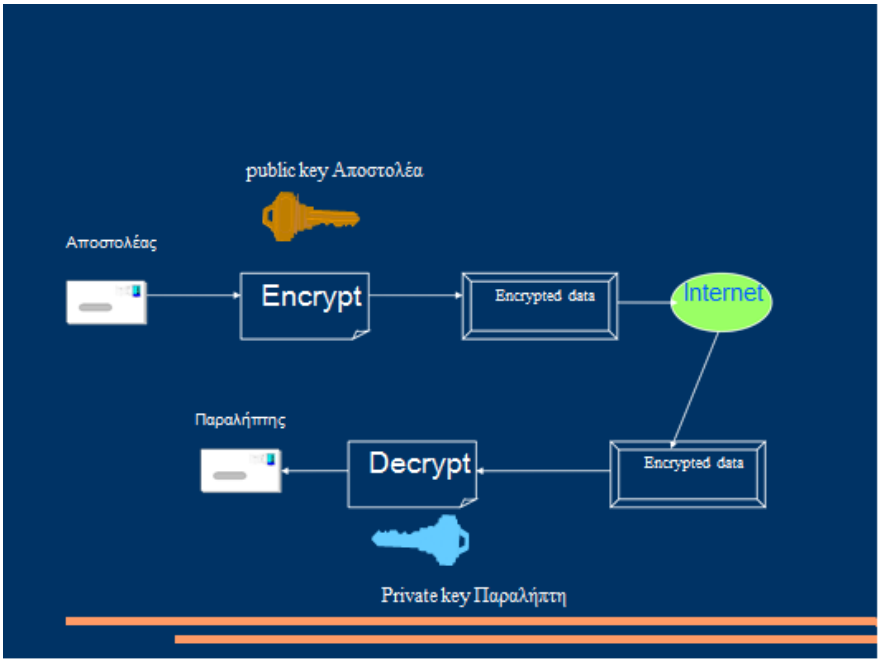
Α.ΤΕΙ ΚΡΗΤΗΣ
ΠΑΡΑΡΤΗΜΑ ΧΑΝΙΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

"ΤΑ ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΚΑΙ ΟΙ ΧΡΗΣΙΜΟΤΗΤΑ ΤΟΥΣ"



ΧΑΤΖΗΣΤΕΦΑΝΟΥ ΣΤΥΛΙΑΝΟΣ

ΧΑΝΙΑ ΜΑΙΟΣ 2013

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΜΠΑΡΜΟΥΝΑΚΗΣ ΙΩΑΝΝΗΣ

Περιεχόμενα

ΠΕΡΙΛΗΨΗ

Στις μέρες μας οι επιθέσεις εναντίον δικτύων έχουν πάρει μεγάλη έκταση και προκαλούν πολλά προβλήματα σε οργανισμούς, εταιρείες και χρήστες. Συνήθως στόχος ενός κακόβουλου είναι η υποκλοπή απόρρητων δεδομένων και η χρήση τους προς όφελός του. Η προστασία και η ασφάλεια της ευαίσθητης αυτής πληροφορίας, που διατηρείται και αποστέλλεται σε ένα δίκτυο κρίνεται επιτακτική. Η διασφάλιση της ακεραιότητας της πληροφορίας απαιτεί την χρήση μαθηματικών τεχνικών οι οποίες παρέχονται μέσω της επιστήμης της Κρυπτογραφίας.

Σκοπός της πτυχιακής εργασίας είναι η μελέτη και η σύγκριση των διαφόρων τεχνικών της Κρυπτογραφίας που έχουν αναπτυχθεί και χρησιμοποιούνται σήμερα. Παρουσιάζονται οι βασικοί κρυπτογραφικοί αλγόριθμοι και γίνεται ενδελεχής ανάλυση της αρχιτεκτονικής ενός συστήματος κρυπτογραφίας.

.

ΕΙΣΑΓΩΓΗ

Το Διαδίκτυο (Internet), φέρνοντας την τελευταία εικοσαετία επανάσταση στον κόσμο των επικοινωνιών, έγινε το κυριότερο εργαλείο για την εξέλιξη και την υποστήριξη διαδικτυακών υπηρεσιών (server – client services). Ένα μέλλον γεμάτο προοπτικές διανοίχτηκε για τον κόσμο του εμπορίου χάρις στην ταχύτατη εξάπλωση της χρήσης του Διαδικύου και στη διαθεσιμότητα μηχανημάτων μεγάλης υπολογιστικής ισχύος. Στις μέρες μας αυτός ο διαδικτυακός ιστός είναι απαραίτητος σαν μηχανισμός διακίνησης πληροφοριών , σαν μέσο επικοινωνίας και συνεργασίας μεταξύ ατόμων, κυβερνητικών υπηρεσιών, οικονομικών οργανισμών, και επιχειρήσεων ανεξαρτήτως της γεωγραφικής τοποθεσίας τους.

Παράλληλα όμως με την ανάπτυξη των τεχνολογιών αυτών, εξελίσσονται και οι επιθέσεις στα συστήματα που τις υλοποιούν. Οι επιθέσεις αυτές μπορούν να πάρουν διάφορες μορφές αλλά και να συνδυάσουν την δράση τους. Δεδομένης της κατάστασης αυτής η ασφάλεια των δικτύων και των εφαρμογών τους από κακόβουλους χρήστες κρίνεται επιτακτική.

Είναι συνεπώς αυτονόητο το γεγονός ότι αυτή η συνεχώς αυξανόμενη χρήση του Διαδικτύου έχει ως άμεση συνέπεια τα προβλήματα ασφάλειας που προκύπτουν να αντιμετωπίζονται απο τους προγραμματιστές με μέγιστη προσοχή και σαφήνεια. Το κυριότερο εργαλείο για την αντιμετώπιση επιθέσεων ασφάλειας είναι η κρυπτογραφία. Η κρυπτογραφία παρέχει στους προγραμματιστές τις απαραίτητες τεχνικές για την διατήρηση της μυστικότητας της πληροφορίας (Confidentiality) , βοηθά στην εξασφάλιση της ακεραιότητάς της (Integrity) , στην πιστοποίηση της προέλευσής της (Authentication) καθώς επίσης και στην μη δυνατότητα άρνησης αποστολής της από ένα χρήστη (Non-repudiation) .

Συνοπτικά τα κεφάλαια της εργασίας είναι δομημένα ως εξής :

- Κεφάλαιο 1: Παρουσίαση των βασικών αρχών της Κρυπτογραφίας και των αλγόριθμων αυτής (συμμετρικοί, αλγόριθμοι δημόσιου κλειδιού) καθώς επίσης και της σύγκρισης αυτών. Αναφέρονται επίσης οι βασικές επιθετικές τεχνικές που χρησιμοποιούνται εναντίον των αλγόριθμων αυτών. Τέλος παρουσιάζονται οι βασικές τεχνικές ψηφιακών υπογραφών.
- Κεφάλαιο 2: Η σημασία της διαχείρισης των κλειδιών σε ένα σύστημα κρυπτογραφίας και ο ρόλος των «εμπιστευόμενων» οντοτήτων (trusted third parties) που υπάρχουν σε αυτό. Επίσης γίνεται ανάλυση στις τεχνικές διανομής δημοσίου κλειδιού.
- Κεφάλαιο 3: Αναλυτική παρουσίαση της αρχιτεκτονικής ενός δικτύου που χρησιμοποιεί τεχνικές κρυπτογραφίας δημόσιου κλειδιού (Public Key Infrastructure)
- Κεφάλαιο 4 : Συμπεράσματα και προτάσεις για βελτιώσεις του όλου πλαισίου ασφάλειας με χρήση τεχνικών κρυπτογραφίας

ΚΕΦΑΛΑΙΟ 1: ΚΡΥΠΤΟΓΡΑΦΙΑ

1.1 ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

Στις μέρες μας οι επιθέσεις εναντίον δικτύων και υπολογιστικών συστημάτων έχουν πάρει μεγάλη έκταση και προκαλούν πολλά προβλήματα σε οργανισμούς, εταιρείες και χρήστες. Συνήθως στόχος ενός κακόβουλου ατόμου είναι η υποκλοπή απόρρητων δεδομένων και η χρήση τους προς όφελός του. Η προστασία και η ασφάλεια της ευαίσθητης αυτής πληροφορίας, είτε διατηρείται κάπου αποθηκευμένη είτε αποστέλλεται μέσω του δδιαδικτύου, κρίνεται επιτακτική.

Η διασφάλιση της ακεραιότητας της πληροφορίας απαιτεί την χρήση μαθηματικών τεχνικών οι οποίες παρέχονται μέσω της επιστήμης της Κρυπτογραφίας. Η επιστήμη αυτή παρέχει την δυνατότητα ασφαλούς αποθήκευσης ευαίσθητης πληροφορίας, καθώς επίσης και αποστολής αυτής μέσω μη ασφαλών δικτύων, εξασφαλίζοντας την ανάγνωσή της μόνο από τον εξουσιοδοτούμενο παραλήπτη. Θα πρέπει να τονισθεί ότι η Κρυπτογραφία δεν αποτελεί το μοναδικό εργαλείο που εξασφαλίζει την ασφάλεια της πληροφορίας, παρά μόνο αποτελεί ένα σύνολο συνεχώς εξελισσόμενων αλγορίθμων.

1.1.1 Στόχοι Κρυπτογραφίας

Οι κυριότεροι στόχοι της Κρυπτογραφίας είναι οι εξής :

1. Η *Μυστικότητα της Πληροφορίας* (Confidentiality) εξασφαλίζει ότι το περιεχόμενο της πληροφορίας είναι διαθέσιμο μόνο στον νόμιμο κάτοχο αυτής και μυστικό σε κάθε άλλο εκτός αυτού. Για την επίτευξη του στόχου αυτού μπορούν να χρησιμοποιηθούν είτε φυσικά μέσα είτε

μαθηματικοί αλγόριθμοι οι οποίοι καθιστούν τα δεδομένα μη αναγνώσιμα.

2. Η *Ακεραιότητα της Πληροφορίας* (Integrity) αναφέρεται στη αλλοίωση των δεδομένων. Για να διακρίνει κάποιος την αλλοίωση της πληροφορίας θα πρέπει να διαθέτει μέσα ώστε να μπορεί να εξετάσει την αποκοπή, αντικατάσταση ή εισαγωγή δεδομένων.

3. Η *Πιστοποίηση της Προέλευσης και Αυθεντικότητας της Πληροφορίας* (Authentication) έχει δύο διαστάσεις. Η πρώτη αναφέρεται στα άκρα της επικοινωνίας (entity authentication): οι δύο οντότητες που επικοινωνούν θα πρέπει να αναγνωρίζουν η μία την άλλη. Σαν δεύτερη προϋπόθεση ορίζεται η αναγνώριση της προέλευσης της πληροφορίας (data origin authentication). Είναι αναγκαίο να πιστοποιείται η προέλευση των δεδομένων, το περιεχόμενό τους, ο χρόνος καθώς η ημερομηνία αποστολής τους.

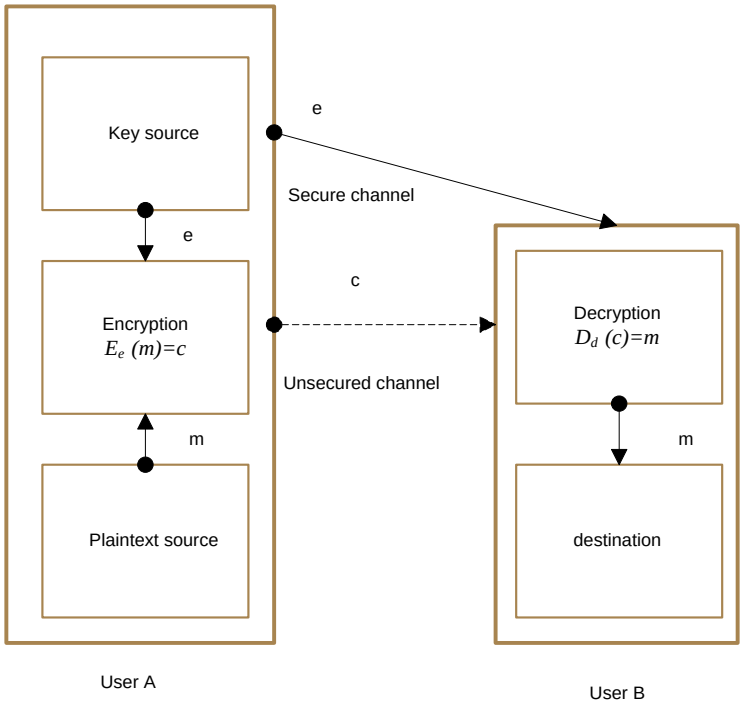
4. Η *Απαγόρευση Άρνησης της Αποστολής της Πληροφορίας* (Non-repudiation) από μία οντότητα είναι απολύτως σημαντική για ένα ασφαλές δίκτυο. Σαν παράδειγμα μπορούμε να αναφέρουμε την περίπτωση μιας οντότητας η οποία εξουσιοδοτεί μια άλλη οντότητα στο να έχει πρόσβαση σε μία πληροφορία και στην συνέχεια να υποστηρίξει πως ουδέποτε είχε παραχωρήσει τέτοια δικαιοδοσία. Στην περίπτωση αυτή κρίνεται αναγκαία η ύπαρξη μιας απολύτως εμπιστευόμενης τρίτης οντότητας (trusted third party) ώστε να δοθεί μία λύση.

Συνεπώς, πρωταρχικός στόχος της Κρυπτογραφίας είναι να συνδυάσει επιτυχώς τα ανωτέρω θεμελιώδη αιτήματα σε επίπεδο εφαρμογής.

1.2 ΑΛΓΟΡΙΘΜΟΙ ΣΥΜΜΕΤΡΙΚΟΥ ΚΛΕΙΔΙΟΥ (SYMMETRIC KEY ENCRYPTION)

Ας θεωρήσουμε ένα μοντέλο κρυπτογράφησης το οποίο αποτελείται από τις μαθηματικές συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης $\{ E_e : e \in K\}$ και $\{ D_d : d \in K\}$, αντίστοιχα , όπου K είναι ένα σύνολο κλειδιών. Το μοντέλο αυτό είναι *συμμετρικού κλειδιού* όταν εξασφαλίζεται η εξής προυπόθεση: για κάθε ζεύγος κλειδιών (***e,d***) μπορεί κάποιος να δημιουργήσει το κλειδί αποκρυπτογράφησης d από το κλειδί κρυπτογράφησης e με μαθηματικούς υπολογισμούς, και το αντίστροφο. Είναι σύνηθες σε πολλά κρυπτογραφικά συστήματα συμμετρικού κλειδιού το κλειδί e να συμπίμπτει με το κλειδί d για καθαρά πρακτικούς λόγους.

Στο μπλοκ διάγραμμα του σχήματος 1.1 απεικονίζεται μια διμερής επικοινωνία με κρυπτογραφία συμμετρικού κλειδιού. Γίνεται κατανοητό ότι η ασφάλεια ενός συμμετρικού αλγόριθμου βασίζεται στο κλειδί. Οι συμμέτοχοι σε ένα σύστημα συμμετρικού κλειδιού είναι αναγκαίο να συμφωνήσουν στο πως θα ανταλλάξουν με σίγουρο και ασφαλή τρόπο το κλειδί πριν αρχίσει η ασφαλής επικοινωνία μεταξύ τους. Το πρόβλημα αυτό είναι θεμελιώδες και ονομάζεται πρόβλημα *διανομής κλειδιού* (key distribution problem). Σε περίπτωση που το κλειδί γίνει γνωστό με οποιοδήποτε τρόπο σε κάποιο εξωτερικό παράγοντα τότε αυτός είναι ικανός να αποκρυπτογραφεί και να κρυπτογραφεί μηνύματα, γεγονός το οποίο είναι απ'ευκταίο. Σύμφωνα με τα παραπάνω, η κρυπτογραφία συμμετρικού κλειδιού συνηθίζεται να λέγεται κρυπτογραφία *μυστικού κλειδιού* (secret-key cryptography) [2].



Σχήμα 1.1 Διμερής επικοινωνία με κρυπτογραφία συμμετρικού κλειδιού

Οι αλγόριθμοι συμμετρικού κλειδιού χωρίζονται σε δύο κατηγορίες ανάλογα με την μεταχείριση της πληροφορίας προς κρυπτογράφηση :

- τους αλγόριθμους που χειρίζονται μπλοκ δυαδικών ψηφίων (block ciphers)
- τους αλγόριθμους που χειρίζονται ξεχωριστά κάθε δυαδικό ψηφίο της πληροφορίας (stream ciphers)

1.2.1 Συμμετρικοί μπλοκ αλγόριθμοι (block ciphers)

Ένας συμμετρικός μπλοκ αλγόριθμος χωρίζει τα μη κρυπτογραφημένα δεδομένα (plaintext) σε μπλοκς δυαδικών ψηφίων συγκεκριμένου μήκους t (block size) και κρυπτογραφεί ξεχωριστά το κάθε ένα από αυτά με τη χρήση ενός μυστικού κλειδιού. Το αποτέλεσμα είναι ένα μπλοκ κρυπτογραφημένων δεδομένων (ciphertext) το οποίο έχει το ίδιο μήκος με το αρχικό. Το σύνολο των κρυπτογραφημένων μπλοκς αποτελεί το κρυπτογραφημένο μήνυμα.

