμό.

Electronic Catalog (E-Catalog) - Ειδικός μηχανισμός που δημιουργείται με δυναμικές ιστοσελίδες και που παρουσιάζει ομαδοποιημένα και συγκεντρωμένα τα προϊόντα ή/και τις υπηρεσίες μιας εταιρείας και όπου έχουν τη δυνατότητα οι χρήστες να κάνουν παραγγελίες προϊόντων ή υπηρεσιών από το ηλεκτρονικό κατάστημα.

E-Mail (Electronic Mail) - Αποδίδεται στα ελληνικά με τον όρο *Ηλεκτρονικό Ταχυδρομείο* ή και *Ηλεκτρονική Αλληλογραφία* και είναι η υπηρεσία (πρόγραμμα πελάτης) για την αποστολή και λήψη των μηνυμάτων ηλεκτρονικής αλληλογραφίας, τα οποία μπορούν να περιέχουν και συνημμένα αρχεία κειμένου ή εικόνας ή video ή ήχου και η οποία διεξάγεται μέσω του Internet. Δημοφιλή προγράμματα για e-mail είναι τα Outlook και Outlook Express της εταιρείας Microsoft, το Netscape Communicator, το Eudora και τώρα τελευταία και το ThunderBird της Mozilla. Μπορούμε να δημιουργήσουμε έναν λογαριασμό ηλεκτρονικής αλληλογραφίας (e-mail account) είτε στον Παροχέα Υπηρεσιών Internet (ISP) που μας εξυπηρετεί είτε σ' ειδικά portals, όπως είναι το hotmail, το yahoo, το in.gr κ.ά. Στη δεύτερη περίπτωση έχουμε το λεγόμενο *Webmail*.

ERP (Enterprise Resource Planning) - Αποδίδεται στα ελληνικά με τον όρο *Σύστημα Ενδοεπιχειρησιακού Σχεδιασμού* και πρόκειται για ειδικό πρόγραμμα με το οποίο μπορούμε να διαχειρισθούμε τις ενδο-επιχειρησιακές διεργασίες μιας εταιρείας, δηλαδή τη διακίνηση των εμπορευμάτων, τα αποθέματα, την τήρηση των βιβλίων, την οργάνωση της παραγωγής και του προσωπικού κ.ά.

E-Shop - Αποδίδεται στα ελληνικά με τον όρο *Ηλεκτρονικό Κατάστημα* και αναφέρεται σ' ένα κανονικό κατάστημα πώλησης προϊόντων που λειτουργεί

μέσω του Διαδικτύου με ολοκληρωμένη διαδικασία παραγγελίας, πώλησης, τιμολόγησης, αποστολής εμπορευμάτων κλπ.

E-Tailing - Η λιανική πώληση (Retailing) προϊόντων μέσα από ένα ηλεκτρονικό κατάστημα (e-Shop).

E-Trade - Όρος που αναφέρεται στην πραγματοποίηση των χρηματοοικονομικών συναλλαγών μέσω του Internet.

E-Wallet - Αποδίδεται στα ελληνικά με τον όρο *Ηλεκτρονικό Πορτοφόλι* και αναφέρεται σ' ένα εξειδικευμένο πρόγραμμα που έχει τη δυνατότητα να διαχειρίζεται ηλεκτρονικά τους τραπεζικούς λογαριασμούς ή την πιστωτική κάρτα ενός χρήστη.

Extranet - Αναφέρεται στην επέκταση του εσωτερικού δικτύου (Intranet ή Ενδοδίκτυο) μιας εταιρείας, ώστε να έχουν πρόσβαση σ' αυτό ειδικά εξουσιοδοτημένα άτομα που μπορεί είναι πελάτες ή προμηθευτές της εταιρείας.

E-zine - Περιοδικό που εκδίδεται σε ηλεκτρονική μορφή και απευθύνεται συνήθως σε συγκεκριμένο (εξειδικευμένο) αναγνωστικό κοινό.

First-Party Loss - Αποδίδεται στα ελληνικά με τον όρο *Άμεσες Απώλειες* και είναι οι απώλειες μιας εταιρείας που έχουν να κάνουν με το η-επιχειρείν, δηλαδή με την εμπορική δραστηριότητα της εταιρείας στο Διαδίκτυο και τέτοιες μπορεί να είναι για παράδειγμα η καταστροφή ή και η αλλοίωση του πληροφοριακού κεφαλαίου της εταιρείας εξαιτίας ενός ιού (virus)

ή ενός σκουληκιού (worm) ή η παρακολούθηση της δραστηριότητας και των απόρρητων στοιχείων της εταιρείας μέσω ενός δούρειου ίππου (trojan horse) ή ακόμα και μια επίθεση κάποιου hacker ή κάποιου cracker κ.ά.

Firewall - Αποδίδεται στα ελληνικά με τον όρο *Πύρινο Τείχος* ή και *Τείχος Προστασίας* και είναι ένα ειδικό σύστημα hardware (μηχάνημα, εξοπλισμός) ή και ειδικό πρόγραμμα (software) που προστατεύει το δίκτυο μιας επιχείρησης ή ενός οργανισμού ή ακόμη και τον προσωπικό υπολογιστή ενός χρήστη, απαγορεύοντας την πρόσβαση των χρηστών του σε συγκεκριμένα sites του Internet ή και το αντίθετο, απαγορεύοντας την πρόσβαση στο δίκτυο της εταιρείας από εξωτερικούς χρήστες ή και ιστοσελίδες. Μπορεί να ρυθμισθεί ώστε να απαγορεύει την πρόσβαση σε συγκεκριμένους χρήστες και για συγκεκριμένες ημέρες ή ώρες της ημέρας.