Το μεγαλύτερο ποσοστό αυτών των αλγόριθμων είναι επαναλαμβανόμενοι καθώς χειρίζονται αλυσιδωτά τα μπλοκ δεδομένων. Ο αριθμός των επαναλήψεων ενός τέτοιου αλγόριθμου εξαρτάται από το επίπεδο της ασφάλειας που θέλει κάποιος να επιτύχει. Όπως είναι φυσικό ένας αυξημένος αριθμός επαναλήψεων αυξάνει σημαντικά την ασφάλεια αλλά έχει αρνητικές συνέπειες στην απόδοσή του καθώς αυξάνεται ο υπολογιστικός χρόνος. Επίσης ένα πολύ σημαντικό στοιχείο είναι και το μέγεθος των μπλοκ δεδομένων (block size). Οι περισσότεροι από τους μπλόκ αλγόριθμους χρησιμοποιούν μεγέθη μπλοκ πάνω από 8 bytes (64 bits). Ένας αλγόριθμος του οποίου το μέγεθος μπλοκ (block size) είναι πολύ μικρό είναι σίγουρο ότι είναι ευάλωτος σε επιθέσεις βασισμένες σε στατιστική ανάλυση (ανάλυση της συχνότητας εμφάνισης συγκεκριμένων συστοιχιών bits (bit patterns) μέσα στα δεδομένα). Εν' τούτοις το να διαλέξει κάποιος ένα μεγάλο μέγεθος μπλοκ αυξάνει σημαντικά τον υπολογιστικό φόρτο του αλγόριθμου.

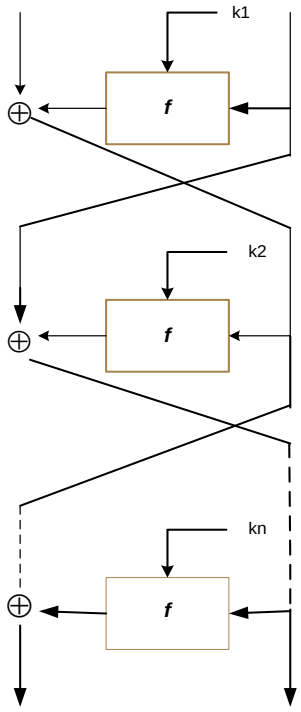
Οι κυριότεροι συμμετρικοί μπλοκ αλγόριθμοι είναι ο DES (Data Encryption Standard), ο Triple-DES και ο AES.

1.2.1.1. Αλγόριθμος Data Encryption Standard (DES)

Ο αλγόριθμος DES είναι ο πιο χαρακτηριστικός συμμετρικός μπλοκ αλγόριθμος που έχει εξελιχθεί τα τελευταία 20 χρόνια. Χρησιμοποιεί μπλοκς των 64 bits και κλειδί των 56 bits. Η είσοδος (input) στον αλγόριθμο είναι μπλοκ των 64 bits μη κρυπτογραφημένου κειμένου (plaintext), και μετά από 16 επαναλήψεις (συνδιασμός μεταθέσεων και αντικαταστάσεων) δίνει έξοδο (output) ένα μπλοκ ίδιου μεγέθους με κρυπτογραφημένα δεδομένα (ciphertext). Αν το μέγεθος του μη κρυπτογραφημένου κειμένου (plaintext) δεν είναι ακέραιο

πολλαπλάσιο του μεγέθους του μπλοκ (64 bits) τότε χρησιμοποιείται μια διαδικασία *συμπλήρωσης* (padding) με bits ώστε να προκύψει plaintext πολλαπλάσιου μεγέθους των 64 bits. Οι πιο γνωστοί μέθοδοι συμπλήρωσης είναι ο PKCS #5 , ο PKCS#7 , ο ISO10126-2Padding και ο X9.23Padding.

Η λειτουργία του DES στηρίζεται στους λεγόμενους αλγόριθμους του Feistel , οι οποίοι ονομάζονται και τύπου DES(σχήμα 1.2)



Σχήμα 1.2 Feistel Cipher

Μια παραλλαγή του DES είναι ο Triple-DES αλγόριθμος, ο οποίος χρησιμοποιεί το ίδιο μέγεθος μπλοκ με τον DES (64 bits) εφαρμόζοντας τον DES τρεις φορές διαδοχικά , με τρία διαφορετικά κλειδιά των 56 bits (K1 , K2 , K3). Η αποκρυπτογράφηση γίνεται με την αντίστροφη διαδικασία, εφαρμόζοντας δηλαδή πρώτα το κλειδί K3, μετά το K2 και τέλος το K1. Συνεπώς η κρυπτογραφική δύναμη του Triple-DES είναι τριπλάσια από αυτή του DES(56*3=168 bits).

Ο αλγόριθμος Triple-DES ανήκει στους αποδεκτούς αλγόριθμους της κυβέρνησης των Η.Π.Α. (US Approved Algorithms List) , ενώ ο DES αφαιρέθηκε από την ανωτέρω λίστα το 2005.

1.2.1.2 Αλγόριθμος Advanced Encryption Standard (AES)

Ο αλγόριθμος AES αναπτύχθηκε το 2000 και προστέθηκε στη λίστα αποδεκτών αλγορίθμων των Η.Π.Α. Ο AES είναι γρηγορότερος από τον DES και υποστηρίζει μεγαλύτερα μεγέθη κλειδιών. Ο τρόπος με τον οποίο κάνει την κρυπτογράφιση είναι παρόμοιος με αυτόν του DES με τις εξής διαφορές : το μέγεθος του μπλοκ του AES είναι 128 bits και υποστηρίζει τρία μεγέθη κλειδιών (128, 192 και 256 bits) , καθιστώντας τον δυνατότερο από τον DES.

1.2.1.3. Τρόποι λειτουργίας (Modes of Operation)

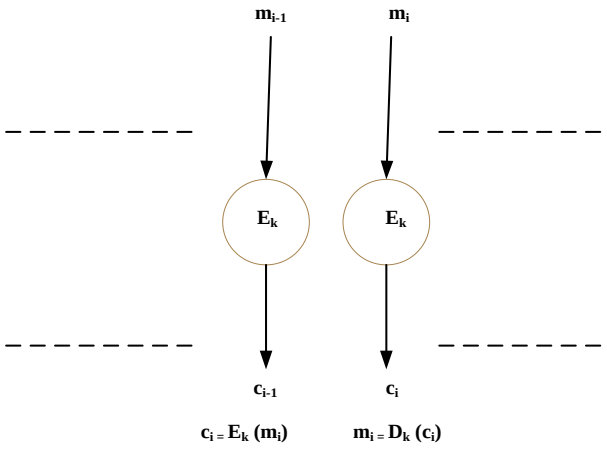
Όπως έχει αναφερθεί προηγουμένως, όταν κάποιος θέλει να κρυπτογραφήσει δεδομένα με μέγεθος που δεν είναι πολλαπλάσιο του μεγέθους του μπλοκ δεδομένων τότε χρησιμοποιείται μια διαδικασία *συμπλήρωσης* (padding) με bits ώστε να προκύψει plaintext πολλαπλάσιου μεγέθους του block size που χρησιμοποιεί ο αλγόριθμος. Στην συνέχεια υπάρχουν δύο δυνατότητες : είτε να κρυπτογραφηθεί κάθε μπλοκ ανεξάρτητα από τα άλλα , είτε να ακολουθηθεί μία πιο πολύπλοκη μέθοδος, σύμφωνα με την οποία η κρυπτογράφηση κάθε μπλοκ εξαρτάται από κάποιες παραμέτρους που προέκυψαν από την κρυπτογράφηση των προηγούμενων μπλοκ. Αυτές οι διαδικασίες ονομάζονται *τρόποι λειτουργίας* (Modes of Operation) και είναι αναγκαίο η επιλογή κάποιου εξ' αυτών να γίνεται με γνώμονα την μέγιστη ασφάλεια και την ελαχιστοποίηση του υπολογιστικού φόρτου του αλγόριθμου. Σύμφωνα με την λίστα των αποδεκτών

τρόπων λειτουργίας (Approved Modes of Operation) οι αλγόριθμοι DES και Triple-DES έχουν 7 αποδεκτούς τρόπους λειτουργίας , ενώ ο AES έχει 5 [3].

Οι κυριότεροι τρόποι λειτουργίας, οι οποίοι εφαρμόζονται αποκλειστικά σε όλες τις πρακτικές εφαρμογές είναι ο ECB (Electronic Code Book) και ο CBC (Cipher Block Chaining) .Ας αναφερθούμε σ'αυτούς αναλυτικότερα.

1.2.1.3.1 Λειτουργία ECB (Electronic Code Book)

Η λειτουργία του τρόπου ECB (σχήμα 1.3) είναι η πιο απλή καθώς ο αλγόριθμος κρυπτογραφεί το κάθε μπλοκ δεδομένων ανεξάρτητα από τα άλλα, παρουσιάζει όμως κάποια προβλήματα.



Σχήμα 1.3 Electronic Code Book

Τα κυριότερα είναι τα εξής:

1. Τα δυαδικά ψηφία που αποτελούν το κρυπτογραφημένο μήνυμα (ciphertext) είναι πάντοτε τα ίδια όταν το μη κρυπτογραφημένο μήνυμα

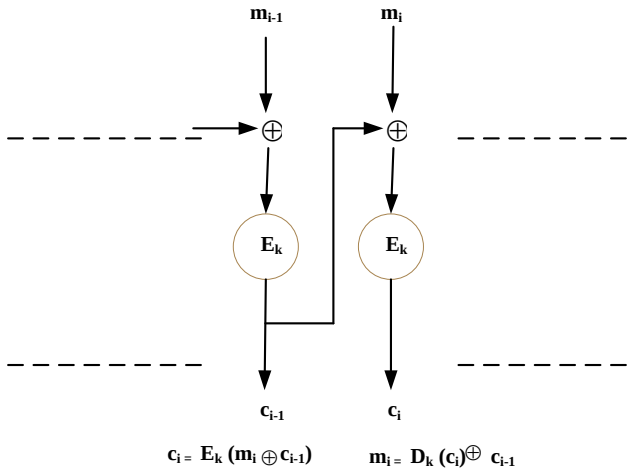
(plaintext) παραμένει το ίδιο. Αυτό έχει επίσης ως αποτέλεσμα την εμφάνιση συγκεκριμένων συστοιχιών bits (bit patterns) μέσα στα κρυπτογραφημένα δεδομένα, γεγονός που μπορεί να εκμεταλλευτεί κάποιος κακόβουλος και να αναδημιουργήσει το αρχικό μήνυμα εύκολα.

2. Η αλλαγή ενός bit στο αρχικό μήνυμα θα επηρεάσει μόνο το συγκεκριμένο μπλοκ στο ciphertext. Το γεγονός αυτό είναι απευκταίο καθώς θα ήταν προτιμότερο, το ciphertext να επηρεάζεται συνολικά για λόγους ασφάλειας.

Μια λύση στα παραπάνω μειονεκτήματα είναι να προστεθεί μία παράμετρος τυχαίου αριθμού στην διαδικασία ώστε η κρυπτογράφηση ενός μπλοκ να επηρεάζεται από τις τιμές των προηγούμενων μπλοκ. Αυτό επιτυγχάνεται με την λειτουργία CBC (Cipher Block Chaining).

1.2.1. Λειτουργία CBC (Cipher Block Chaining Mode)

Η λειτουργία αυτή (σχήμα 1.4) χρησιμοποιεί ένα συμπληρωματικό μπλοκ, το οποίο χρησιμοποιείται για την αρχικοποίηση της διαδικασίας (μπλοκ c_0 του σχήματος), καθώς και την λογική πράξη αποκλειστικό-ή (XOR). Συγκεκριμένα κάθε μπλοκ του plaintext υπόκειται στη λογική πράξη XOR με τα προηγούμενα μπλοκ του ciphertext, και στη συνέχεια κρυπτογραφείται.



Σχήμα 1.4 Cipher Block Chaining Mode

Με την λειτουργία CBC επιτυγχάνουμε δύο σημαντικά πράγματα:

1. Η κρυπτογράφηση ενός μηνύματος ποτέ δεν θα έχει το ίδιο αποτέλεσμα το ciphertext δηλαδή δεν θα είναι ποτέ το ίδιο.
2. Η αλλαγή ενός bit στο plaintext θα επηρεάσει όχι μόνο το μπλοκ στο οποίο ανήκει , αλλά θα αλλάξει ολόκληρο το ciphertext.

Είναι, συνεπώς, κατανοητό το γεγονός ότι οι αλγόριθμοι DES, Triple-DES, και AES χρησιμοποιούνται ευρέως σε λειτουργία CBC σε πρωτόκολλα όπως IPSec, SSL και TLS.

1.2.2 Stream Ciphers

Οι stream ciphers είναι αλγόριθμοι συμμετρικής κρυπτογραφίας και είναι σχεδιασμένοι έτσι ώστε να είναι πολύ πιο γρήγοροι από τους block ciphers. Ενώ οι τελευταίοι δουλεύουν πάνω σε μεγάλα μπλοκ δεδομένων, οι stream ciphers χρησιμοποιούν για την κρυπτογραφία συνήθως μόνο ένα bit. Θα μπορούσαμε λοιπόν να πούμε ότι αποτελούνμια παραλλαγή των block ciphers μόνο που το block size τους είναι του ενός bit.

Όπως γνωρίζουμε το κρυπτογραφημένο αποτέλεσμα (ciphertext) των block ciphers είναι, για συγκεκριμένο plaintext, πάντα το ίδιο, όταν χρησιμοποιηθεί το ίδιο κλειδί. Εντούτοις , με τους stream ciphers, το ciphertext θα εξαρτηθεί από το πότε, μέσα στη διαδικασία της κρυπτογράφησης, θα χειριστεί ο αλγόριθμος το κάθε bit. Το ciphertext, συνεπώς, είναι πάντα διαφορετικό και μπορούμε να πούμε ότι οι stream ciphers έχουν *«μνήμη»*, εξαρτώνται δηλαδή από την προηγούμενη κατάστασή τους (state ciphers). Αυτή όμως η διαφορά μεταξύ των block και stream ciphers δεν είναι κατ' ανάγκη ουσιαστική. Αν προσθέσουμε την ιδιότητα της «μνήμης» σε block ciphers (όπως συμβαίνει στον CBC) μπορούμε να έχουμε μία μορφή stream cipher με μεγαλύτερα μεγέθη μπλοκ από ένα bit.

Στην πραγματικότητα, η λειτουργία ενός stream cipher παρουσιάζει αρκετές διαφοροποιήσεις από έναν μπλοκ cipher. Κάθε τέτοιος αλγόριθμος δημιουργεί μία ακολουθία bits που χρησιμεύουν ως κλειδί και ονομάζονται *keystream*. Η

κρυπτογράφηση γίνεται εκτελώντας την λογική πράξη XOR για κάθε bit του μη κρυπτογραφημένου μηνύματος και του keystream. Οι stream ciphers διακρίνονται σε δύο κατηγορίες, ανάλογα με την συμπεριφορά του keystream:

- Synchronous stream ciphers, όταν η δημιουργία του keystream είναι ανεξάρτητη του plaintext και του ciphertext
- Self-synchronizing stream ciphers, όταν το keystream εξαρτάται από τα δεδομένα και την κατάσταση της κρυπτογράφησης αυτών.

Οι περισσότεροι stream ciphers που χρησιμοποιούνται ανήκουν στην πρώτη από αυτές τις δύο κατηγορίες και ο σπουδαιότερος από αυτούς είναι ο RC4.

1.3 HASH FUNCTIONS, MESSAGE DIGEST KAI MAC (Message Authentication Code)

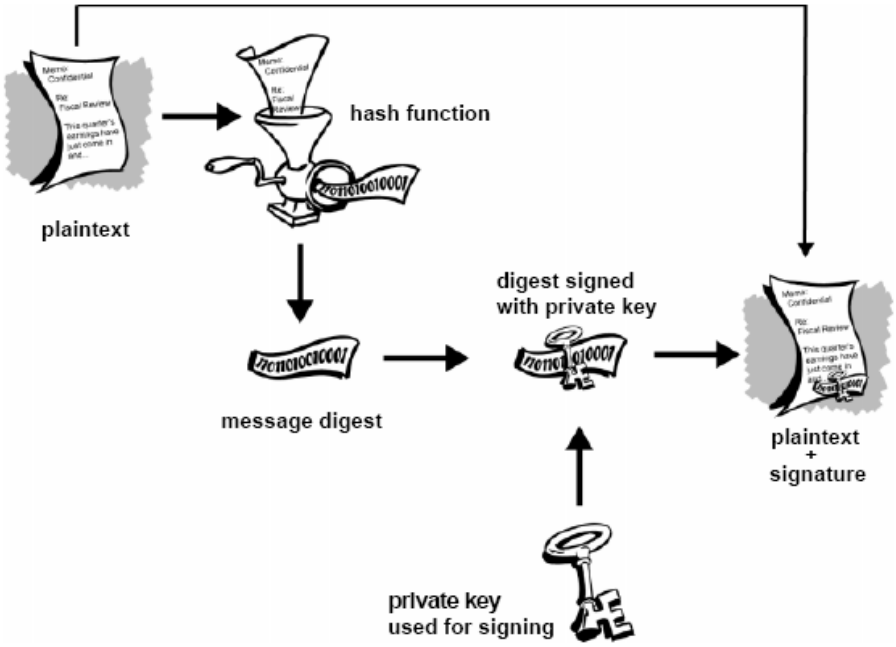
1.3.1 Hash Functions

Μία hash function είναι συνάρτηση που παίρνει μία είσοδο m και επιστρέφει μία ακολουθία δυαδικών ψηφίων συγκεκριμένου μήκους, η οποία ονομάζεται τιμή hash *h* (hash value), δηλαδή *h =H (m).* Οι κυριότερες απαιτήσεις στην κρυπτογραφία, για μία τέτοια συνάρτηση είναι οι εξής:

- Η είσοδος (input) μπορεί να είναι μεταβλητού μήκους.
- Η έξοδος (output) είναι συγκεκριμένου μήκους.
- Η συνάρτηση *H(x)*, για δεδομένο x , είναι εύκολα υπολογίσιμη.
- Η *H(x)* είναι μη-αντιστρέψιμη συνάρτηση, δηλαδή για δεδομένο hash value *h* είναι υπολογιστικώς αδύνατο να βρεθεί *x*, ώστε να ισχύει *H(x)=h.*
- Η *H(x)* είναι συνάρτηση 1-1, δηλαδή για $x \neq y$, ισχύει $H(x) \neq H(y)$ και το αντίστροφο.

Η τιμή hash αντιπροσωπεύει το μη κρυπτογραφημένο κείμενο από το οποίο προήλθε (plaintext) και γι' αυτό ονομάζεται και *message digest*. Ουσιαστικά το message digest αποτελεί ένα «ψηφιακό αποτύπωμα» του plaintext και είναι μοναδικό.

Η συνήθης χρήση των συναρτήσεων hash στην κρυπτογραφία εντοπίζεται στις ψηφιακές υπογραφές και στην πιστοποίηση της ακεραιότητας των δεδομένων. Στις ψηφιακές υπογραφές, στις οποίες θα αναφερθούμε ειδικότερα σε επόμενο κεφάλαιο, το αρχικό κείμενο δίνεται σε μία hash function για επεξεργασία, και στη συνέχεια υπογράφεται, με το ιδιωτικό κλειδί, το message digest το οποίο προκύπτει (σχήμα 1.5). Ο παραλήπτης της υπογραφής χρησιμοποιεί την ίδια hash function στο αρχικό κείμενο και επιβεβαιώνει ότι η υπογραφή αντιστοιχεί στο message digest που παρέλαβε (αφού το αποκρυπτογραφήσει με το δημόσιο κλειδί του αποστολέα).



Σχήμα 1.5 Σχηματικό παράδειγμα ψηφιακής υπογραφής

Ο τρόπος αυτός μειώνει σε σημαντικό βαθμό τον υπολογιστικό χρόνο και τον αποθηκευτικό χώρο που θα χρειαζόταν αν η υπογραφή γινόταν πάνω στο αρχικό κείμενο. Τότε θα έπρεπε το κείμενο να χωριζόταν σε επιμέρους μπλοκ δεδομένων, καθένα από τα οποία θα υπογραφόταν ξεχωριστά.

Οι συναρτήσεις hash χρησιμεύουν σε μεγάλο βαθμό και στον έλεγχο της ακεραιότητας του αρχικού κειμένου. Ο καθένας μπορεί, σε οποιαδήποτε στιγμή να υπολογίζει το message digest δεδομένων που τον ενδιαφέρουν και να το

συγκρίνει με το message digest των ίδιων δεδομένων που έχει υπολογίσει σε προγενέστερη χρονική στιγμή. Με τον τρόπο αυτό μπορεί να ξέρει αν τα δεδομένα έχουν υποστεί ανεπιθύμητη αλλοίωση. Αυτή η ιδιότητα χρησιμεύει σε εφαρμογές που αφορούν προστασία από ιούς και διανομή software.

Επίσης οι συναρτήσεις hash βρίσκουν εφαρμογή και σε πρωτόκολλα όπως το SSL (Secure Socket Layer) που χρησιμοποιείται για πιστοποίηση ακεραιότητας δεδομένων [4].

Οι γνωστότεροι αλγόριθμοι (hash functions) είναι ο MD5(Message Digest 5) και ο SHA (Secure Hash Algorithm) που προτάθηκε από το εθνικό ινστιτούτο επιστημών των Η.Π.Α. (NIST) και χρησιμοποιείται από το 1994. Στη συνέχεια αναφερόμαστε σύντομα στον δεύτερο αλγόριθμο hash..

1.3.1.1. SHA (Secure Hash Algorithm)

Ο αλγόριθμος SHA (Secure Hash Algorithm) ορίζεται αναλυτικά στο πρότυπο Secure Hash Standard (SHS, FIPS PUB 180). Μια βελτιστοποίηση του SHA είναι ο SHA-1 ο οποίος δημοσιεύτηκε το 1994 και διόρθωσε κάποιες αδυναμίες που παρουσίαζε ο αρχικός αλγόριθμος.

Ο αλγόριθμος SHA-1 παίρνει ένα μήνυμα, το οποίο πρέπει να είναι σε μέγεθος λιγότερο από 2^{64} bits, και παράγει message digest μήκους 160 bit. Είναι πιο γρήγορος από αλγόριθμους όπως ο Triple-DES και AES αλλά πιο αργός από τον hash αλγόριθμο MD5. Το πλεονέκτημά του είναι ότι διασφαλίζει μεγάλο βαθμό ασφάλειας απέναντι σε επιθέσεις, λόγω του μεγάλου μήκους του message digest που παράγει. Άλλες εκδόσεις του αλγόριθμου αυτού είναι ο SHA-256, ο οποίος παράγει message digest μήκους 256 bits, και ο SHA-512 του οποίου το message digest είναι 512 bits.

1.3.2 Hash Functions Με Κλειδί (MACs)

Οι secure hash αλγόριθμοι, όπως ο SHA-1, παίρνουν ως μόνη είσοδο ένα μη κρυπτογραφημένο μήνυμα (plaintext), χωρίς να χρησιμοποιούν κλειδί. Ως αποτέλεσμα, ο καθένας μπορεί να υπολογίσει την hash value ενός μηνύματος, η οποία είναι πάντοτε η ίδια. Υπάρχουν όμως περιπτώσεις που απαιτείται ένας βαθμός ασφάλειας. Στην περίπτωση αυτή είναι αναγκαία η ύπαρξη ενός κλειδιού το οποίο θα προστατεύει το μήνυμα, και ο υπολογισμός του hash value θα γίνεται μόνο από τον κάτοχο αυτού του κλειδιού. Συνεπώς μία τέτοια συνάρτηση F θα έχει δύο εισόδους , το κλειδί K και το plaintext M, και θα είναι της μορφής $F_K(M)$. Ένας hash αλγόριθμος αυτής της μορφής ονομάζεται Keyed Hash ή Message Authentication Code (MAC).

Υπάρχουν τρεις τύποι MAC αλγόριθμων :

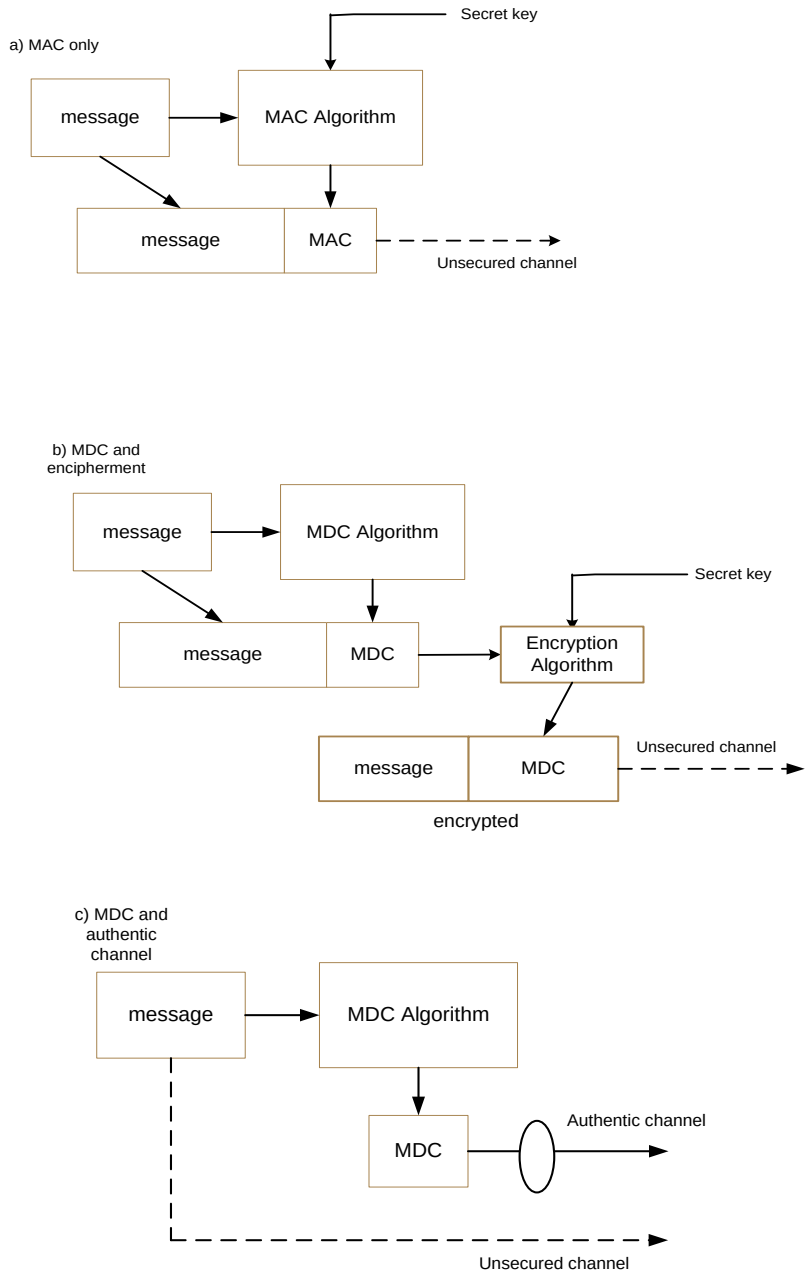
- αυτοί που βασίζονται σε hash αλγόριθμους
- αυτοί που βασίζονται σε stream cipher αλγόριθμους
- τέλος, αυτοί που βασίζονται σε block cipher αλγόριθμους

Οι πιο ευρέως διαδεδομένοι είναι οι hash MACs και ένας από αυτούς είναι ο HMAC (Hash Message Authentication Code).

1.3.2.1 HMAC (Hash Message Authentication Code)

Ο αλγόριθμος HMAC χρησιμοποιεί τον SHA αλγόριθμο, και λειτουργεί αναμειγνύοντας τα bits του κλειδιού με αυτά του μηνύματος προς κρυπτογράφηση, με βάση το hash του SHA. Το κλειδί μπορεί να έχει οποιοδήποτε μήκος, αλλά συνήθως δημιουργούμε κλειδιά ίσου μήκους με το output του SHA αλγόριθμου. Χρησιμοποιείται σε πρωτόκολλα-εφαρμογές όπως SSL(Secure Socket Layer), IPSec(IP Security) και SSH(Secure Shell). Ανάλογα με την έκδοση του SHA, έχουμε τον HMAC-SHA-1, τον HMAC-SHA-256 και τον HMAC-SHA-512.

Τέλος, στο σχήμα 1.6, παρουσιάζονται τρεις τρόποι μετάδοσης δεδομένων με την χρήση hash αλγορίθμων, οι οποίοι διασφαλίζουν ακεραιότητα των δεδομένων (integrity) και πιστοποίηση της προέλευσής τους (authentication).

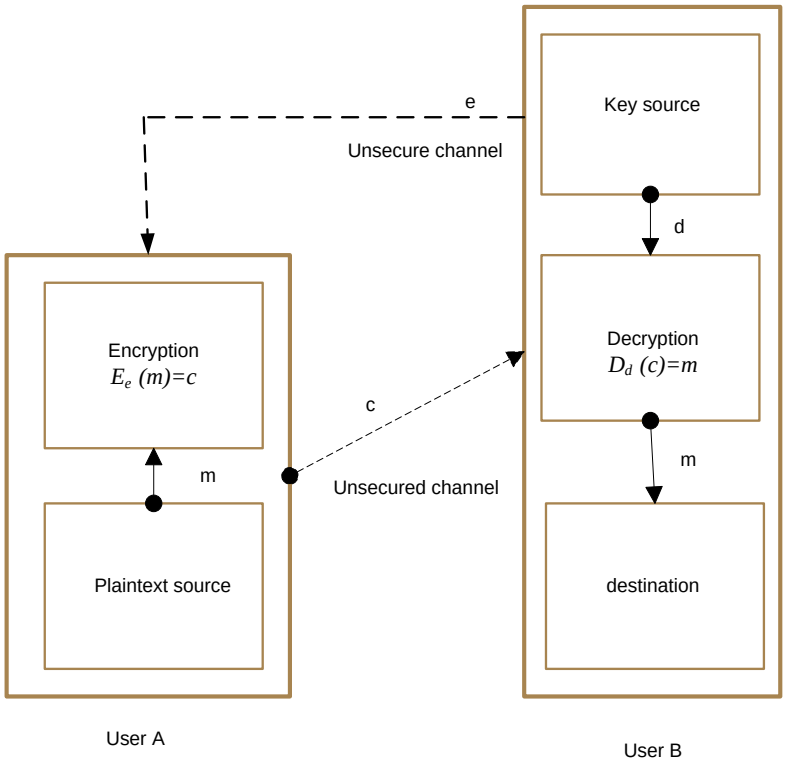


Σχήμα 1.6 Data integrity methods using hash functions (MDC –Unkeyed hashes(MD5 SHA))

1.4 ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ (PUBLIC KEY CRYPTOGRAPHY)

Ας θεωρήσουμε ένα μοντέλο κρυπτογράφησης το οποίο αποτελείται από τις μαθηματικές συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης $\{ E_e : e \in K\}$ και $\{ D_d : d \in K\}$, αντίστοιχα , όπου K είναι ένα σύνολο κλειδιών. Το μοντέλο αυτό ονομάζεται *ασύμμετρου κλειδιού* όταν εξασφαλίζεται η εξής προϋπόθεση: δεδομένου ότι κάποιος γνωρίζει το κλειδί κρυπτογράφησης e είναι υπολογιστικώς αδύνατο να δημιουργήσει το αντίστοιχο κλειδί αποκρυπτογράφησης d. Παρουσιάζεται, λοιπόν, μία θεμελιώδης διαφορά με την συμμετρική κρυπτογραφία, όπου τα κλειδιά e και d είναι τα ίδια.

Στο σχήμα 1.7 διαφαίνεται το διάγραμμα μιας διμερούς επικοινωνίας με ασύμμετρη κρυπτογραφία. Ο Bob αρχικά δημιουργεί το ζεύγος κλειδιών (e,d) και στέλνει στην Alice το κλειδί κρυπτογράφησης e, το οποίο ονομάζεται *δημόσιο κλειδί (public key).* Παράλληλα, κρατά το κλειδί αποκρυπτογράφησης d μυστικό, διασφαλίζοντας με κάθε τρόπο την ασφάλεια αυτού. Το κλεδί αυτό ονομάζεται *ιδιωτικό κλειδί (private key).* Στην συνέχεια η Alice στέλνει ένα κρυπτογραφημένο μήνυμα c (ciphertext) στον Bob, εφαρμόζοντας την συνάρτηση κρυπτογράφησης, με το δημόσιο κλειδί του Bob, σε ένα μήνυμα m $(E_e(m)=c)$. Ο Bob παίρνει το ciphertext c και εφαρμόζει σε αυτό την αντίστροφη συνάρτηση αυτής που χρησιμοποίησε η Alice, που αντιστοιχεί στο ιδιωτικό του κλειδί d. Με τον τρόπο αυτό δημιουργεί το αρχικό κείμενο m που του στάλθηκε από την Alice $(m=D_d(c))$. Εφόσον το κλειδί κρυπτογράφησης e δεν είναι αναγκαίο να διατηρείται μυστικό, μπορεί να διανέμεται δημοσίως,ώστε οποιοσδήποτε να μπορεί να στέλνει κρυπτογραφημένα μηνύματα στον Bob με αυτό. Τα μηνύματα αυτά, βέβαια, μπορεί να αποκρυπτογραφήσει επιτυχώς μόνο ο κάτοχος του ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί, δηλαδή ο Bob. Σύμφωνα με τα παραπάνω εξηγείται γιατί η ασύμμετρη κρυπτογραφία ονομάζεται και *κρυπτογραφία δημοσίου κλειδιού (public key cryptography).*



Σχήμα1.7 Κρυπτογραφία με τεχνική δημοσίου κλειδιού

Η δημιουργία, μετάδοση και αποθήκευση των κλειδιών ονομάζεται *διαχείριση κλειδιών (key management).* Σε ένα σύστημα κρυπτογραφίας δημόσιου κλειδιού, επειδή είναι αναγκαία η διατήρηση της μυστικότητας των ιδιωτικών κλειδιών, παρουσιάζονται συχνά προβλήματα στην ασφαλή διαχείρηση αυτών, ιδιαίτερα σε δίκτυα με μεγάλο αριθμό χρηστών.