FTP (File Transfer Protocol) - Αποδίδεται στα ελληνικά με τον όρο *Πρωτόκολλο Μεταφοράς Αρχείων* και είναι μια από τις χρήσιμες υπηρεσίες του Internet, όπου με τη βοήθειά της μπορούμε να κατεβάσουμε (download) προγράμματα ή αρχεία από διάφορα sites του Internet ή και να δημοσιεύσουμε (publish) ή να ανεβάσουμε (upload) δικά μας αρχεία ή/και ιστοσελίδες για δημοσίευση στο Internet. Οι υπολογιστές που προσφέρουν αρχεία για κατέβασμα αποκαλούνται FTP Servers και αν υπάρχει η δυνατότητα να κατεβάσει αρχεία ένας οποιοσδήποτε χρήστης, τότε μιλάμε για *ανώνυμο (anonymous) ftp*, όπου θα πρέπει να δώσουμε ως username το anonymous και ως password το e-mail μας για να μπορέσουμε να συνδεθούμε. Εξυπακούεται ότι τα αρχεία που διατίθενται ελεύθερα για download είναι περιορισμένα. Αν έχουμε εξουσιοδότηση σε κάποιον FTP Server, τότε θα μας έχει παραχωρήσει δικά μας username και password και θα μπορούμε έτσι με τη βοήθεια ειδικών προγραμμάτων να κατεβάσουμε ή και να ανεβάσουμε αρχεία από ή προς τον FTP Server. Η διαδικασία του FTP μπορεί να γίνει και με τη χρήση του προγράμματος Εξερεύνησης των Windows και ενός browser, όπου στον browser θα πρέπει να γράψουμε την ftp διεύθυνση με την οποία θέλουμε να συνδεθούμε, όπως για παράδειγμα ftp://www.myftp.gr, να δώσουμε το username και password για να μπορέσουμε να συνδεθούμε και μετά να κάνουμε μεταφορά ή copy/paste των αρχείων που θέλουμε από το ένα παράθυρο στο άλλο. Μέσα στο παράθυρο του FTP Server μπορούμε να δημιουργήσουμε φακέλους (καταλόγους), να μετονομάσουμε και να αντιγράψουμε αρχεία και γενικά να εργαστούμε σαν να πρόκειται για ένα παράθυρο του δικού μας υπολογιστή.

Gateway - Αποδίδεται στα ελληνικά με τον όρο *Πύλη* και πρόκειται για ειδική συσκευή που αναλαμβάνει να διασυνδέσει δύο ή και περισσότερα δίκτυα που χρησιμοποιούν εντελώς διαφορετικά πρωτόκολλα.

GUI (Graphical User Interface) - Αποδίδεται στα ελληνικά με τον όρο *Γραφικό Περιβάλλον Χρήστη* και αναφέρεται στην ευκολία διαχείρισης που παρέχει το γραφικό περιβάλλον σ' όλους τους χρήστες των υπολογιστών και ιδιαίτερα στους αρχάριους. Στο γραφικό περιβάλλον επικοινωνίας με τον υπολογιστή χρησιμοποιείται πολύ το ποντίκι σ' αντίθεση με το πληκτρολόγιο που χρησιμοποιείτο στα παλαιότερα λειτουργικά συστήματα.

House Ads - Ειδικός τύπος διαφημιστικού banner που προβάλλει ένας δικτυακός τόπος στον δικό του δικτυακό τόπο, όταν δεν υπάρχει πληρωμένη καταχώρηση τρίτων. Συνήθως αφορά στην προώθηση προϊόντων ή υπηρεσιών του ίδιου του δικτυακού τόπου.

Home Page - Αποδίδεται στα ελληνικά με τον όρο *Αρχική Σελίδα* ή *Κεντρική Σελίδα* ή και *Οικοσελίδα* και είναι η ιστοσελίδα που εμφανίζεται πρώτη όταν

εισερχόμαστε σ' έναν δικτυακό τόπο. Αποτελεί την πύλη εισόδου μας σ' έναν δικτυακό τόπο και θα πρέπει να περιέχει κάτι σαν έναν πίνακα περιεχομένων για να είναι έτσι πιο φιλική η περιήγησή μας στο Web site.

HTML (HyperText Maskup Language) - Αποδίδεται στα ελληνικά ως *Γλώσσα Σήμανσης Υπερκειμένου* και πρόκειται για γλώσσα σήμανσης ή μορφοποίησης περισσότερο και όχι για γλώσσα προγραμματισμού, η οποία χρησιμοποιεί τα λεγόμενα tags (ετικέτες), όπως είναι τα <b>, <i>, <a href>, <table> και πολλά άλλα, ώστε να μπορέσει να καταλάβει ο φυλλομετρητής (browser) που θα διαβάσει τον HTML κώδικα, πώς θα πρέπει να εμφανίσει το κείμενο στην οθόνη του υπολογιστή. Ένα αρχείο που περιέχει HTML κώδικα είναι γνωστό σαν ιστοσελίδα (Web page) και αποθηκεύεται με την επέκταση (extension) .htm ή .html.

HTTP (HyperText Transfer Protocol) - Αποδίδεται στα ελληνικά ως *Πρωτόκολλο Μεταφοράς Υπερκειμένου* και είναι ένα ειδικό πρωτόκολλο επικοινωνίας που χρησιμοποιείται για τη μεταφορά κειμένου και εικόνων μέσω του Internet. Τα γνωστά σύμβολα http:// που χρησιμοποιούμε πριν από μια URL διεύθυνση σημαίνουν απλά ότι θα πρέπει να χρησιμοποιηθεί το πρωτόκολλο HTTP. Άλλα γνωστά πρωτόκολλα είναι το https://, δηλ. το ασφαλές (secure) http, το ftp://, το news:, το POP3, το SMTP κ.ά.

IMAP (Internet Message Access Protocol) - Πρωτόκολλο που χρησιμοποιείται στην υπηρεσία ηλεκτρονικού ταχυδρομείου (e-mail).

Interactive Relationship Managers (IRM) - Εταιρείες που η δουλειά τους είναι να συγκεντρώνουν πληροφορίες (στοιχεία) για τους πελάτες των Παροχέων Υπηρεσιών Internet (ISPs) σχετικά με τους συνηθέστερους τόπους στους οποίους κάνουν πλοήγηση καθώς και τις προτιμήσεις τους. Τα στοιχεία αυτά μπορούν να αξιοποιηθούν για το marketing και την προώθηση των προϊόντων άλλων εταιρειών που είναι πλέον πελάτες σε μια εταιρεία IRM.

Interstitial - Ειδική μορφή διαφήμισης που παρεμβάλλεται ανάμεσα στην διεπαφή ενός χρήστη με μια ιστοσελίδα. Όταν ο χρήστης καλέσει μια συγκεκριμένη ιστοσελίδα ενός δικτυακού τόπου, βλέπει αρχικά μια διαφήμιση που καταλαμβάνει ολόκληρη την οθόνη και η οποία έχει συγκεκριμένη διάρκεια και μετά εμφανίζεται η κανονική ιστοσελίδα που είχε αρχικά ζητηθεί. Τα interstitials είναι παρόμοια με τα superstitials, με τη διαφορά ότι η

διαδικασία φόρτωσής τους γίνεται αντιληπτή στον χρήστη και μπορεί να είναι ενοχλητική βέβαια για μερικούς.

Intranet - Αποδίδεται στα ελληνικά με τον όρο *Ενδοδίκτυο* και πρόκειται για ένα εσωτερικό δίκτυο μιας επιχείρησης ή ενός οργανισμού, το οποίο χρησιμοποιεί αυστηρούς περιοριστικούς κανόνες ως προς την επικοινωνία των χρηστών του με το Internet και για να μπορέσει να μπει ένας εξωτερικός χρήστης (συνεργάτης) στο ενδοδίκτυο μιας εταιρείας θα πρέπει να διαθέτει ειδικό λογαριασμό (user name και password).

IP (Internet Protocol) - Αποδίδεται στα ελληνικά με τον όρο *Πρωτόκολλο του Internet* και είναι το ένα από τα δύο βασικότερα πρωτόκολλα του Internet, όπου το άλλο είναι το TCP. Το πρωτόκολλο IP αναλαμβάνει τη δρομολόγηση των πακέτων που παραλαμβάνει από το πρωτόκολλο TCP, ώστε αυτά να φθάσουν με ασφάλεια στον προορισμό τους.

Island Position - Όρος που αναφέρεται σε μια διαφημιστική καταχώρηση στο Διαδίκτυο η οποία είναι περικυκλωμένη από κείμενο, χωρίς να υπάρχουν άλλες διαφημιστικές καταχωρήσεις στην ίδια ιστοσελίδα, οι οποίες συνήθως αποσπούν την προσοχή του κοινού. Από τον τρόπο της τοποθέτησής της πήρε και το όνομα island.

Issuing Bank - Αποδίδεται στα ελληνικά με τον όρο *Τράπεζα Έκδοσης* και είναι η τράπεζα στην οποία έχουμε λογαριασμό και μας εκδίδει την πιστωτική ή "έξυπνη" κάρτα (smart card).

Java - Πολύ δημοφιλής αντικειμενοστραφής γλώσσα προγραμματισμού, που δημιουργήθηκε από την εταιρεία Sun Microsystems, και που μπορεί να δημιουργήσει αυτόνομες εφαρμογές ή μικροεφαρμογές, που αποκαλούνται *applets*, για ενσωμάτωση μέσα σε ιστοσελίδες. Τα πηγαία αρχεία της Java έχουν την επέκταση .java, ενώ αυτά που δημιουργούνται με τη μεταγλώττιση (compilation) έχουν επέκταση .class και αποτελούν έναν ενδιάμεσο κώδικα (bytecode) που μπορούν να αναγνωρίσουν οι φυλλομετρητές και να εκτελέσουν μέσα από μια ιστοσελίδα. Υπάρχουν πάρα πολλές έτοιμες εφαρμογές σε Java στο Διαδίκτυο, όπου στις περισσότερες είναι κρυμμένος ο πηγαίος κώδικας. Οι εφαρμογές της Java δίνουν ζωντάνια στις ιστοσελίδες μας καθώς μπορούμε να δημιουργήσουμε πολύ ωραία εφέ αλλά και να υπάρχει μια αλληλεπίδραση (interaction) με τον χρήστη. Παραδείγματα από εφαρμογές σε Java υπάρχουν στην εξής διεύθυνση : http://dide.flo.sch.gr/Plinet/Java/Java.html

JavaScript - Πολύ δημοφιλής γλώσσα προγραμματισμού, που δημιουργήθηκε από την εταιρεία Netscape και είναι ανταγωνιστική της γλώσσας

προγραμματισμού VBScript, της εταιρείας Microsoft. Οι γλώσσες αυτές αποκαλούνται *γλώσσες συγγραφής σεναρίων (scripting languages)*, δηλ. μπορούμε να γράψουμε μικρά προγράμματα ή σενάρια (scripts) και να τα ενσωματώσουμε μέσα στον HTML κώδικα μιας ιστοσελίδας. Η JavaScript δεν είναι τόσο αντικειμενοστραφής όσο η Java, αλλά είναι πιο απλή στη σύνταξή της και έχει το πολύ καλό πλεονέκτημα ότι μπορούμε να δούμε τον πηγαίο κώδικά της. Με τις γλώσσες αυτές επιτυγχάνουμε το λεγόμενο *client-side scripting*, δηλ. το γράψιμο προγραμμάτων στην πλευρά του χρήστη-πελάτη (client) και όχι του server. Παραδείγματα από εφαρμογές σε JavaScript υπάρχουν στις εξής διευθύνσεις : http://dide.flo.sch.gr/Plinet/JavaScript/JavaScript.html και http://dide.flo.sch.gr/Plinet/Applications/JavaScript.html

Landing Page - Είναι η ιστοσελίδα στην οποία πηγαίνουμε αφού έχουμε κάνει κλικ σε κάποιο διαφημιστικό banner. Ο απώτερος σκοπός μιας τέτοιας ιστοσελίδας είναι η περαιτέρω προώθηση της υπηρεσίας ή του προϊόντος που αναφέρεται στην αρχική καταχώρηση ενός δικτυακού τόπου.