Μια ακόμη χρησιμότητα της κρυπτογραφίας δημοσίου κλειδιού είναι οι ψηφιακές υπογραφές, οι οποίες βοηθούν στην διαδικασία ταυτοποίησηςauthentication. Δημιουργούνται με το ιδιωτικό κλειδί και μήνυμα προς αποστολή (plaintext) μετά από ένα μαθηματικό υπολογισμό. Στην συνέχεια, ο αποστολέας στέλνει την ψηφιακή υπογραφή συννημένη με το αρχικό μήνυμα. Ο δέκτης το μόνο που έχει να κάνει είναι να χρησιμοποιήσει το δημόσιο κλειδί του αποστολέα ώστε να επιβεβαιώσει ότι η ψηφιακή υπογραφή αντιστοιχεί στο μήνυμα το οποίο έλαβε και ταυτοχρόνα ότι στάλθηκε από τον συγκεκριμένο αποστολέα. Σε περίπτωση που η ψηφιακή υπογραφή δεν

αντιστοιχεί στο plaintext τότε αυτή είναι ψευδής ή τα δεδομένα του μηνύματος έχουν υποστεί αλλοίωση.

Ο κύριος στόχος της κρυπτογραφίας δημόσιου κλεδιού είναι η μυστικότητα της πληροφορίας (Confidentiality). Είναι εμφανές όμως ότι η τεχνική της κρυπτογράφησης ενός κειμένου με το δημόσιο κλειδί δεν μπορεί από μόνη της να διασφαλίσει βασικά αιτήματα όπως την ακεραιότητα της πληροφορίας (data integrity) και την πιστοποίηση της προέλευσής της (data origin authentication). Για την επίτευξη αυτών των στόχων είναι αναγκαία η υιοθέτηση τεχνικών, όπως της ψηφιακής υπογραφής, που αναφέρθηκε ανωτέρω, και η χρήση των αλγορίθμων MAC (Message Authentication Code).

Σε γενικές γραμμές οι αλγόριθμοι ασύμμετρου κλειδιού είναι πιο αργοί από τους αλγόριθμους συμμετρικού κλειδιού, όπως ο DES. Για τον λόγο αυτό χρησιμοποιούνται κυρίως για ασφαλή μετάδοση συμμετρικών κλειδιών και για κρυπτογράφηση δεδομένων μικρού μεγέθους (PINs και αριθμούς πιστωτικών καρτών). Τέλος, λόγω των πλεονεκτημάτων που παρουσιάζουν, χρησιμοποιούνται ευρέως και σε πρωτόκολλα όπως TLS(Transport Layer Security), IPSec(IP Security) και SSH(Secure Shell).

1.4.1 Αλγόριθμοι Δημοσίου Κλειδιού (Public Key Algorithms)

Οι κυριότεροι αλγόριθμοι που χρησιμοποιούνται στην κρυπτογραφία δημοσίου κλειδιού είναι ο Diffie-Hellman, ο RSA και ο El-Gamal.

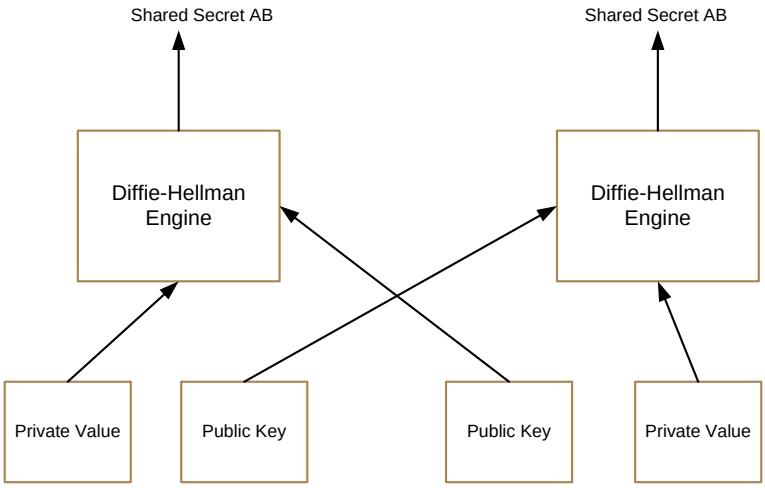
1.4.1.1 Αλγόριθμος Diffie-Hellman

Οι τεχνολογίες κρυπτογράφησης δημοσίου κλειδιού βασίζονται στον *αλγόριθμο συμφωνίας κλειδιού (key agreement algorithm)* που εισήγαγαν την δεκαετία του ’70 οι Diffie-Hellman.

Είναι γνωστό ότι αλγόριθμοι όπως ο AES και Triple-DES έχουν ως προυπόθεση ότι, για να επιτευχθεί ασφαλής επικοινωνία μεταξύ δύο πλευρών *A* και *B*, το κλειδί *K* το οποίο θα χρησιμοποιηθεί είναι γνωστό. Το ερώτημα το οποίο προκύπτει είναι πως θα μοιραστούν οι δύο πλευρές το κλειδί αυτό, στην περίπτωση που δεν έχουν συμφωνήσει ακόμη και η επικοινωνία τους γίνεται

πάνω από μία μη ασφαλή γραμμή (πχ. τηλεφωνική γραμμή), η οποία παρακολουθείται από έναν τρίτο *C*. Η λύση στο πρόβλημα αυτό δόθηκε από τους Diffie και Hellman, οι οποίοι εισήγαγαν έναν αλγόριθμο που επιτρέπει στους *A* και *B* να συμφωνήσουν σε ένα μυστικό κλειδί, το οποίο ο κακόβουλος *C* δεν θα μπορέσει να εντοπίσει. Η επιτυχία του αλγόριθμου στηρίζεται στις εξής δύο διαπιστώσεις :

- δοθέντων τεσσάρων οποιωνδήποτε ακεραίων αριθμών a, b, x and p ισχύει : $(x^a)^b \mod p = (x^b)^a \mod p$
- δοθέντος ενός μεγάλου πρώτου αριθμού *p (p>1024)* και ενός άλλου πρώτου αριθμού *x*, το πρόβλημα του Διακριτού Λογάριθμου (Discrete Logarithm) είναι αδύνατο να λυθεί (δηλαδή είναι αδύνατο, να βρεθεί ο αριθμός *a*, ο οποίος ικανοποιεί την σχέση $W = x^a \mod p$, δοθέντων *W*,*x* και *p*)



Εικόνα 1.8 Key Agreement between two parties

Στην συνέχεια θα αναλύσουμε σε βήματα την συμφωνία κλειδιού μεταξύ του *A* και *B* , λαμβάνοντας υπ'όψη τις παραπάνω διαπιστώσεις (εικόνα 1.8) :

1. στους *A* και *B* είναι γνωστοί οι παράμετροι του λογαρίθμου : ένας μεγάλος πρώτος αριθμός *p (p>1024)* και ένας πρώτος αριθμός *x*

2. ο *A* δημιουργεί έναν αριθμό *a* και στέλνει στον *B* το αποτέλεσμα της σχέσης x^a *mod p* (το οποίο είναι το δημόσιο κλειδί του *A*).

3. ο *B* δημιουργεί έναν αριθμό *b* και στέλνει στον *A* το αποτέλεσμα της σχέσης x^b *mod p* (το οποίο είναι το δημόσιο κλειδί του *B*).

4. Στη συνέχεια και οι δύο δημιουργούν το κοινό μυστικό κλειδί $K = x^{ab}$ *mod p* (Πιο συγκεκριμένα ο *A* ξέρει το *a* και το x^b*mod p* και υπολογίζει το κλειδί ως $K = (x^b)^a$ *mod p*.Αντίστοιχα δημιουργει το κλειδί και ο *B*).

5. Ο κακόβουλος *C* γνωρίζει τα x^b *mod p* και x^a *mod p* αλλά δεν μπορεί να υπολογίσει το κλειδί $K = x^{ab}$ *mod p.*

Εφόσον οι πλευρές έχουν συμφωνήσει σε ένα κοινό μυστικό κλειδί, μπορούν να επιλέξουν με ποιον αλγόριθμο θα γίνει η επικοινωνία μεταξύ τους, όπως ο AES ή ο Triple-DES.

Ο αλγόριθμος Diffie-Hellman, που μόλις περιγράφηκε, αποτελεί την βάση για κάθε κρυπτογραφημένη επικοινωνία που γίνεται μέσω του διαδικτύου σήμερα καθιστώντας τον θεμελιώδη για την επιστήμη της Κρυπτογραφίας.

1.4.1.2 Αλγόριθμος El-Gamal

Ο αλγόριθμος El-Gamal παρουσιάζει πολλές ομοιότητες με αυτόν των Diffie-Hellman. Χρησιμοποιείται ευρέως, καθώς είναι ο προτιμούμενος αλγόριθμος για την κρυπτογράφηση με κλειδιά στο πρωτόκολλο Open PGP (RFC 2440). Στην συνέχεια θα αναλύσουμε σε βήματα τον αλγόριθμο για την επικοινωνία μεταξύ του *A* και του *B*:

1. στους *A* και *B* είναι γνωστοί οι παράμετροι του λογαρίθμου : ένας μεγάλος πρώτος αριθμός *p (p>1024)* και ένας πρώτος αριθμός *x*

2. ο *A* δημιουργεί ένα τυχαίο αριθμό *α,* ο οποίος είναι το ιδιωτικό του κλειδί.

3. ο *A* υπολογίζει την τιμή x^a *mod p,* η οποία είναι το δημόσιο κλειδί του και το διανέμει στο δίκτυο.

4.ο *B* θέλει να στείλει ένα κρυπτογραφημένο μήνυμα στον *A*.

Αρχικά δημιουργεί ένα τυχαίο αριθμό *b*.
Υπολογίζει το κοινό μυστικό κλειδί $K = (x^a)^b \ mod \ p$,
κρυπτογραφεί το μήνυμα με το κλειδί *K* με την βοήθεια ενός αλγόριθμου (πχ. τον AES) . Στην συνέχεια στέλνει το κρυπτογραφημένο μήνυμα μαζί με το αποτέλεσμα της σχέσης $x^b \ mod \ p$.

5. ο Α λαμβάνει το αρχείο, διαβάζει το αποτέλεσμα της σχέσης $x^b \ mod \ p$ και υπολογίζει το κοινό μυστικό κλειδί $K = (x^a)^b \ mod \ p$ (αφού χρησιμοποιήσει το ιδιωτικό του κλειδί α).
6. Τέλος ο Α αποκρυπτογραφεί το μήνυμα.

1.4.1.3 Αλγόριθμος RSA (Rivest – Shamir - Adleman)

Ο αλγόριθμος RSA δόθηκε στη δημοσιότητα το 1977 από τους Rivest, Shamir και Adleman. Είναι ο πιο διαδεδομένος αλγόριθμος που χρησιμοποιείται σε κρυπτογραφικές τεχνικές, οι οποίες έχουν εφαρμογή σε μία μεγάλη ποικιλία από προϊόντα. Χρησιμοποιείται ευρέως σε εφαρμογές λογισμικού και σε λειτουργικά συστήματα γνωστών εταιρειών όπως της Microsoft, της Sun, της Apple και της Novell. Όσο αφορά το hardware, συναντούμε τον RSA σε «έξυπνες» κάρτες καθώς και σε κάρτες δικτύου Ethernet. Πολλά πρωτόκολλα που παρέχουν ασφαλή επικοινωνία στο διαδίκτυο έχουν τον αλγόριθμο RSA σαν βάση της αρχιτεκτονικής τους (τα κυριότερα είναι το SSL (Secure Socket Layer), το S/MIME (Secure/Multipurpose Internet Mail Extensions), το S/WAN, το IPSec (IP Security), το TLS (Transport Layer Security)).

Το χαρακτηριστικό, όμως, που επιβεβαιώνει την σημασία αυτού του αλγορίθμου και διασφαλίζει την διαρκή εξέλιξή του είναι το γεγονός ότι αποτελεί αντικείμενο ενδελεχούς μελέτης από διεθνείς οργανισμούς και επιχειρήσεις, καθώς και από εργαστήρια και πανεπιστήμια σε όλο τον κόσμο.

1.4.1.3.1 Λειτουργία του RSA και Χρησιμότητά του στην Κρυπτογραφία

Ας θεωρήσουμε ένα μοντέλο κρυπτογράφησης το οποίο αποτελείται από τις μαθηματικές συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης $\{ E_e : e \in K\}$ και $\{ D_d : d \in K\}$, αντίστοιχα , όπου K είναι ένα σύνολο κλειδιών. Η λειτουργία του αλγόριθμου στηρίζεται συο γεγονός ότι, για δεδομένο ζεύγος συναρτήσεων (E_e , D_d) και για συγκεκριμένο κρυπτογραφημένο μήνυμα c (ciphertext), είναι υπολογιστικώς αδύνατο να δημιουργήσουμε το αρχικό μήνυμα m (plaintext) τέτοιο ώστε $E_e(m)=c$. Είναι λοιπόν αδύνατο, γνωρίζοντας το κλειδί κρυπτογράφησης e, να δημιουργήσουμε το κλειδί αποκρυπτογράφησης d.

Η μαθηματική «καρδιά» του αλγορίθμου είναι σχετικά απλή στην κατανόηση. Αρχικά δημιουργούμε δύο μεγάλους πρώτους αριθμούς p και q, και υπολογίζουμε τις σχέσεις :

$n=p*q$, όπου το n ονομάζεται *modulus* και

$e*d=1 \ mod \ (p-1) \ (q-1)$, όπου το e ονομάζεται *δημόσιος εκθέτης* (public exponent) και το d *ιδιωτικός εκθέτης* (private exponent).

Τότε, δεδομένου ενός μηνύματος m, οι διεργασίες της κρυπτογράφησης και αποκρυπτογράφησης έχουν, αντίστοιχα, τις εξής μορφές :

$c = m^e \ mod \ n$

$m = c^d \ mod \ n$, όπου c είναι το κρυπτογραφημένο μύνημα (ciphertext)

Το δημόσιο κλειδί είναι το ζεύγος (n, e) και το ιδιωτικό κλειδί το ζεύγος (n, d). Μετά την δημιουργία τους, οι παράγοντες p και q θα ήταν καλό είτε να κρατώνται μυστικοί μαζί με το ιδιωτικό κλειδί, είτε να καταστρέφονται.

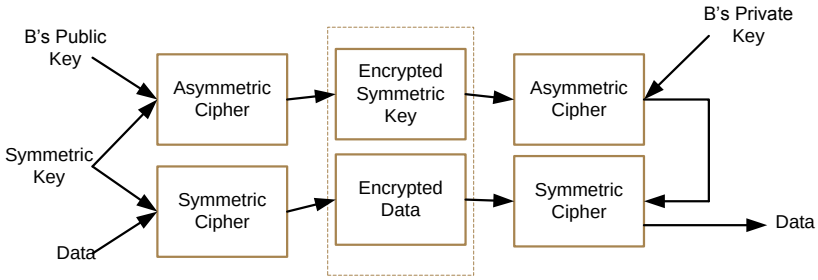
Η λειτουργικότητα του αλγόριθμου RSA στηρίζεται στο γεγονός ότι είναι πολύ δύσκολο να δημιουργήσει κάποιος πολύ μεγάλους αριθμούς. Αυτό το χαρακτηριστικό εγγυάται σε μεγάλο βαθμό την ασφάλεια του αλγορίθμου, καθώς είναι πάρα πολύ δύσκολο να δημιουργήσει κάποιος τον ιδιωτικό εκθέτη d , γνωρίζοντας το ζεύγος του δημοσίου κλειδιού (n, e).

Ο αλγόριθμος RSA χρησιμοποιείται σε εφαρμογές που εξασφαλίζουν μυστικότητα των δεδομένων (data privacy) και πιστοποιούν την προέλευσή τους (data authentication).

1.4.1.3.1.1. RSA και Μυστικότητα (Privacy)

Ο RSA, για να εξασφαλίσει την μυστικότητα των δεδομένων, συνδιάζεται με αλγόριθμους συμμετρικού κλειδιού, όπως ο DES, και δημιουργεί έναν «ψηφιακό φάκελο».

Ας υποθέσουμε μία διμερή επικοινωνία μεταξύ των πλευρών Α και Β, όπου ο Α θέλει να στείλει ένα κρυπτογραφημένο μήνυμα στον Β.(εικόνα 1.9).



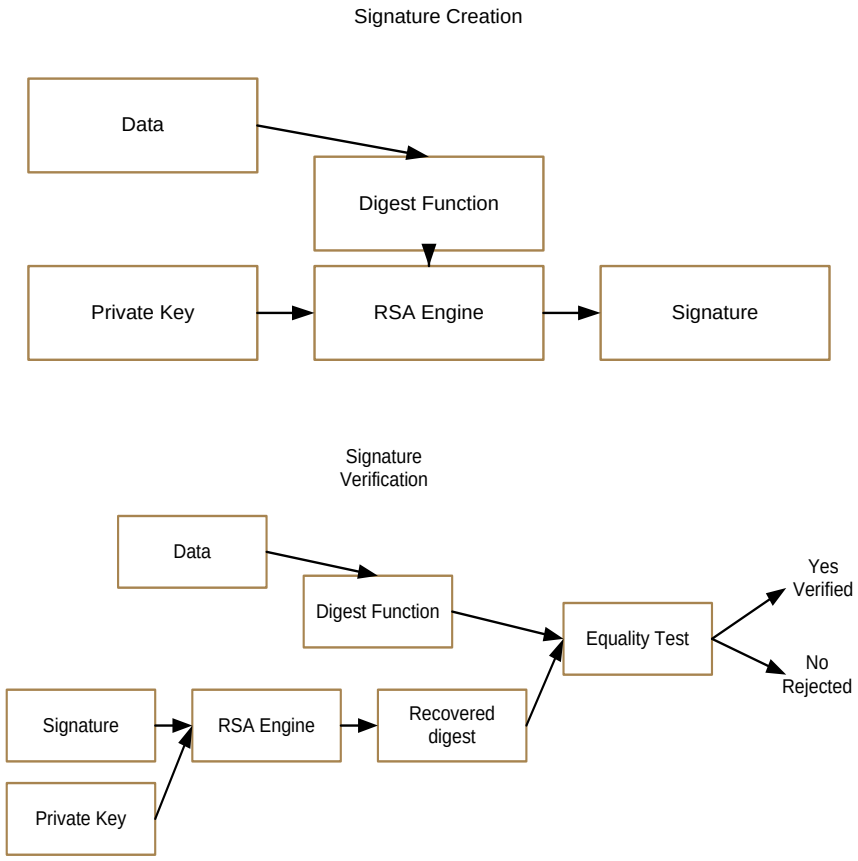
Εικόνα 1.9 Encrypted data using key Exchange

Αρχικά ο Α κρυπτογραφεί το μήνυμα με τον αλγόριθμο DES, χρησιμοποιώντας ένα τυχαίο DES κλειδί. Στην συνέχεια κρυπτογραφεί το DES κλειδί με το δημόσιο κλειδί του Β, και το στέλνει στον Β μαζί με το κρυπτογραφημένο κείμενο. Με τον τρόπο αυτό δημιουργείται και στέλνεται στον Β ένας ψηφιακός RSA φάκελος. Μόλις ληφθεί ο ψηφιακός αυτός φάκελος, ο Β αποκρυπτογραφεί το DES κλειδί με το ιδιωτικό του κλειδί, και στην συνέχεια το χρησιμοποιεί για να αποκρυπτογραφήσει το μήνυμα. Παρατηρούμε συνεπώς ότι η τεχνική αυτή συνδυάζει την πολύ υψηλή ταχύτητα του αλγορίθμου DES και το χαρακτηριστικό της διαχείρησης των κλειδιών που προσφέρει ο αλγόριθμος RSA.

1.4.1.3.1.2. RSA και Authentication

Τα κρυπτοσυστήματα δημοσίου κλειδιού με την χρήση του αλγορίθμου RSA βοηθούν σημαντικά στον παράγοντα authentication (πιστοποίηση, δηλαδή της προέλευσης των δεδομένων και της ταυτότητας του αποστολέα). Αυτό είναι εφικτό λόγω του γεγονότος ότι σε κάθε μία οντότητα αντιστοιχεί ένα μυστικό, ιδιωτικό κλειδί, στο οποίο δεν έχει πρόσβαση κανένας παρά μόνο ο κάτοχός του.

Στην επόμενη εικόνα 1.10, παρουσιάζεται η επικοινωνία δύο πλευρών, όπου εξετάζεται ο παράγοντας authentication με την χρήση ψηφιακής υπογραφής.



Σχήμα 1.10 Τεχνικές ψηφιακής υπογραφής RSA

Υποθέτουμε ότι ο Α θέλει να στείλει ένα υπογεγραμμένο μήνυμα στον Β. Αρχικά ο Α εφαρμόζει μία hash συνάρτηση στο μήνυμα που θέλει να στείλει,

δημιουργώντας μία «περίληψη» του μηνύματος, η οποία ονομάζεται *message digest*. Το message digest είναι μοναδικό για κάθε μήνυμα και αποτελεί το «ψηφιακό αποτύπωμά» του. Στην συνέχεια κρυπτογραφεί το message digest με το ιδιωτικό του κλειδί RSA, και δημιουργεί την ψηφιακή υπογραφή του μηνύματος, την οποία στέλνει στον Β μαζί με το αρχικό μήνυμα. Όταν ο Β παραλάβει τα δεδομένα, αποκρυπτογραφεί πρώτα την υπογραφή με το δημόσιο κλειδί του Α για να πάρει το message digest του μηνύματος. Αυτό που έχει να κάνει στην συνέχεια είναι να εφαρμόσει την ίδια hash function στο αρχικό μήνυμα και να εξετάσει την ομοιότητα των δύο message digest που έχουν προκύψει. Αν είναι απολύτως όμοια μεταξύ τους, τότε έχει επικυρώσει την ψηφιακή υπογραφή και μπορεί να είναι απολύτως σίγουρος ότι το μήνυμα έχει αποσταλεί από τον Α. Στην αντίθετη περίπτωση πρέπει να απορρίψει το μήνυμα διότι αποδεικνύεται ότι είτε ο αποστολέας δεν είναι ο Α, είτε τα δεδομένα έχουν υποστεί αλλοίωση μετά την αποστολή τους.

Η περίπτωση που περιγράφηκε πιο πάνω δεν εξασφαλίζει την μυστικότητα του μηνύματος που αποστέλει ο Α. Στην περίπτωση που αυτός ήθελε να προστατεύσει το μήνυμα από την ανάγνωσή τους από τρίτους, θα έπρεπε να το κρυπτογραφήσει με το ιδιωτικό κλειδί του Β. Τότε το μήνυμα δεν θα είναι εφικτό να διαβάσει κάποιος κακόβουλος παρά μόνο ο Β, αφού βέβαια το αποκρυπτογραφήσει πρώτα με το ιδιωτικό του κλειδί.

Ένα σημείο τα οποίο θα πρέπει να προσεχθεί είναι ο δημόσιος εκθέτης *e*. Σε πρακτικές εφαρμογές όπως αυτές που περιγράφηκαν, είναι πιο αποτελεσματικό η τιμή του να είναι αρκετά μικρή. Αυτό βοηθά στο να γίνεται η επικύρωση μιας υπογραφής πολύ πιο γρήγορα από την δημιουργία της, εφόσον η υπογραφή ενός μηνύματος γίνεται μία φορά μόνο ενώ η επικύρωσή του πάρα πολλές φορές.

Για να έχουμε μία ακόμη πιο ολοκληρωμένη εικόνα για τον παράγοντα authentication σε σχέση με τον αλγόριθμο RSA, και κατά συνέπεια με τις ψηφιακές υπογραφές, θα πρέπει να επισημανθεί και ο ρόλος του ψηφιακού πιστοποιητικού. Τα ψηφιακά πιστοποιητικά είναι υπογεγραμμένα αρχεία, τα οποία συνδέουν ένα δημόσιο κλειδί με μία οντότητα. Η χρησιμότητά του είναι σημαντική καθώς αποτρέπουν κάποιον κακόβουλο από το να υιοθετήσει παράνομα την ταυτότητα κάποιου άλλου. Η παρουσία, συνεπώς, του πιστοποιητικού σε μία επικοινωνία βοηθά τους συμμετέχοντες σε αυτή, στο να

ελέγχουν την εγκυρότητα των δημόσιων κλειδιών που χρησιμοποιούν. Τα ψηφιακά πιστοποιητικά θα αναλυθούν εκτενέστερα σε επόμενο κεφάλαιο.

1.4.1.3.2 Ταχύτητα RSA αλγόριθμου

Όπως έχει αναφερθεί, η λειτουργία του αλγόριθμου RSA στηρίζεται σε εκθετικούς υπολογισμούς. Σε πρακτικές εφαρμογές είναι προτιμότερο να επιλέγεται μικρό μέγεθος δημόσιου εκθέτη e , ώστε να γίνεται πολύ πιο γρήγορα η κρυπτογράφηση των δεδομένων από την αποκρυπτογράφησή τους, και επίσης η επικύρωση μιας υπογραφής από την δημιουργία της. Πιο συγκεκριμένα, για αλγόριθμους εκθετικής συμπεριφοράς όπως ο RSA, η διαδικασία της κρυπτογράφησης με το δημόσιο κλειδί είναι $O(k^2)$ τάξης, αυτή της αποκρυπτογράφησης με το ιδιωτικό κλειδί είναι $O(k^3)$ τάξης και αυτή της δημιουργίας των κλειδιών είναι $O(k^4)$ τάξης, όπου k το πλήθος των bits του modulus.

Η απόδοση και η ταχύτητα εφαρμογών software και hardware που υλοποιούν τον αλγόριθμο RSA αυξάνεται συνεχώς. Σε σύγκριση με συμμετρικούς μπλοκ αλγόριθμους, όπως τον DES, ο RSA υπολοίπεται σε ταχύτητα. Σε software εφαρμογές έχει διαπιστωθεί ότι ο DES είναι μέχρι και 100 φορές πιο γρήγορος από τον RSA, ενώ σε hardware το χάσμα αυτό μεγαλώνει θεαματικά (ανάλογα με την υλοποίηση, ο DES είναι μέχρι και 10.000 φορές πιο γρήγορος).

1.4.1.3.3. Μέγεθος κλειδιού του RSA

Ο παράγοντας ο οποίος καθορίζει το μέγεθος του κλειδιού RSA είναι το μέγεθος του modulus n. Η ιδανική περίπτωση είναι το μέγεθος των δύο συντελεστών που συνθέτουν το modulus, δηλαδή οι πρώτοι αριθμοί p και q, να είναι το ίδιο. Αν, δηλαδή, κάποιος θελήσει να έχει modulus μεγέθους 768 bits, τότε οι πρώτοι αριθμοί θα πρέπει να έχουν μέγεθος ακριβώς 384 bits. Στην αντίθετη περίπτωση, αν έχουν μεγάλη διαφορά στο μέγεθός τους 100-200 bits, θα είναι πολύ πιο εύκολο για κάποιον τρίτο να δημιουργήσει τον μικρότερο από αυτούς και να «σπάσει» τον αλγόριθμο.

Όταν, βέβαια, θέλουμε να εφαρμόσουμε τον RSA σε ένα ολοκληρωμένο κρυπτοσύστημα, τότε οι προδιαγραφές του θα είναι διαφορετικές και θα εξαρτώνται από τις απαιτήσεις ασφάλειάς του. Πρέπει να γνωρίζουμε ότι η αύξηση του μεγέθους του modulus μπορεί να αυξάνει το επίπεδο της ασφάλειας αλλά ταυτόχρονα σημαίνει και αναπόφευκτη μείωση της απόδοσης του αλγορίθμου. Οι κυριότεροι παράγοντες που πρέπει να ληφθούν υπ'όψη για τον καθορισμό του μεγέθους του κλειδιού είναι το μέγεθος των δεδομένων που πρέπει να προστατευτούν, το χρονικό διάστημα της προστασίας τους, καθώς και η αξιολόγηση των κινδύνων που μπορούν να διαβάλλουν το κρυπτοσύστημα.

Βέβαια, οι τεχνικές που έχουν αναπτυχθεί για το «σπάσιμο» των αλγόριθμων συνεχώς εξελίσσονται και παράλληλα με την ανάπτυξή τους είναι αναγκαίο να ανανεώνονται και οι προδιαγραφές ασφαλείας που πρέπει να πληρούνται από τα συστήματα κρυπτογραφίας. Όσο αφορά τον αλγόριθμο RSA με κλειδί 512 bits, έχει αποδειχτεί, μετά από μελέτη το 1999, ότι μπορεί να «σπάσει» μετά από οχτάμηνη προσπάθεια και επιχορήγηση λιγότερη του ενός εκατομμυρίου δολλαρίων[5]. Συνεπώς είναι επόμενο ότι κλειδιά των 512 bit δεν πληρούν τις σύγχρονες προδιαγραφές ασφαλείας, παρά προσφέρονται μόνο για χρήση σε βραχυχρόνιες διαδικασίες.

Τα RSA Laboratories προτείνουν τα ακόλουθα μεγέθη κλειδιών για τις διάφορες χρήσεις :

- Κλειδιά με μέγεθος 768 bits, για προσωπική χρήση (personal use)
- Κλειδιά με μέγεθος 1024 bits, για χρήση τους από ομάδες, εταιρίες και επιχειρήσεις (corporate use)
- Κλειδιά με μέγεθος 2048 bits, όταν η ασφάλεια παρέχουν πρέπει να είναι υψηλότατης βαθμίδας, όπως το βασικό ζεύγος κλειδιών (root key-pair) ενός CA (Certificate Authority)

Τα RSA Laboratories προτείνουν επίσης, σε τακτά χρονικά διαστήματα, νέα μήκη κλειδιών, ώστε να προσαρμόζεται ο κάθενας στις συνεχώς αυστηρότερες απαιτήσεις ασφάλειας που προκύπτουν.

Ένα σημείο το οποίο πρέπει να προσεχθεί είναι ότι το κάθε κλειδί έχει ένα προκαθορισμένο χρονικό διάστημα μέσα στο οποίο είναι έγκυρο, συνήθως δύο χρόνια. Όταν το χρονικό αυτό όριο λήξει, τότε ο κάτοχος πρέπει να αντικαταστήσει το υπάρχον κλειδί με ένα νέο το οποίο θα ήταν καλό να

συμβαδίζει με τις νεότερες κρυπτογραφικές τεχνικές και το νέο μέγεθός του να πληρεί τις προδιαγραφές ασφαλείας. Αυτό το χαρακτηριστικό είναι αρκετά σημαντικό καθώς δίνει την δυνατότητα σε κάποιον να αλλάζει κλειδιά σε τακτά χρονικά διαστήματα και να διατηρεί ένα υψηλό επίπεδο ασφάλειας στο σύστημά του.

Τέλος πρέπει να σημειωθεί ότι τα μεγέθη κλειδιών του RSA (αλλά και των άλλων ασύμμετρων αλγορίθμων) είναι πολύ μεγαλύτερα από αυτά των συμμετρικών μπλοκ αλγόριθμων, όπως του DES.

1.5 ΣΥΓΚΡΙΣΗ ΑΛΓΟΡΙΘΜΩΝ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ-ΣΥΜΜΕΤΡΙΚΟΥ ΚΛΕΙΔΙΟΥ

Τα μοντέλα κρυπτογραφίας που υλοποιούν ασύμμετρους αλγόριθμους και αλγόριθμους δημόσιου κλειδιού παρουσιάζουν πολλά πλεονεκτήματα αλλά και αρκετά μειονεκτήματα, μερικά από τα οποία είναι κοινά. Στη συνέχεια θα συνοψίσουμε τα βασικότερα από αυτά, σύμφωνα με αυτά που έχουν ειπωθεί μέχρι το σημείο αυτό.

1. Πλεονεκτήματα Ασύμμετρης Κρυπτογραφίας

   - Οι ασύμμετροι αλγόριθμοι έχουν σχεδιαστεί ώστε να έχουν υψηλές τιμές διαμεταγωγής δεδομένων. Hardware-based εφαρμογές επιτυγχάνουν την κρυπτογράφηση εκαντοντάδων megabytes το δευτερόλεπτο, ενώ εφαρμογές λογισμικού καταφέρνουν την κρυπτογράφηση αρκετών megabytes το δευτερόλεπτο.
   - Τα κλειδιά των συμμετρικών αλγόριθμων είναι αρκετά μικρά
   - Οι αλγόριθμοι αυτοί αποτελούν την πρώτη ύλη για την δημιουργία πολύ χρήσιμων εφαρμογών, όπως των συναρτήσεων hash και τεχνικών που χρησιμοποιούν ψηφιακές υπογραφές.

2. Μειονεκτήματα Ασύμμετρης Κρυπτογραφίας

   - Σε μία διμερή επικοινωνία είναι αναγκαίο το κλειδί να παραμένει μυστικό και από τις δύο πλευρές.
   - Σε ένα ευρύτερο δίκτυο τα κλειδια που πρέπει να διαχειρίζονται οι χρήστες είναι πάρα πολλά. Καθίσταται αναγκαία λοιπόν η ύπαρξη μιας οντότητας την οποία θα πρέπει όλοι να την εμπιστεύονται «τυφλά» και ονομάζεται trusted third party (TTP). Η οντότητα αυτή θα έχει πλήρη πρόσβαση στα μυστικά κλειδιά των χρηστών και θα καθιστά δυνατή την ασφαλή επικοινωνία τους.
   - Σε μία διμερή επικοινωνία πρέπει τα κλειδιά να ανανεώνονται σε τακτά χρονικά διαστήματα. Ιδανικό είναι να αλλάζουν πριν από κάθε σύνοδο επικοινωνίας.
   - Οι μηχανισμοί ψηφιακής υπογραφής που υλοποιούν αλγόριθμους συμμετρικής κρυπτογραφίας, προϋποθέτουν είτε πολύ μεγάλα μεγέθη κλειδιών για την επικύρωση της υπογραφής, είτε την ύπαρξη ενός trusted third party.