LAN (Local Area Network) - Αποδίδεται στα ελληνικά με τον όρο *Τοπικό Δίκτυο Υπολογιστών* και είναι ένα δίκτυο υπολογιστών που καλύπτει μια μικρή γεωγραφική έκταση, όπως είναι το κτίριο μιας υπηρεσίας ή ενός σχολείου κλπ. Τα τοπικά δίκτυα υπολογιστών έχουν γίνει πολύ δημοφιλή τελευταία καθώς είναι πολύ εύκολη και φθηνή η διασύνδεση των υπολογιστών τους, ενώ οι υπολογιστές του τοπικού δικτύου μπορούν να λειτουργήσουν και αυτόνομα.

Για τη σύνδεση των υπολογιστών ενός τοπικού δικτύου απαιτείται η χρήση ενός κατανεμητή ή πλήμνης (hub ή switch) και με τη βοήθεια ενός δρομολογητή (router) είναι δυνατή η πρόσβαση στο Internet χωρίς να παρεμβάλλεται κατ' ανάγκην ο υπολογιστής server του τοπικού δικτύου. Στα πλεονεκτήματα ενός τοπικού δικτύου συγκατελέγεται και η δυνατότητα για ταχύτατη μεταφορά αρχείων από υπολογιστή σε υπολογιστή καθώς και η κοινή χρήση εκτυπωτών, scanners και άλλων περιφερειακών συσκευών.

MIME (Multi-Purpose Internet Mail Extensions) - Πρόκειται για μια επέκταση του πρωτοκόλλου που χρησιμοποιείται στο ηλεκτρονικό ταχυδρομείο (e-mail) και η οποία επέκταση δίνει τη δυνατότητα για ανταλλαγή αρχείων πολυμέσων (εικόνας και ήχου) και όχι μόνο κειμένου.

Mobile Commerce (m-commerce) - Όρος που αναφέρεται στο κινητό ηλεκτρονικό εμπόριο και γενικότερα σε εφαρμογές η-επιχειρείν μέσω κινητής τηλεφωνίας, όπως είναι για παράδειγμα η χρηματιστηριακή ενημέρωση, οι πληροφορίες πλοήγησης, οι υπηρεσίες πρόβλεψης καιρού και οι αεροπορικές

κρατήσεις που πραγματοποιούνται μέσω υπολογιστή παλάμης (PDA) ή κινητού τηλεφώνου.

New Economy - Αποδίδεται στα ελληνικά με τον όρο *Νέα Οικονομία* είναι ένας σύγχρονος όρος που αναφέρεται στην καινούργια νοοτροπία που δημιουργεί η οικονομία του Internet. Με την ευρύτερη έννοια περιλαμβάνει τομείς υλικού (hardware) και λογισμικού (software), μέσα ενημέρωσης και τηλεπικοινωνίες. Τα όρια μεταξύ των μεμονωμένων αυτών τομέων δεν είναι πλέον σαφή όπως και ο διαχωρισμός της νέας από την παλιά (συμβατική) οικονομία. Αυτό οφείλεται ιδιαίτερα στο γεγονός ότι οι παραδοσιακές επιχειρήσεις βασίζουν πλέον όλο και περισσότερο μεγάλο μέρος της δραστηριότητάς τους στο Internet.

Opt In/Opt Out - Όρος που αναφέρεται στην αποδοχή εκ μέρους ενός χρήστη της λήψης ενημερωτικών/διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου από έναν δικτυακό τόπο (opt in) και αντίστοιχα η επιλογή που δίνει ο δικτυακός τόπος στον χρήστη να ζητήσει όποτε θελήσει τη διαγραφή της ηλεκτρονικής του διεύθυνσης από τη λίστα αποδεκτών του προωθητικού υλικού (opt out). Με τον τρόπο αυτό μια επιχείρηση μπορεί να προωθήσει τις υπηρεσίες ή/και τα προϊόντα της αποτελεσματικά, χωρίς να αναγκάζεται να καταφεύγει σε ενέργειες spamming, που είναι πολύ ενοχλητικές για τους περισσότερους χρήστες αλλά και δημιουργούν άσχημη εικόνα για την εταιρεία.

Packet - Αποδίδεται στα ελληνικά με τον όρο *Πακέτο* και αναφέρεται στα κομμάτια δεδομένων στα οποία διασπάται ένα μήνυμα ώστε να μπορέσει να φθάσει πιο αποτελεσματικά στον προορισμό του. Το κάθε πακέτο έχει μια δική του αρίθμηση έτσι ώστε να γίνεται σωστά η επανασύνδεση των πακέτων όταν αυτά φθάσουν στον τελικό παραλήπτη. Το κάθε πακέτο μπορεί να ακολουθήσει διαφορετική διαδρομή μέχρι τον τελικό προορισμό του και αν κάποιο πακέτο χαθεί ή δεν φθάσει έγκαιρα στον προορισμό του θα πρέπει να ζητηθεί από τον παραλήπτη η αποστολή του εκ νέου. Στη φιλοσοφία αυτή στηρίχθηκε το σύστημα άμυνας των ΗΠΑ απέναντι σε ενδεχόμενη σοβιετική πυρηνική επίθεση στις δεκαετίες του '50 και του '60 και αποτέλεσε και τη βάση για τη λειτουργία του Internet.

PGP (Pretty Good Privacy) - Αποτελεί ένα από τα πιο δημοφιλή προγράμματα που χρησιμοποιούνται για την κρυπτογράφηση μηνυμάτων και την αποστολή τους μέσω του Internet. Χρησιμοποιεί την κρυπτογράφηση με συνδυασμό δημόσιου και ιδιωτικού κλειδιού (public key - private key). Θεωρείται απόλυτα ασφαλές. Το δημόσιο κλειδί είναι γνωστό σ' όλους και μπορούμε να το κατεβάσουμε (download) από κάποια ιστοσελίδα ή να μας

στείλει ο κάτοχός του, ενώ το ιδιωτικό κλειδί είναι αυστηρά προσωπικό για τον κάθε χρήστη. Ό,τι κωδικοποιείται με το ένα κλειδί μπορεί να αποκωδικοποιηθεί με το άλλο και αντίστροφα. Όμως, είναι εξαιρετικά δύσκολη, αν όχι αδύνατη, η εύρεση του ιδιωτικού κλειδιού όταν γνωρίζουμε το δημόσιο κλειδί ενός χρήστη. Όταν ένα μήνυμα κωδικοποιείται με το ιδιωτικό κλειδί ενός χρήστη, μπορεί να αποκωδικοποιηθεί από οποιονδήποτε τρίτο με το γνωστό δημόσιο κλειδί του ίδιου χρήστη, αλλά αυτό αποτελεί μια επιβεβαίωση της ταυτότητας του χρήστη. Επίσης, η κωδικοποίηση ενός μηνύματος με το δημόσιο κλειδί ενός χρήστη εξασφαλίζει το ότι μόνο ο συγκεκριμένος χρήστης θα μπορέσει να το αποκωδικοποιήσει και συνεπώς να το διαβάσει.

Pop-Up Window (Ad) - Μια από τις πιο δημοφιλείς μορφές διαφήμισης, σύμφωνα με την οποία εμφανίζεται ένα μικρό παράθυρο μπροστά ή και πίσω από τον φυλλομετρητή του χρήστη τη στιγμή που αυτός εισέρχεται στην κεντρική ιστοσελίδα ενός δικτυακού τόπου. Μέσα σ' ένα Pop Window, που είναι γνωστό και ως Ad, μπορεί να εμφανίζεται μια απλή εικόνα ή και μια ολόκληρη ιστοσελίδα με διάφορες πληροφορίες. Τα Pop Windows μπορούν να εμφανίζονται μπροστά, οπότε αποκαλούνται *Pop-Up*, ή και πίσω από τον φυλλομετρητή (Web Browser) του χρήστη, οπότε αποκαλούνται *Pop-Under*.

POP3 (Post Office Protocol 3) - Ένα από τα πιο δημοφιλή πρωτόκολλα που χρησιμοποιείται για τη λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail).

Portal - Αποδίδεται στα ελληνικά με τον όρο *Πύλη* και αναφέρεται σε ειδικούς δικτυακούς τόπους (Web sites), όπου ο χρήστης μπορεί να κάνει εγγραφή και να αποκτήσει προσωπικό username και password, να έχει δική του θυρίδα μηνυμάτων, να βλέπει τρέχουσες ειδήσεις που τον ενδιαφέρουν, ειδήσεις για τον καιρό, να συμμετέχει σε fora συζητήσεων, σε δημοσκοπήσεις, σε guest books, να χρησιμοποιεί μηχανές αναζήτησης κ.ά. Η δημιουργία δικτυακής πύλης και όχι δικτυακού τόπου είναι πολύ δημοφιλής τελευταία στο Internet καθώς υπάρχει πληθώρα προγραμμάτων, όπως τα PHP Nuke, PostNuke, PHP Mambo κ.ά., και είναι πολύ εύκολη η διαχείρισή τους, η οποία μπορεί να γίνει από οποιονδήποτε υπολογιστή έχει σύνδεση στο Internet.

Promo Text - Μορφή διαφήμισης που ξεκίνησε από τα e-mail newsletters και τώρα εφαρμόζεται με επιτυχία και σε ιστοσελίδες. Είναι ένα μικρό κείμενο διαφημιστικού περιεχομένου (τίτλος και περιγραφή) που μπορεί να τοποθετηθεί σ' οποιοδήποτε σημείο μέσα σ' έναν δικτυακό τόπο.

Public Key Encryption - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτογράφηση με Δημόσιο Κλειδί* και πρόκειται για ένα σύστημα

κρυπτογράφησης που χρησιμοποιεί έναν συνδυασμό από ένα δημόσιο και ένα ιδιωτικό κλειδί για την κρυπτογράφηση των μηνυμάτων. Με τον τρόπο αυτό αποφεύγουμε την αποστολή του κλειδιού από τον αποστολέα στον παραλήπτη, κάτι που είναι πολύ επικίνδυνο για υποκλοπή.

ROI (Return of Investment) - Αποδίδεται στα ελληνικά με τον όρο *Απόδοση Επένδυσης* και αναφέρεται κυρίως σε επένδυση που έγινε σε μια διαφημιστική εκστρατεία στο Διαδίκτυο και στο αποτέλεσμα που είχε η διαφημιζόμενη εταιρεία.