3. Πλεονεκτήματα Κρυπτογραφίας Δημοσίου Κλειδιού

   - Μόνο το ιδιωτικό κλειδί πρέπει να διατηρείται μυστικό
   - Το ζεύγος δημοσίου-ιδιωτικού κλειδιού μπορεί να παραμένει το ίδιο για μεγάλα χρονικά διαστήματα, και να ανανεώνεται ανάλογα με τους κινδύνους που μπορούν να προκύψουν από την χρήση του
   - Οι αλγόριθμοι αυτοί μπορούν να χρησιμοποιηθούν για την υλοποίηση πολύ αποδοτικών μοντέλων ψηφιακής υπογραφής. Τα μεγέθη κλειδιών που απαιτούνται για τους μηχανισμούς επικύρωσης της υπογραφής είναι πολύ μικρότερα σε σύγκριση με αυτά των συμμετρικών αλγόριθμων
   - Σε μεγάλα δίκτυα, ο αριθμός ζευγών κλειδιών που απαιτούνται είναι σαφώς μικρότερος από τον αριθμό μυστικών κλεδιών, σε

περίπτωση υλοποίησης του δικτύου με συμμετρική κρυπτογραφία

- Για την διαχείρηση των κλειδιών σε ένα μεγάλο δίκτυο αρκεί η ύπαρξη ενός trusted third party, το οποίο το εμπιστεύονται οι χρήστες αλλά δεν έχει πρόσβαση στα ζεύγη των κλειδιών τους.

4. Μειονεκτήματα Κρυπτογραφίας Δημοσίου Κλειδιού
   - Οι αλγόριθμοι αυτοί άρχισαν να αναπτύσσονται πολύ πρόσφατα σε σχέση με τους συμμετρικούς, μόλις στα μέσα της δεκαετίας του ‘70.
   - Οι ρυθμοί throughput δεδομένων είναι πολύ πιο μικροί από αυτούς των τεχνικών που υλοποιούν συμμετρικούς αλγόριθμους
   - Κανένα μοντέλο κρυπτογράφησης δημοσίου κλειδιού δεν έχει αποδειχτεί ότι είναι απολύτως ασφαλές
   - Τα μεγέθη των κλειδιών που απαιτούνται είναι πολύ μεγαλύτερα από αυτά των συμμετρικών αλγορίθμων.

Τα σύγχρονα συστήματα κρυπτογραφίας επωφελούνται από τα πλεονεκτήματα που παρουσιάζουν και οι δύο τύποι αλγόριθμων και προσπαθούν να τους συνδιάσουν προσδωκώντας μέγιστη απόδοση και ασφάλεια. Συνοψίζοντας μπορούμε να πούμε ότι οι αλγόριθμοι δημόσιου κλειδιού προσφέρουν το χαρακτηριστικό του key management και χρησιμοποιούνται σε μηχανισμούς ψηφιακής υπογραφής, διασφαλίζοντας το αίτημα non-repudiation. Από την άλλη πλευρά, οι συμμετρικοί αλγόριθμοι είναι πολύ χρήσιμοι και αποδοτικοί στην κρυπτογράφηση δεδομένων και στην διασφάλιση της ακεραιότητάς τους (data integrity).

1.6 ΕΙΔΗ ΕΠΙΘΕΣΕΩΝ ΣΕ ΑΛΓΟΡΙΘΜΟΥΣ

Η *Κρυπτανάλυση* (Cryptanalysis) είναι η επιστήμη σύμφωνα με την οποία είναι εφικτό το «σπάσιμο» του κώδικα, η αποκρυπτογράφηση των κρυπτογραφημένων δεδομένων και γενικότερα η παραβίαση των κρυπτογραφικών τεχνικών. Η επιστήμη αυτή βασίζεται στις αδυναμίες που παρουσιάζουν οι διάφορες τεχνικές τις κρυπτογραφίας, και η εφαρμογή της πάνω σε ένα κρυπτοσύστημα ονομάζεται *επίθεση (*attack*).*

Μπορούμε να διακρίνουμε τις επιθέσεις σε δύο κατηγορίες:

- Η *παθητική επίθεση (passive attack)*, στην οποία ένας τρίτος απλώς καταγράφει την ροή δεδομένων μέσα από ένα κανάλι επικοινωνίας. Η επίθεση αυτού του τύπου προσβάλλει μόνο την μυστικότητα της πληροφορίας (Confidentiality).
- Η ενεργητική επίθεση (active attack), όπου ένας τρίτος προσπαθεί να διαγράψει, να προσθέσει δεδομένα και γενικότερα να αλλοιώσει την μετάδοσή τους μέσα από το κανάλι επικοινωνίας. Η επίθεση αυτού του τύπου δεν προσβάλλει μόνο τον παράγοντα της μυστικότητας, αλλά την ακεραιότητα της πληροφορίας καθώς και τον παράγοντα authentication.

Στη συνέχεια θα αναφερθούμε στα κυριότερα είδη επιθέσεων για κάθε μία κρυπτογραφική τεχνική.

1.6.1 Επιθέσεις σε Συμμετρικούς Μπλοκ Αλγόριθμους

Μπορούμε να διακρίνουμε κυρίως 3 είδη επιθέσεων σε Συμμετρικούς Μπλοκ Αλγόριθμους : *διαφορική κρυπτανάλυση (differential cryptanalysis),γραμμική (linear cryptanalysis)* και την εκμετάλλευση των «αδύναμων» κλειδιών (weak keys).

Η *διαφορική κρυπτανάλυση (differential cryptanalysis)* στηρίζεται στην ανάλυση της εξέλιξης που παρουσιάζουν οι διαφορές ανάμεσα σε δύο σχετιζόμενα plaintexts, που κρυπτογραφούνται με το ίδιο κλειδί. Με προσεκτική ανάλυση των σχετιζόμενων δεδομένων, μπορεί κάποιος να δημιουργήσει πιθανά κλειδιά που μπορεί να χρησιμοποιήθηκαν για την κρυπτογράφηση (το πιο πιθανό από αυτά τα κλειδιά θεωρείται το σωστό).

Αυτές οι τεχνικές αρχικά αναπτύχθηκαν από τον Murphy, αλλά αναπτύχθηκαν και τελειοποιήθηκαν από τους Biham και Shamir, που τις χρησιμοποίησαν σε επιθέσεις εναντίον του αλγόριθμου DES[6].

Οι τενικές *γραμμιμής κρυπτανάλυσης (linear cryptanalysis)* χρησιμοποιούν μία γραμμική προσέγγιση για να περιγράψουν την συμπεριφορά ενός block cipher. Αν κάποιος έχει στην διάθεσή του αρκετά ζεύγη plaintext και του αντίστοιχου ciphertext που προκύπτει, μπορεί να ανακτήσει κομμάτια πληροφορίας που αποτελούν το κλειδί. Όσο μεγαλύτερο είναι το μέγεθος της πληροφορίας που έχει κάποιος στην διάθεσή του, τόσο πιο πιθανή είναι η δημιουργία του σωστού κλειδιού. Η τεχνική αυτή αναπτύχθηκε κυρίως από τον Matsui εναντίον του αλγόριθμου DES[7]. Τα βασικότερα χαρακτηριστικά των τεχνικών γραμμικής και διαφορικής κρυπτανάλυσης συνδυάστηκαν με επιτυχία από τους Langford και Hellman, για να δημιουργηθεί η *διαφορική-γραμμική κρυπτανάλυση* [8].

Υπάρχουν κλειδιά, τα οποία, όταν χρησιμοποιηθούν σε μπλοκ αλγόριθμο, παράγουν αποτελέσματα τα οποία παρουσιάζουν μεγάλες ομοιότητες μεταξύ τους. Αυτά τα κλειδιά ονομάζονται *αδύναμα* κλειδιά (weak keys). Για παράδειγμα, στον αλγόριθμο DES, υπάρχουν 4 κλειδιά για τα οποία η κρυπτογράφηση είναι όμοια με την αποκρυπτογράφηση. Αυτό σημαίνει ότι, αν κάποιος κρυπτογραφήσει ένα κείμενο δύο φορές με ένα από αυτά τα κλειδιά, τότε θα προκύψει το αρχικό plaintext. Παρόλα αυτά, επειδή το πλήθος αυτών των κλειδιών είναι πολύ μικρό σε σχέση με το πλήθος των διαθέσιμων κλειδιών, η πιθανότητα να χρησιμοποιηθεί κάποιο από αυτά είναι απειροελάχιστη. Υπάρχουν όμως συμμετρικοί μπλοκ αλγόριθμοι στους οποίους παρουσιάζεται μεγάλος πλήθος «αδύναμων» κλειδιών. Η ύπαρξή τους, συνεπώς, επηρεάζει σημαντικά το επίπεδο ασφάλειας που προσφέρει ένας αλγόριθμος.

1.6.2 Τεχνικές εναντίον των Hash Function

Τα κυριότερα χαρακτηριστικά των συναρτήσεων hash, σύμφωνα με προηγούμενο κεφάλαιο, είναι το γεγονός ότι είναι μη-αντστρέψιμες συναρτήσεις και 1-1. Συνεπώς, η πιο απλή επίθεση θα ήταν να χρησιμοποιήσει κάποιος τυχαίες εισόδους μέχρι να βρει εκείνη, η οποία θα παράγει ένα αποτέλεσμα το οποίο περιμένει (τεχνική που καταρρίπτει ότι η συνάρτηση είναι μη-αντιστρέψιμη), είτε να βρει δύο εισόδους που παράγουν το ίδιο αποτέλεσμα (γεγονός που καταρρίπτει την ιδιότητα 1-1).

Η κυριότερη επίθεση εναντίον hash functions είναι η *γενέθλια επίθεση* (*birthday attack*). Παίρνει το όνομά της από το εκπληκτικό γεγονός ότι η πιθανότητα να έχουν δύο ή περισσότερα άτομα γενέθλια την ίδια ημερομηνία, σε ένα γκρουπ των 23 ατόμων, είναι μεγαλύτερη από ½. Αυτό το παράδοξο ονομάζεται *παράδοξο των γενεθλίων.* Ας προσαρμόσουμε το γεγονός αυτό στο πεδίο του ενδιαφέροντός μας.Υποθέτουμε ότι έχουμε μία συνάρτηση η οποία , όταν πάρει μια τυχαία είσοδο, δίνει έξοδο η οποία ανήκει σε ισοπιθανοτικό σύνολο με πλήθος τιμών ίσο με *k*. Τότε, για δύο διαφορετικές εισόδους, θα πάρουμε το ίδιο αποτέλεσμα μετά από $1.2k^{1/2}$ προσπάθειες. Στην περίπτωση μιας hash function τώρα, όταν προσπαθήσουμε να βρούμε την ίδια έξοδο για δύο διαφορετικές εισόδους, τότε θα τα καταφέρουμε αφού δοκιμάσουμε $1.2(2^{n/2})$ διαφορετικές εισόδους, σύμφωνα με το παράδοξο των γενεθλίων (καταρρίπτουμε έτσι ότι η συνάρτηση είναι 1-1). Οι Van Oorschot και Wiener ανέπτυξαν υλοποίηση για μια τέτοια επίθεση[9].

1.6.3 Επιθέσεις εναντίον Stream Ciphers

Όπως έχει αναφερθεί, η πιο διαδεδομένη χρήση των stream ciphers είναι η εφαρμογή του *keystream* (μία ακολουθία bits που δημιουργούνται από ένα μυστικό κλειδί), στο μη κρυπτογραφημένο κείμενο, με την χρήση της λογικής πράξης αποκλειστικό-ή. Ο στόχος είναι τα bits που αποτελούν το keystream να είναι τυχαία και να μην υπάρχει κανένας παράγοντας συσχέτισης μεταξύ τους. Παρόλα αυτά μπορεί κάποιος να μελετήσει την συχνότητα εμφάνισης συγκεκριμένων bit ή ακόμα και μεγαλύτερων ακολουθιών από αυτά, μετά από την διεξαγωγή συγκεκριμένων τεστ. Επιπρόσθετα, αυτά τα τεστ μπορούν να μελετήσουν το βαθμό *συσχέτισης (correlation)* κάποιων bit που εμφανίζονται σε συγκεκριμένο σημείο, με την εμφάνιση bit σε άλλα σημεία της ακολουθίας. Ο μόνος τρόπος αντιμετώπισης τέτοιων επιθέσεων είναι ο σχεδιασμός ενός αλγόριθμου με πολύ μικρή περίοδο του keystream, όπου περίοδος είναι το πλήθος των bit του keystream μέχρι το σημείο που αυτός αρχίζει να επαναλαμβάνεται. Ενας stream αλγόριθμος συνεπώς, μπορεί να χαρακτηριστεί ασφαλής και «δυνατός», όταν ο σχεδιασμός του είναι τέτοιος ώστε να ελαχιστοποιείται ο παράγοντας συσχέτισης που μπορεί να παρουσιαστεί μέσα στην ακολουθία των bits του keystream.

Επίσης, υπάρχουν και οι επιθέσεις τύπου *διαίρει και βασίλευε (divide and conquer)*, στόχος των οποίων είναι να βρεθεί μέρος του μυστικού κλειδιού. Ο κρυπταναλυτής προσπαθεί να βρει κάποια ακολουθία του μυστικού κλειδιού που επηρεάζει άμεσα το περιεχόμενο του keystream. Αυτή η συσχέτιση, μεταξύ του παραγόμενου keystream από μία εικασία για ένα κομμάτι του κλειδιού και του αρχικού keystream, αποτελεί το χαρακτηριστικό επιθέσεων συσχέτισης, που ονομάζονται *correlation attacks*. Οι επιθέσεις τύπου *διαίρει και βασίλευε (divide and conquer)* αποτελούν ένα τύπο των *correlation attacks*.

1.6.4 Επιθέσεις εναντίον των MACs (Message authentication Code)

Η ασφάλεια του MAC μπορεί να διαταραχτεί από πολλούς παράγοντες. Πρωταρχικά, είναι αναγκαίο η χρήση του αλγόριθμου αυτού να μην αποκαλύπτει καμία πληροφορία του μυστικού κλειδιού που χρησιμοποιήθηκε. Δευτερευόντως, ένας τρίτος δεν πρέπει να έχει την δυνατότητα να αλλοιώσει το MAC ενός μηνύματος, χωρίς να έχει την γνώση του μυστικού κλειδιού. Τρίτον, όταν στέλνεται το ζεύγος μήνυμα-MAC, θα πρέπει να είναι αδύνατη η αντικατάσταση του μηνύματος από ένα άλλο μη αυθεντικό.

Η πιο σημαντική κατηγορία επιθέσεων είναι αυτή που αναπτύχθηκε από τους Preneel και Van Oorschot [11]. Αυτές οι επιθέσεις βασίζονται στην εφαρμογή του παράδοξου των γενεθλιών (birthday paradox) στην ανάλυση του ζεύγους μηνύματος-MAC, και βοήθησαν σημαντικά στο να βρεθούν λάθη στην δομή των MAC, με άμεση συνέπεια την βελτίωσή τους.

1.6.5 Επιθέσεις εναντίον των Ασύμμετρων Αλγόριθμων

Στο κεφάλαιο αυτό θα επικεντρωθούμε κυρίως σε επιθέσεις που αφορούν στον αλγόριθμο RSA. Η πιο σοβαρή επίθεση στον RSA είναι αυτή η οποία βοηθά τον επιτιθέμενο να ανακτήσει το ιδιωτικό κλειδί κάποιου. Αυτό θα του επιτρέψει να διαβάσει κάθε κρυπτογραφημένο μήνυμα που μεταδίδεται (το οποίο, βέβαια, θα έχει κρυπτογραφηθεί με το αντίστοιχο δημόσιο κλειδί) και θα του δώσει παράλληλα την δυνατότητα να «πλαστογραφήσει» ψηφιακές υπογραφές. Ο τρόπος για να τελεσφορήσει μια τέτοια επίθεση είναι ο υπολογισμός του modulus n, και των δύο συντελεστών του p και q, οι οποίοι είναι πρώτοι αριθμοί. Ανακτώντας τους συντελεστές p , q, και τον δημόσιο εκθέτη e, ο επιτιθέμενος μπορεί να υπολογίσει και τον ιδιωτικό εκθέτη d (που ουσιαστικά είναι το ιδιωτικό κλειδί). Το δύσκολο κομμάτι, βέβαια, είναι ο υπολογισμός του modulus n, αφού η ασφάλεια του RSA στηρίζεται εξ'ολοκλήρου στην δυσκολία υπολογισμού του.

Μια άλλη τεχνική για να «σπάσει» κάποιος τον αλγόριθμο RSA είναι να βρει μία τεχνική ώστε να υπολογίζει το υπόλοιπο της διαίρεσης των e-ιοστών ριζών του ciphertext c με το modulus n (εφόσον ισχύει $c = m^e \bmod n$,το υπόλοιπο της

διαίρεσης της *e*-ιοστής ρίζας του *c*, είναι το αρχικό μήνυμα *m*). Με αυτή την τεχνική ο επιτιθέμενος μπορεί να ανακτήσει τα μηνύματα που στέλνει κάποιος και να πλαστογραφήσει ψηφιακές υπογραφές ακόμη και χωρίς να γνωρίζει το ιδιωτικό κλειδί.