Router - Αποδίδεται στα ελληνικά με τον όρο *Δρομολογητής* και είναι ειδική δικτυακή συσκευή που αναλαμβάνει να δρομολογήσει (κατευθύνει) τα πακέτα των μηνυμάτων προς τον προορισμό τους καθώς και να διασυνδέσει τοπικά δίκτυα υπολογιστών (LANs). Ένας router διαθέτει στατική IP διεύθυνση και μπορεί να προγραμματισθεί με τη χρήση φορητού υπολογιστή ή και από μακριά (τηλεχειρισμός). Αν συνδεόμαστε στο Internet μέσω τοπικού δικτύου (LAN) και router, τότε η IP διεύθυνσή μας που φαίνεται προς τα έξω είναι αυτή του router, ενώ τοπικά διαθέτουμε άλλη IP διεύθυνση που την αποδίδει ο router ανάλογα με τη σειρά που συνδέονται οι υπολογιστές του τοπικού δικτύου.

RSA - Μια μέθοδος κρυπτογράφησης δημόσιου κλειδιού που μπορεί να χρησιμοποιηθεί και για την κρυπτογράφηση μηνυμάτων και για τη δημιουργία ψηφιακών υπογραφών, δηλ. για την επιβεβαίωση της ταυτότητας του αποστολέα ενός μηνύματος.

Secret Key Encryption - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτογράφηση με Κρυφό Κλειδί* και πρόκειται για ένα σύστημα κρυπτογράφησης με το οποίο αποστέλλεται στον παραλήπτη το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ενός μηνύματος.

Secure Electronic Transaction (SET) - Πρόκειται για ένα σύστημα ασφαλών τραπεζικών πληρωμών που έχει δημιουργηθεί από γνωστές εταιρείες πιστωτικών καρτών. Χρησιμοποιεί τη λεγόμενη *Έμπιστη Τρίτη Οντότητα (Third Trusted Party)* στις συναλλαγές εμπόρου-πελάτη, δηλ. μια ιδιωτική εταιρεία εμπιστοσύνης που παρεμβάλλεται ως τρίτος στις συνδιαλλαγές και εκδίδει τα ψηφιακά πιστοποιητικά ταυτότητας των συναλλασσομένων.

Secure HyperText Transfer Protocol (HTTPS) - Πρόκειται για μια ασφαλή μορφή του γνωστού πρωτοκόλλου μεταφοράς υπερκειμένου HTTP, ώστε να είναι εξασφαλισμένη η ανταλλαγή πληροφοριών ανάμεσα στον φυλλομετρητή και τον Web server.

Secure Sockets Layer (SSL) - Πρόκειται για ένα σύστημα (πρωτόκολλο) κρυπτογράφησης που έχει δημιουργήσει η γνωστή εταιρεία Netscape, με σκοπό την ασφαλή σύνδεση (επικοινωνία) ενός φυλλομετρητή με τον Web server. Τα δεδομένα που στέλνονται ανάμεσα στους δύο είναι κρυπτογραφημένα αλλά το σύστημα δεν εξασφαλίζει την ταυτότητα ούτε του αποστολέα ούτε του παραλήπτη.

Secure Web Server - Ένας Web server που εργάζεται με πιστοποιητικά (πρωτόκολλα) ασφαλείας. Οι συνδέσεις που γίνονται μ' έναν τέτοιο Web server είναι ασφαλείς και όλα τα μηνύματα (δεδομένα) που ανταλλάσσονται με τους πελάτες (clients) του είναι κρυπτογραφημένα.

Shopping Cart - Αποδίδεται στα ελληνικά με τον όρο *Καλάθι Αγορών* και είναι ένα εικονικό καλάθι αγορών που εμφανίζεται κατά την περιήγησή μας σ' ένα ηλεκτρονικό κατάστημα. Μπορούμε ανά πάσα στιγμή να προσθέσουμε ή και να αφαιρέσουμε είδη από το καλάθι αγορών και να βλέπουμε το συνολικό κόστος τους. Όταν κάνουμε οριστικοποίηση της παραγγελίας μας, εμφανίζεται μια προεπισκόπηση του συνόλου των ειδών που διαλέξαμε και μπορούμε να επιλέξουμε τρόπο πληρωμής και τρόπο αποστολής των εμπορευμάτων μας.

Shopping Mall - Όρος που αναφέρεται στα εικονικά εμπορικά κέντρα του Internet.

Smart Card - Αποδίδεται στα ελληνικά με τον όρο *Έξυπνη Κάρτα* και είναι ένα είδος πιστωτικής κάρτας που περιέχει μια CPU (μικροεπεξεργαστή) και όπου μπορούμε να προσθέσουμε ή να αφαιρέσουμε ψηφιακό (ηλεκτρονικό), δηλ. εικονικό, χρήμα.

SMTP (Simple Mail Transfer Protocol) - Είναι το πιο διαδεδομένο πρωτόκολλο για την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail).

Splash Page - Είναι γνωστή και ως jump page και αποτελεί μια ειδική σελίδα υποδοχής σ' έναν δικτυακό τόπο, αλλά κάτι διαφορετικό από τη γνωστή μας αρχική σελίδα (home page). Χρησιμοποιείται για καθαρά διαφημιστικούς λόγους με στόχο να στέλνονται οι χρήστες που έκαναν κλικ σε συγκεκριμένα διαφημιστικά banners σε μια άλλη ιστοσελίδα και να λαμβάνουν περισσότερες πληροφορίες για κάποιο προϊόν που τους ενδιαφέρει.

Start-Up - Μικρή εταιρία που ξεκινά την δραστηριότητά της στον χώρο του Internet.