Οι ανωτέρω τεχνικές πρασπαθούν να διαβάλλουν την «καρδιά» του αλγόριθμου RSA και να ανακτήσουν κάθε μήνυμα που κρυπτογραφείται με ένα κλειδί. Υπάρχουν όμως τεχνικές σύμφωνα με τις οποίες ο στόχος είναι να αποκρυπτογραφηθεί ένα συγκεκριμένο μήνυμα. Η πιο απλή από αυτέςονομάζεται *guessed plaintext attack.* Σύμφωνα με αυτή, ο επιτιθέμενος προσπαθεί να μαντέψει ποιο μπορεί να είναι το αρχικό μήνυμα ενός ciphertext και το κρυπτογραφεί με το δημόσιο κλειδί του αποστολέα. Συγκρίνοντας το αυθεντικό ciphertext μπορεί να δει αν έχει μαντέψει σωστά. Η πιθανότητα επιτυχίας μιας τέτοιας επίθεσης είναι απειροελάχιστη και μπορεί εύκολα να εξουδετερωθεί προσθέτοντας τυχαία bits μήνυμα μέσω padding.

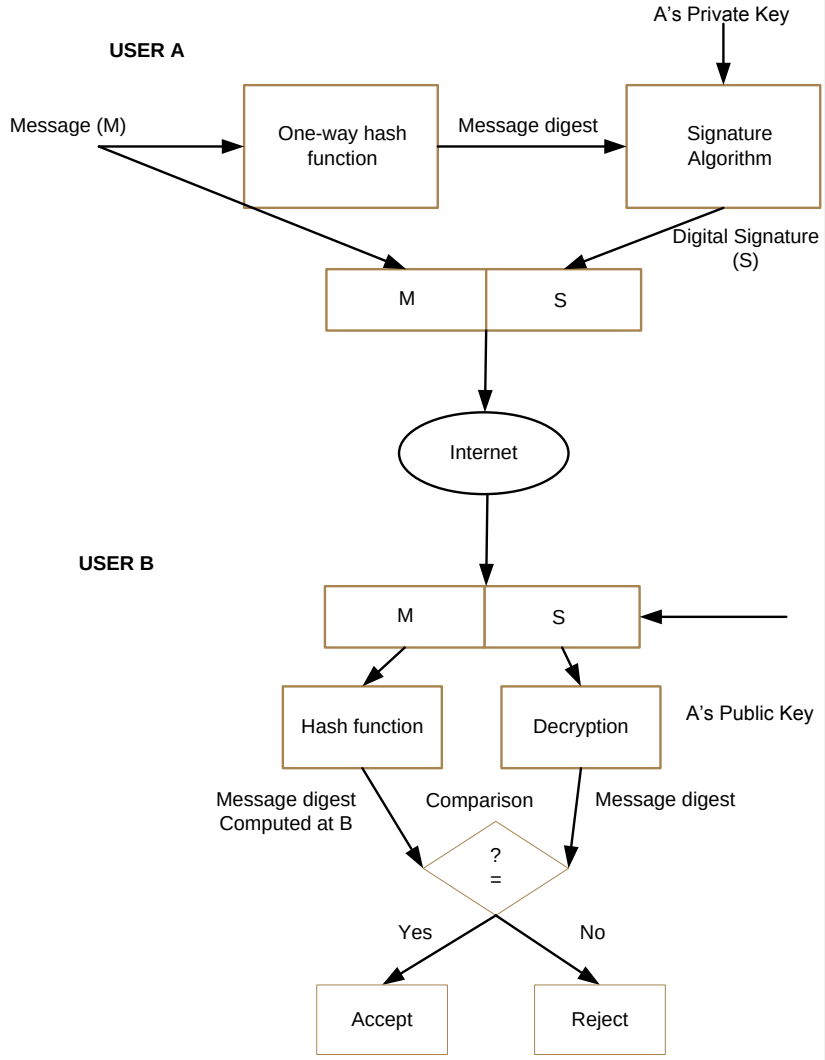
Τέλος, πρέπει να δώσουμε ιδιαίτερη έμφαση σε επιθέσεις οι οποίες δεν έχουν ως στόχο να διαβάλλουν τον αλγόριθμο RSA αυτό καθ’αυτό, αλλά την υλοποίησή του. Εκμεταλλεύονται, δηλαδή, μία αδυναμία στην υλοποίηση του αλγορίθμου και δεν ψάχνουν για αδύναμα σημεία στην μαθηματική αρχιτεκτονική του. Για παράδειγμα, αν κάποιος αποθηκεύσει το ιδιωτικό του κλειδί χωρίς να εξασφαλήσει μεγάλο βαθμό ασφάλειάς του, κάποιος κακόβουλος μπορεί εύκολα να το υποκλέψει. Έχει παρατηρηθεί ότι οι πιο πετυχημένες επιθέσεις είναι αυτές που προσανατολίζονται εναντίον εφαρμογών με επισφαλή υλοποίηση και κακό key management.

1.7 ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ ΚΑΙ ΤΕΧΝΙΚΕΣ

Όπως έχει αναφερθεί στην ενότηταπου αφορά τους αλγόριθμους δημοσίου κλειδιού, και ειδικότερα τον αλγόριθμο RSA, η τεχνική της ψηφιακής υπογραφής είναι απολύτως χρήσιμη στην επιστήμη της Κρυπτογραφίας. Ο στόχος της είναι να συνδυάσει μοναδικά την πληροφορία με την ταυτότητα του κατόχου της. Δύο είναι οι ενέργειες που απορρέουν από την ψηφιακή υπογραφή: η δημιουργία της και η επικύρωσή της από έναν τρίτο.

Η σωστή εφαρμογή της ψηφιακής υπογραφής σε ένα κρυπτοσύστημα διασφαλίζει θεμελιώδεις απαιτήσεις ασφάλειας όπως την αυθεντικότητα των δεδομένων και της πηγής (data origin authentication, data source authentication), την ακεραιότητα της πληροφορίας (data integrity), την εξουσιοδότηση του υπογράφοντα (authorization) και την αποφυγή άρνησης αποστολής της από αυτόν (non-repudiation). Η απαίτηση για non-repudiation προσθέτει ένα επιπλέον επίπεδο ασφάλειας σε ένα κρυπτοσύστημα καθώς, εάν ο δημιουργός μιας υπογραφής την αποστείλει και στην συνέχεια το αρνηθεί, αυτό σημαίνει ότι ψεύδεται διότι η υπογραφή θα επικυρώνεται με την χρήση του δημόσιου κλειδιού του.

Στο διάγραμμα που ακολουθεί παρουσιάζεται ένα βασικό μοντέλο ψηφιακής υπογραφής (digital signature) ανάμεσα σε δύο πλευρές A και B.



Σχήμα 1.11 Digital Signature Scheme

Υποθέτουμε ότι ο Α θέλει να στείλει ένα υπογεγραμμένο μήνυμα στον Β. Αρχικά ο Α εφαρμόζει μία hash συνάρτηση στο μήνυμα που θέλει να στείλει, δημιουργώντας μία «περίληψη» του μηνύματος, η οποία ονομάζεται *message digest*. Το message digest είναι μοναδικό για κάθε μήνυμα και αποτελεί το «ψηφιακό αποτύπωμά» του. Στην συνέχεια κρυπτογραφεί το message digest με το ιδιωτικό του κλειδί, και δημιουργεί την ψηφιακή υπογραφή του μηνύματος, την οποία στέλνει στον Β μαζί με το αρχικό μήνυμα. Όταν ο Β παραλάβει τα

δεδομένα, αποκρυπτογραφεί πρώτα την υπογραφή με το δημόσιο κλειδί του Α για να πάρει το message digest του μηνύματος. Αυτό που έχει να κάνει στην συνέχεια είναι να εφαρμόσει την ίδια hash function στο αρχικό μήνυμα και να εξετάσει την ομοιότητα των δύο message digest που έχουν προκύψει. Αν είναι απολύτως όμοια μεταξύ τους, τότε έχει επικυρώσει την ψηφιακή υπογραφή και μπορεί να είναι απολύτως σίγουρος ότι το μήνυμα έχει αποσταλεί από τον Α. Στην αντίθετη περίπτωση πρέπει να απορρίψει το μήνυμα διότι αποδεικνύεται ότι είτε ο αποστολέας δεν είναι ο Α, είτε τα δεδομένα έχουν υποστεί αλλοίωση μετά την αποστολή τους.

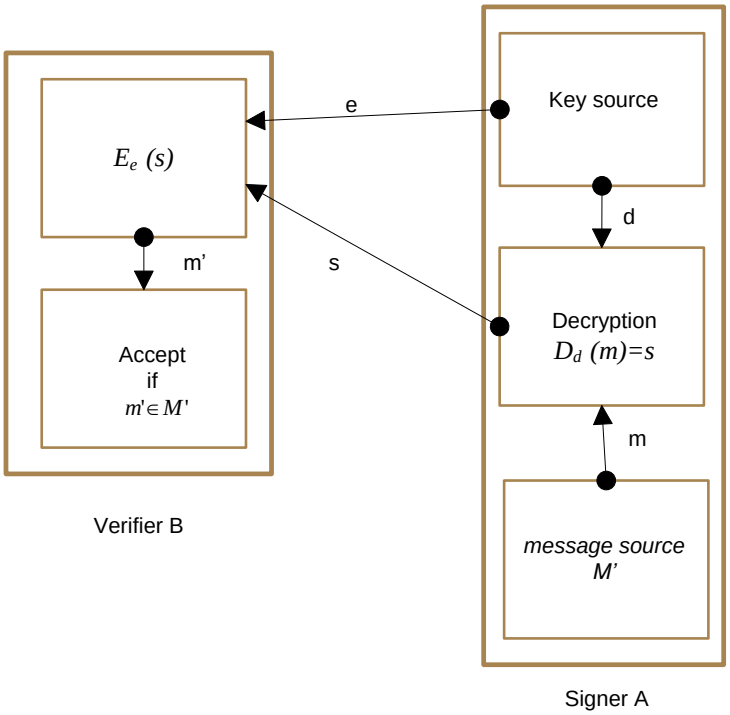
Η πιο σημαντική εφαρμογή της ψηφιακής υπογραφής είναι η πιστοποίηση των δημόσιων κλειδιών ενός μεγάλου δικτύου. Η πιστοποίηση είναι ένα μέσο για μια εμπιστευόμενη τρίτη οντότητα (trusted third party) να συνδέσει το δημόσιο κλειδί με την ταυτότητα του κατόχου του με την δημιουργία ενός ψηφιακού πιστοποιητικού (digital certificate). Αυτό δίνει την δυνατότητα σε άλλες οντότητες να ελέγχουν την αυθεντικότητα ενός δημοσίου κλειδιού, σε μελλοντικές στιγμές, χωρίς τη βοήθεια ενός trusted third party.

Ένα σημείο το οποίο πρέπει να τονιστεί είναι το γεγονός ότι όλοι οι αλγόριθμοι ψηφιακής υπογραφής βασίζονται στην χρήση των τεχνικών των hash functions και των message digest. Αυτό οφείλεται στο ότι οι ασύμμετροι αλγόριθμοι παρουσιάζουν περιορισμούς στο μέγεθος των μηνυμάτων μπορούν να επεξεργαστούν. Οδηγούμαστε λοιπόν στο συμπέρασμα ότι το μέγεθος της πληροφορίας που μπορούμε να υπογράψουμε θα πρέπει να ορίζεται από το μέγεθος των δεδομένων εκ των οποίων δημιουργείται το message digest. Το μέγεθος του κλειδιού το μόνο που κάνει είναι συνεπώς να προστατεύει το message digest.

Τα μοντέλα ψηφιακής υπογραφής που έχουν αναπτυχθεί στις μέρες μας χωρίζονται σε δύο κατηγορίες:

- Στα μοντέλα με *παράρτημα* (*appendix schemes*), τα οποία χρησιμοποιούν το αυθεντικό μήνυμα ως είσοδο στον αλγόριθμο που θα κάνει το verification της υπογραφής. Το βασικότερο μοντέλο είναι αυτό που υλοποιεί τον αλγόριθμο DSA (Digital Signature Algorithm). Ένα τέτοιο μοντέλο παρουσιάζεται στο σχήμα 1.11.

• Στα μοντέλα *ανάκτησης του μηνύματος* (*message recovery schemes*), στα οποία δεν απαιτείται η προηγούμενη γνώση του αυθεντικού μηνύματος. Στην περίπτωση αυτή, ο αλγόριθμος ανακτά το μήνυμα από την ίδια την υπογραφή. Ο ευρύτερα χρησιμοποιούμενος αλγόριθμος σε αυτά τα μοντέλα είναι ο RSA. Ένα τέτοιο μοντέλο παρουσιάζεται στο σχήμα 1.12



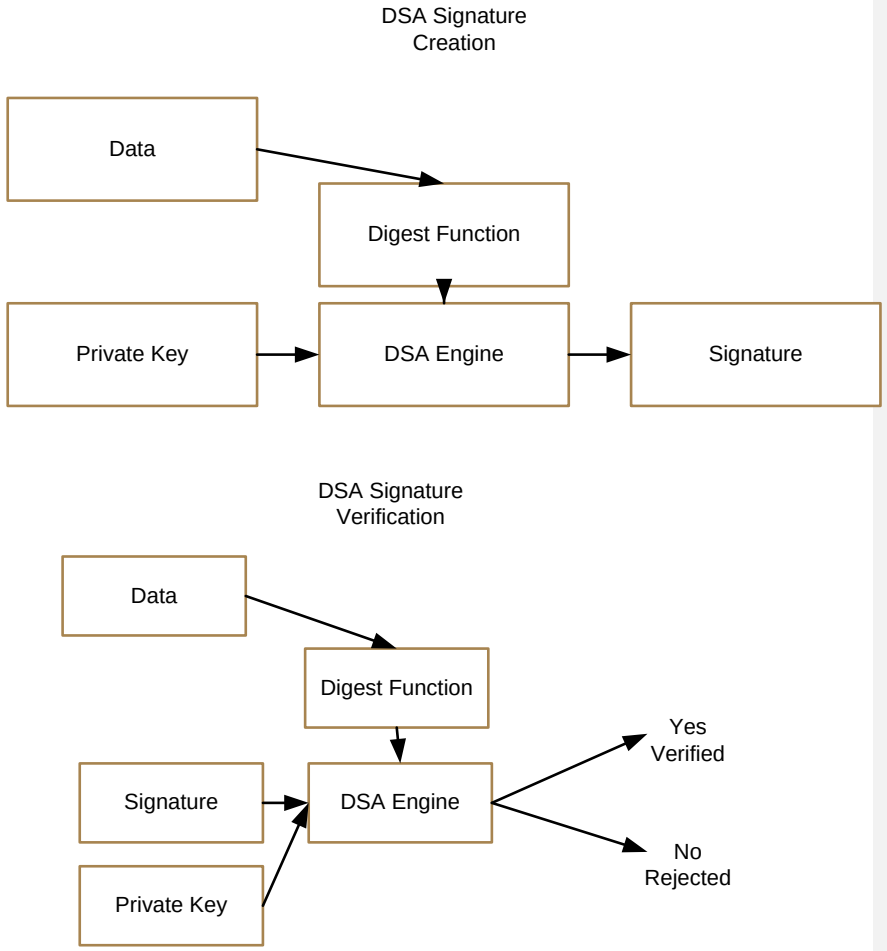
Σχήμα 1.12 Μοντέλο ψηφιακής υπογραφής με ανάκτηση μηνύματος

Για το RSA digital signature message recovery scheme έχει γίνει εκτενέστατη αναφορά στο υποκεφάλαιο «RSA και Authentication» (1.4.1.3.1.2). Στην συνέχεια θα αναφερθούμε στο μοντέλο appendix, και ειδικότερα στον αλγόριθμο DSA (Digital Signature Algorithm).

1.7.1 Αλγόριθμος DSA (Digital Signature Algorithm)

Ο αλγόριθμος DSA (Digital Signature Algorithm) δημοσιεύτηκε από το NIST (National Institute of Standards and Technology) το 1991 και στη συνέχεια συμπεριλήφθηκε στο DSS (Digital Signature Standard) τον Μάιο του 1994.

Ο DSA βασίζεται στην δυσκολία υπολογισμού των διακριτών λογαρίθμων (discrete logarithm problem) και μελετήθηκε σε τεχνικές που δημοσίευσαν οι El-Gamal και Schnorr. Στο επόμενο σχήμα παρουσιάζεται ένα μοντέλο ψηφιακής υπογραφής με την χρήση του DSA.



Σχήμα 1.13 DSA Signature Processes

Πρέπει να τονισθεί το γεγονός ότι ο αλγόριθμος είναι έτσι σχεδιασμένος ώστε να μην μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση δεδομένων. Μπορεί να χρησιμοποιηθεί αποκλειστικά για την επιβεβαίωση μιας υπογραφής με την χρήση ενός δημοσίου κλειδιού. Για τον λόγο αυτό άλλωστε, χρειάζεται το αυθεντικό μήνυμα για να επικυρώσει μία υπογραφή. Αντίθετα, αλγόριθμοι, όπως ο RSA, που έχουν κρυπτογραφικές ιδιότητες, όταν χρησιμοποιηθούν σε μοντέλα ψηφιακής υπογραφής, έχουν την δυνατότητα να ανακτούν το αυθεντικό μήνυμα μέσω της διαδικασίας επικύρωσης της υπογραφής. Είναι συνεπώς λογικό το γεγονός ότι, στον DSA, η διαδικασία δημιουργίας της υπογραφής είναι πολύ πιο γρήγορη από την επικύρωσή της, ενώ στον RSA συμβαίνει εντελώς το αντίθετο.