StoreFront - Η διεπαφή (interface) ενός ηλεκτρονικού καταστήματος στο Internet, όπου ο πελάτης μπορεί να ενημερωθεί για τους καταλόγους των προσφερόμενων προς πώληση προϊόντων, μπορεί να συμπληρώσει τις φόρμες παραγγελίας, να δει όλες τις απαραίτητες πληροφορίες για το ηλεκτρονικό κατάστημα, να ενημερωθεί για τους όρους της συναλλαγής, τους τρόπους πληρωμής και αποστολής των εμπορευμάτων καθώς για τα συστήματα διασφάλισης της όλης διαδικασίας.

Superstitial - Ένα είδος online διαφήμισης που φορτώνεται χωρίς αυτό να γίνεται αντιληπτό από τον χρήστη και προβάλλεται αφού έχει φορτωθεί όλο το σύνολο του περιεχομένου του, σ' ένα νέο παράθυρο του φυλλομετρητή. Τα superstitials προτιμώνται από τους διαφημιστές, καθώς επιτρέπουν μεγαλύτερες σε μέγεθος και περισσότερο διαδραστικές διαφημίσεις απ' ό,τι το κοινό (απλό) banner και γιατί είναι λιγότερο ενοχλητικά στους χρήστες απ' ό,τι τα pop-up windows και τα interstitials.

Targeting - Αποδίδεται στα ελληνικά με τον όρο *Στόχευση* και χρησιμοποιείται σε online διαφημιστικές εκστρατείες οι οποίες διενεργούνται υπό συγκεκριμένα κριτήρια και απευθύνονται σε συγκεκριμένο καταναλωτικό κοινό. Για παράδειγμα, μπορεί να εμφανίζονται διαφημιστικά μηνύματα μόνο για γιατρούς συγκεκριμένης ειδικότητας ή μόνο σ' όσους κατοικούν σε μια συγκεκριμένη πόλη ή νομό. Μια εταιρεία μπορεί να επιλέξει το λεγόμενο *target group (ομάδα στόχευσης)*, δηλ. συγκεκριμένη ομάδα ή κατηγορία καταναλωτών στην οποία θα πρέπει να απευθυνθεί για να έχει περισσότερες πιθανότητες παραγγελιών.

Telnet - Είναι μια από τις πιο παλιές εφαρμογές του Internet, όπου έχουμε τη δυνατότητα για απομακρυσμένη διαχείριση ενός υπολογιστή από έναν άλλον, συνήθως μακρινό υπολογιστή. Με το πρόγραμμα αυτό μπορεί να γίνει και ο προγραμματισμός από απόσταση (τηλεχειρισμός) ενός δρομολογητή (router).

Traffic Manager - Όρος που αναφέρεται στο άτομο που έχει την ευθύνη της διαχείρισης και της παρακολούθησης των διαφημιστικών εκστρατειών ενός δικτυακού τόπου μέσω ειδικών προγραμμάτων (Ad Servers). Οι αρμοδιότητές του περιλαμβάνουν την τοποθέτηση των διαφημιστικών εκστρατειών και των δημιουργικών τους (creatives) καθώς και την δημιουργία αναφορών (reports) για την αποτελεσματικότητα της διαφημιστικής εκστρατείας.

UECA (Uniform Electronic Transactions Act) - Νομοθεσία σχετικά με το ηλεκτρονικό εμπόριο, που στηρίζεται στο μοντέλο του ΟΗΕ (Οργανισμός Ηνωμένων Εθνών).

URL (Uniform Resource Locator) - Αποδίδεται στα ελληνικά με τον όρο *Ομοιόμορφος Εντοπιστής Πόρων* και αναφέρεται στην πλήρη διεύθυνση μιας ιστοσελίδας στο Internet, που περιέχει το πρωτόκολλο, το domain name, την διαδρομή με τους φακέλους (αν υπάρχει) καθώς και το όνομα του αρχείου της ιστοσελίδας, όπου το προκαθορισμένο (default) όνομα αρχείου είναι συνήθως το index.html. Για παράδειγμα, ένα πλήρες URL είναι το εξής : http://www.florina.gr/Prespes/index.html.

User Tracking - Όρος που περιγράφει σε γενικές γραμμές την διαδικασία παρακολούθησης ή/και αναγνώρισης ενός χρήστη και καταγραφής της συμπεριφοράς του και των προτιμήσεών του καθώς αυτός πλοηγείται ανενόχλητος στο Internet. Η παρακολούθηση (tracking) ενός χρήστη μπορεί να γίνεται είτε για την κατανόηση των αναγκών του και την καλύτερη έτσι αυτόματη εξυπηρέτησή του είτε για την προβολή διαφημιστικών banners στην οθόνη του ανάλογα με τις προτιμήσεις του. Κάτι ανάλογο μπορεί να γίνει και με τη βοήθεια των cookies. Οι τεχνικές αυτές αποτελούν πολύτιμους αρωγούς του σύγχρονου marketing (e-marketing).

Verisign - Μια από τις πιο γνωστές διεθνώς εταιρείες που λειτουργεί ως Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ) και εκδίδει ψηφιακές ταυτότητες (digital ID's) σε τρίτους (ιδιώτες ή και εταιρείες). Οι εταιρείες αυτές αποκαλούνται και Έμπιστες Τρίτες Οντότητες (ΕΤΟ), δηλ. Trusted Third Parties (TTP), ή και Αρχές Πιστοποίησης (CA, Certification Authorities). Μια εταιρεία Παροχής Υπηρεσιών Πιστοποίησης μπορούν να εξουσιοδοτήσει άλλες εταιρείες σ' άλλες χώρες ή και σ' άλλες πόλεις για να κάνουν πιστοποιήσεις ατόμων ή εταιρειών και να σχηματιστεί έτσι ένα δένδρο από τους Οργανισμούς Πιστοποίησης.

Viral (Virual Marketing) - Ένας τρόπος έμμεσης διαφήμισης ενός δικτυακού τόπου, ο οποίος χρησιμοποιεί τους ίδιους τους χρήστες του ως διαφημιστές. Για παράδειγμα, οι περισσότεροι δικτυακοί τόποι που προσφέρουν δωρεάν λογαριασμούς ηλεκτρονικού ταχυδρομείου (e-mail) επισυνάπτουν κι ένα σύντομο διαφημιστικό ή ενημερωτικό μήνυμα στο τέλος του κάθε e-mail που στέλνουν οι χρήστες τους.

WAN (Wide Area Network) - Αποδίδεται στα ελληνικά με τον όρο *Δίκτυο Ευρείας Περιοχής* και είναι ένα δίκτυο υπολογιστών που καλύπτει μεγάλη γεωγραφική έκταση, όπως είναι τα δίκτυα των Τραπεζών, των αεροπορικών εταιρειών κ.ά. σε αντίθεση με τα Τοπικά Δίκτυα (LANs), που καλύπτουν περιορισμένη γεωγραφική έκταση, όπως είναι ο χώρος ενός σχολείου ή μιας εταιρείας ή μιας υπηρεσίας κ.ά.

Web Browser - Αποδίδεται στα ελληνικά με τον όρο *Φυλλομετρητής* ή *Πρόγραμμα Περιήγησης* ή *Πρόγραμμα Ανάγνωσης Ιστοσελίδων* ή *Πλοηγός* ή και *Ιστηλάτης* και είναι ένα ειδικό λογισμικό (πρόγραμμα) για την πρόσβαση σε δικτυακούς τόπους (Web sites) και την προβολή και αποθήκευση στον υπολογιστή του χρήστη των ιστοσελίδων (Web pages) που αυτοί περιέχουν, δηλ. αρχείων με επέκταση .html ή .htm ή και άλλα.

Με τα προγράμματα αυτά μπορούμε σήμερα εκτός από την υπηρεσία του Παγκόσμιου Ιστού (World Wide Web) να εκμεταλλευτούμε και άλλες υπηρεσίες του Internet, όπως είναι το Web mail για λήψη και αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mails), το FTP για αποστολή (uploading) και κατέβασμα (downloading) αρχείων από τους Web servers κ.ά. Οι πιο γνωστοί φυλλομετρητές είναι σήμερα ο Internet Explorer της εταιρείας Microsoft, ο Netscape, ο Mozilla και ο Opera.

Web Campaign - Όρος που αναφέρεται σε μια διαφημιστική εκστρατεία που προορίζεται ή εκτελείται αποκλειστικά στο Internet.

Web Hosting - Έτσι αποκαλείται η υπηρεσία παροχής χώρου (Web space) για την φιλοξενία ή και υποστήριξη της δημιουργίας και της συντήρησης ενός δικτυακού τόπου (Web site). Παρέχεται συνήθως από τους λεγόμενους Παροχείς Υπηρεσιών Internet (ISPs - Internet Service Providers).

Web Page - Αποδίδεται στα ελληνικά με τον όρο *Ιστοσελίδα* και είναι ένα αρχείο με επέκταση .html ή .htm ή .shtml ή και .asp, .php, .cfm, .jsp, αν πρόκειται για δυναμικά παραγόμενες ιστοσελίδες. Πολλές ιστοσελίδες μαζί, κατάλληλα οργανωμένες και με τους σχετικούς συνδέσμους (links) αποτελούν έναν δικτυακό τόπο (Web site). Μπορούμε να δημιουργήσουμε ένα αρχείο ιστοσελίδας είτε μ' ένα από τα γνωστά προγράμματα όπως είναι το FrontPage και το Dreamweaver ή και να γράψουμε απευθείας σε κώδικα HTML μέσα από ένα πρόγραμμα όπως είναι το Σημειωματάριο (Notepad) των Windows και να κάνουμε αποθήκευση με μια από τις αποδεκτές επεκτάσεις που αναφέραμε νωρίτερα.

Web Promotion - Όρος που αναφέρεται στις online προσφορές που μπορούν να αξιοποιηθούν μέσω του Internet. Εκτός από τις online διαφημίσεις, κατάλληλες τεχνικές promotion μπορούν να θεωρηθούν ότι αποτελούν και οι καταχωρήσεις σε μηχανές αναζήτησης (search engines) ή οι αντίστοιχες ανακοινώσεις σε ομάδες ειδήσεων ή καταλόγους ηλεκτρονικού ταχυδρομείου κ.ά.

Web Server - Αποδίδεται στα ελληνικά με τον όρο *Εξυπηρετητής Παγκόσμιου Ιστού* και είναι ένας ειδικός server που βρίσκεται στις εγκαταστάσεις ενός Παροχέα Υπηρεσιών Internet (ISP - Internet Service Provider), περιέχει αποθηκευμένες τις ιστοσελίδες των χρηστών (πελατών) του ISP και αναλαμβάνει να εξυπηρετήσει όσους τρίτους ζητήσουν κάποια από τις ιστοσελίδες αυτές.

Web Site - Αποδίδεται στα ελληνικά με τον όρο *Δικτυακός Τόπος* ή *Ιστοχώρος* ή *Ιστότοπος* και είναι ένα σύνολο από κατάλληλα οργανωμένες ιστοσελίδες με τους σχετικούς συνδέσμους (links) ανάμεσά τους, ώστε να μπορούμε να πλοηγούμαστε στον δικτυακό τόπο. Ένας δικτυακός τόπος θα πρέπει να διαθέτει και μια αρχική σελίδα ή οικοσελίδα (Home Page), που θα αποτελεί την πύλη εισόδου μας στον δικτυακό τόπο, θα πρέπει να περιέχει δηλαδή κάτι σαν έναν εύχρηστο πίνακα περιεχομένων για να είναι έτσι πιο φιλική η περιήγησή μας.