Ο αλγόριθμος δέχθηκε οξεία κριτική για κάποια θέματα τα οποία αφορούσαν τα τεχνικά χαρακτηριστικά του και όχι μόνο. Τα βασικότερα από αυτά είναι τα εξής : 1) υστερεί σε ευελιξία έναντι του RSA, 2) η επικύρωση των υπογραφών είναι πολύ αργή 3) το γεγονός ότι έγινε αποκλειστικό standard πολύ γρήγορα δεν επιτρέπει την εύκολη υιοθέτηση ενός άλλου μηχανισμού authentication από προγραμματιστές software και hardware. Παρά, όμως, την συνεχή κριτική που δέχονται αυτά τα χαρακτηριστικά του έχει αναπτυχθεί σε πολυάριθμες εφαρμογές και συστήματα. Στην συνέχεια θα αναφερθούμε συνολικά στις εφαρμογές των μηχανισμών ψηφιακής υπογραφής που παρουσιάζουν το μεγαλύτερο ενδιαφέρον.

1.7.2 Εφαρμογές της Ψηφιακής Υπογραφής

Οι τεχνικές ψηφιακής υπογραφής χρησιμοποιούνται ευρέως και έχουν ενσωματωθεί σε πολλαπλές εφαρμογές. Η τεχνολογία, άλλωστε, της ψηφιακής υπογραφής εξελίσσεται συνεχώς, γεγονός που διασφαλίζει την χρήση της και την πρόοδό της και στο μέλλον. Στην συνέχεια θα αναφερθούμε συνοπτικά στις κυριότερες εφαρμογές από αυτές.

Ασφάλεια Ηλεκτρονικού Ταχυδρομείου (E-mail)

Το ηλεκτρονικό ταχυδρομείο είναι απαραίτητο να υποστηρίζει την δυνατότητα της ψηφιακής υπογραφής, ιδιαίτερα σε περιπτώσεις όπου μεταδίδεται ευαίσθητη πληροφορία και απαιτούνται υπηρεσίες ασφάλειας όπως

authentication, non-repudiation και integrity. Το πρωτόκολλο MOSAIC εμπεριέχει τον αλγόριθμο DSA και τον χρησιμοποιεί για την υπογραφή των E-mails και των πιστοποιητικών δημοσίου κλειδιού. Επίσης το πρωτόκολλο PGP (Pretty Good Privacy) προσφέρει υπηρεσίες ασφαλείας για την αποστολή μηνυμάτων και αρχείων χρησιμοποιώντας τεχνικές ψηφιακής υπογραφής, κρυπτογράφησης και συμπίεσης (zip). Ένα ακόμη πρωτόκολλο που χρησιμοποιεί ψηφιακές υπογραφές είναι το S/MIME (Secure/Multipurpose Internet Mail Extensions) το οποίο είναι ουσιαστικά μια βελτιωμένη έκδοση, σε επίπεδο ασφάλειας, του MIME Internet e-mail format, και βασίζεται στον αλγόριθμο RSA. Αν και τα δύο πρωτόκολλα που προαναφέρθησαν (PGP και S/MIME) αποτελούν standards του IETF (Internet Engineering Task Force), είναι σίγουρο ότι το πρώτο θα προτιμάται περισσότερο για προσωπική χρήση, ενώ το δεύτερο θα υιοθετηθεί σε μεγάλο βαθμό από την βιομηχανία για εμπορική χρήση.

Ασφάλεια οικονομικών συναλλαγών

Είναι πολύ σημαντικό το γεγονός να διασφαλίζεται η ασφάλεια των οικονομικών συναλλαγών που διεξάγονται μέσω του διαδικτύου. Η *Ηλεκτρονική Μεταφορά Κεφαλαίων (Electronic Funds Transfer)* επωφελείται σε σημαντικό βαθμό με την χρήση της ψηφιακής υπογραφής.

Το πιο γνωστό πρωτόκολλο που σχετίζεται με το ηλεκτρονικό εμπόριο είναι το SET (Secure Electronic Transaction). Το SET εισήγαγε ένα νέο μοντέλο ψηφιακών υπογραφών που ονομάζεται διπλές υπογραφές (dual signatures). Μία διπλή υπογραφή δημιουργείται υπολογίζοντας το message digest δύο μηνυμάτων : αυτό της παραγγελίας και αυτό της πληρωμής. Το πρωτόκολλο SET χρησιμοποιεί τις ανωτέρω κρυπτογραφικές τεχνικές για να παρέχει μυστικότητα της πληροφορίας, για να διασφαλίζει την ακεραιότητα της πληρωμής και την πιστοποίηση της ταυτότητας αυτών που εμπλέκονται στην συναλλαγή.

Προστασία του software

Μια ακόμη χρησιμότητα των ψηφιακών υπογραφών είναι στην προστασία του software. Υπογράφοντας το software διασφαλίζεται η ακεραιότητα κατά την διανομή του. Η υπογραφή επικυρώνεται όταν εγκαθίσταται το προϊόν στον

υπολογιστή του αγοραστή και με τον τρόπο αυτό είναι σίγουρος ότι δεν έχει υποστεί καμία ανεπιθύμητη αλλοίωση κατά την διανομή του.

Ασφάλεια της ηλεκτρονικής αρχειοθέτησης (electronic filing)

Όπως γνωρίζουμε, για την υπογραφή ενός συμβολαίου χρειάζεται η υποβολή κάποιων πιστοποιητικών από τους συμβαλλόμενους. Είναι απαραίτητη λοιπόν η αρχειοθέτηση κάποιων γραπτών φορμών ή πιστοποιητικών τα οποία πρέπει να επικυρωθούν με μία γραπτή υπογραφή. Σήμερα όμως η αρχειοθέτηση γίνεται με ηλεκτρονικό τρόπο και η ψηφιακή υπογραφή μπορεί να αντικαταστήσει την γραπτή διασφαλίζοντας υπηρεσίες ασφάλειας, όπως ακεραιότητα και πιστοποίηση της αυθεντικότητας. Ένα πεδίο στο οποίο βρίσκει πολλή καλή εφαρμογή αυτή η διαδικασία είναι η υποβολή των φορολογικών δηλώσεων.

1.7.3 Επιθέσεις εναντίον των Ψηφιακών Υπογραφών

Ο στόχος ενός κακόβουλου ατόμου είναι να μπορέσει να πλαστογραφήσει ψηφιακές υπογραφές. Με τον τρόπο αυτό θα μπορεί να δημιουργεί υπογραφές οι οποίες φαινομενικά θα φαίνονται ότι προέρχονται από μία άλλη οντότητα. Στην συνέχεια αναφέρονται τύποι επιτυχών επιθέσεων σε ψηφιακές υπογραφές.

- Συνολική κατάρρευση της υπογραφής (total break), στην οποία το κακόβουλο άτομο έχει καταφέρει να δημιουργήσει την πληροφορία του ιδιωτικού κλειδιού του κατόχου, ή έχει καταφέρει να δημιουργήσει έναν αποδοτικό αλγόριθμο ψηφιακής υπογραφής ο οποίος είναι όμοιος με αυτόν που χρησιμοποίησε ο κάτοχος.
- Επιλεκτική πλαστογράφηση της υπογραφής (selective forgery). Στην περίπτωση αυτή ο κακόβουλος έχει καταφέρει να δημιουργήσει μία αποδεκτή υπογραφή ενός συγκεκριμένου μηνύματος, ή περισσοτέρων, που έχει επιλέξει ο ίδιος a priori.
- Πλαστογράφηση υπάρχοντος μηνύματος (existential forgery). Στην περίπτωση αυτή ο κακόβουλος καταφέρνει να δημιουργήσει μία αποδεκτή υπογραφή ενός ή περισσοτέρων μηνυμάτων, τα οποία δεν έχει επιλέξει ο ίδιος, αλλά ο νόμιμος υπογράφων.

Συμπερασματικά μπορούμε να πούμε ότι οι τεχνικές που ακολουθούνται από κακόβουλους για την επίτευξη πλαστογράφησης χωρίζονται σε δύο κατηγορίες :
α) σε αυτές που ο κακόβουλος γνωρίζει μόνο το δημόσιο κλειδί του υπογράφοντα και ονομάζονται *key-only attacks*
β) σε αυτές που ο κακόβουλος εξετάζει υπογραφές μηνυμάτων που ο ίδιος γνωρίζει, είτε μηνυμάτων που έχει ο ίδιος δημιουργήσει προηγουμένως. Αυτές ονομάζονται *message attacks*.
Το επίπεδο ασφάλειας που απαιτείται σε ένα μοντέλο ψηφιακής υπογραφής εξαρτάται αποκλειστικά από την υλοποίησή του. Για παράδειγμα, σε περίπτωση όπου ένας κακόβουλος έχει την δυνατότητα μιας key-only επίθεσης, θα πρέπει να σχεδιαστεί ένα μοντέλο το οποίο να τον αποτρέπει απόεπιλεκτική πλαστογράφηση της υπογραφής (selective forgery). Επιπλέον, όταν ένα μοντέλο είναι ευάλωτο σε message επιθέσεις, πρέπει να εξασφαλίζεται ότι ένας τρίτος δεν θα μπορεί να επιτυγχάνει πλαστογράφηση υπάρχοντος μηνύματος (existential forgery).

ΚΕΦΑΛΑΙΟ 2: ΠΡΩΤΟΚΟΛΛΑ ΚΑΙ ΤΕΧΝΙΚΕΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΛΕΙΔΙΩΝ

2.1 ΓΕΝΙΚΑ ΓΙΑ ΤΗΝ ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΩΝ – KEY MANAGEMENT

Οι κύριοι στόχοι της διαχείρισης κλειδιών είναι η ασφαλής δημιουργία, διανομή και αποθήκευση των κλειδιών που χρησιμοποιούνται μέσα σε ένα δίκτυο. Πρόκειται για ένα σύνολο από τεχνικές και διαδικασίες οι οποίες υποστηρίζουν την εγκαθίδρυση και διατήρηση σχέσεωνμεταξύ των οντοτήτων ενός δικτύου, που αφορούν τα κλειδιά.

Συνοπτικά η διαχείριση των κλειδιών αποτελείται από τις εξής διαδικασίες :

1. Αρχικοποίηση ενός δικτύου χρηστών
2. δημιουργία, διανομή και εγκατάσταση των κλειδιών
3. έλεγχος της χρήσης τους
4. ανανέωση, ανάκληση και καταστροφή τους
5. αποθήκευση και αρχειοθέτησή τους

2.1.1 Χρήση των κλειδιών

Τα συστήματα Κρυπτογραφίας διαχωρίζονται σε δύο κατηγορίες σύμφωνα με τους αλγόριθμους που δημιουργούν τα κλειδιά. Ένα *συμμετρικό κρυπτοσύστημα,* είναι ένα σύστημα το οποίο βασίζεται σε δύο μετασχηματισμούς που αφορούν τα κλειδιά, έναν για τον αποστολέα και έναν για τον παραλήπτη. Και οι δύο μετασχηματισμοί κάνουν χρήση είτε ενός κοινού συμμετρικού μυστικού κλειδιού, είτε δύο διαφορετικών κλειδιών, το καθένα εκ των οποίων υπολογίζεται πολύ εύκολα από το άλλο. Από την άλλη πλευρά, ένα *ασύμμετρο κρυπτοσύστημα* περιλαμβάνει δύο σχετιζόμενους μετασχηματισμούς, ο πρώτος εκ των οποίων προσδιορίζεται από ένα δημόσιο κλειδί (public key) και ο δεύτερος από ένα ιδιωτικό κλειδί (private key) .Όπως έχει τονισθεί στο κεφάλαιο που αφορά την ασύμμετρη κρυπτογραφία, είναι αναγκαίο για την ασφάλεια του συστήματος, ο υπολογισμός του μετασχηματισμού που περιέχει το ιδιωτικό κλειδί να είναι αδύνατο να υπολογιστεί από τον μετασχηματισμό που περιλαμβάνει το δημόσιο κλειδί. Στον ακόλουθο πίνακα (πίνακας 2.1) παρουσιάζεται συνοπτικά η σύνδεση

των διάφορων αλγορίθμων, συμμετρικών και ασύμμετρων, με τους κρυπτογραφικούς στόχους που επιτυγχάνουν.

Κρυπτογραφικός Στόχος	Τύπος Αλγόριθμου	
	Δημόσιου κλειδιού	Συμμετρικού κλειδιού
Confidentiality	Κρυπτογράφηση	Κρυπτογράφηση
Data origin authentication	Ψηφιακή Υπογραφή	MAC
Key Agreement	Diffie-Hellman	Διάφορες μέθοδοι
Entity Authentication	1.Ψηφιακή Υπογραφή 2.Αποκρυπτογράφηση	1.MAC 2.Κρυπτογράφηση

Πίνακας 2.1 Αλγόριθμοι και Απαιτήσεις Ασφάλειας

2.1.2 Διαβάθμιση των κλειδιών ανάλογα με την χρήση τους

Για να έχουμε μία σωστή διαχείριση των κλειδιών τα διακρίνουμε σε κατηγορίες ανάλογα με την πληροφορία που προστατεύουν. Πρόκειται για τις ακόλουθες κατηγορίες [1]:

- τα ***master keys***, τα οποία βρίσκονται στην υψηλότερη θέση της ιεραρχίας και δεν προστατεύονται με κάποιο κρυπτογραφικό τρόπο. Για την εξασφάλιση της μυστικότητάς τους, η διανομή τους γίνεται είτε δια χειρός, είτε προστατεύονται με ηλεκτρονικό τρόπο στο σύστημα στο οποίο εγκαταστάθηκαν. Τα ιδιωτικά κλειδιά ανήκουν σε αυτή την κατηγορία.
- ***Τα key-encrypting keys*** τα οποία χρησιμοποιούνται για να κρυπτογραφούν άλλα κλειδιά. Τα κλειδιά αυτά, συμμετρικά ή δημόσια, χρησιμεύουν για την μεταφορά και αποθήκευση άλλων κλειδιών.
- Τα ***κλειδιά δεδομένων*** (*data keys*), τα οποία χρησιμοποιούνται σε κρυπτογραφικές λειτουργίες πάνω σε δεδομένα ενός χρήστη, π.χ. κρυπτογράφηση, πιστοποίηση. Στην κατηγορία αυτή ανήκουν κυρίως τα συμμετρικά κλειδιά μικρής διάρκειας ζωής. Θα μπορούσαμε να πούμε ότι στην κατηγορία αυτή ανήκει και το ζεύγος δημόσιου-ιδιωτικού κλειδιού, αν και η διάρκεια ζωής τους είναι πολύ μεγάλη.

Η χρησιμότητα αυτής της κατηγοριοποίησης βασίζεται στο γεγονός ότι τα κλειδιά μιας βαθμίδας προστατεύουν αυτά που βρίσκονται στην αμέσως χαμηλότερη. Με τον τρόπο αυτό οι επιθέσεις καθίσταται πιο δύσκολο να επιτύχουν τους στόχους τους καθώς μειώνεται στο ελάχιστο η διαβλητότητα του συστήματος λόγω της αυστηρής διαβάθμισής του.

2.1.3 Βασικές πληροφορίες που καθορίζουν την χρήση των κλειδιών

Είναι αναγκαίο κάθε κλειδί να συνδέεται με πληροφορίες που καθορίζουν τον τρόπο με τον οποίο μπορεί να το χρησιμοποιήσει κάποιος, ώστε να αποφεύγεται η κατάχρησή του. Οι πληροφορίες αυτές καθορίζονται κυρίως στα ψηφιακά πιστοποιητικά που εκδίδει μία αρχή. Οι κυριότερες από αυτές είναι οι ακόλουθες [2]:

1. ο ιδιοκτήτης του κλειδιού
2. το χρονικό διάστημα που μπορεί ο κάτοχός του να το χρησιμοποιήσει
3. οι εφαρμογές στις οποίες μπορεί να χρησιμοποιηθεί (confidentiality, data origin authentication, entity authentication, key agreement)
4. ο αλγόριθμος που χρησιμοποιείται
5. τα ονόματα των οντοτήτων τα οποία συνδέονται με την δημιουργία, την καταχώρηση και την πιστοποίηση των κλειδιών
6. το σύστημα ή το περιβάλλον που μπορούν να χρησιμοποιηθούν τα κλειδιά
7. μία πληροφορία αναγνώρισης του κλειδιού (key identifier)
8. το checksum του κλειδιού, το οποίο χρησιμοποιείται σε διαδικασίες authentication

Μία βασική αρχή, ώστε ένα κρυπτοσύστημα να παραμένει ασφαλές, είναι να μην επιτρέπεται η χρήση ενός κλειδιού για περισσότερες από μία κρυπτογραφικές τεχνικές. Για τον λόγο αυτό θα πρέπει τα κλειδιά τα οποία χρησιμοποιούνται για διαφορετικές κρυπτογραφικές τεχνικές να είναι κρυπτογραφικώς διαχωρισμένα μεταξύ τους. Η αρχή αυτή ονομάζεται *διαχωρισμός των κλειδιών (key separation principle).* Για παράδειγμα, ένα κλειδί το οποίο χρησιμεύει στο να κρυπτογραφεί άλλα κλειδιά (key-encryption key) δεν θα πρέπει να χρησιμοποιείται για κρυπτογράφηση δεδομένων, διότι τα αποκρυπτογραφημένα κλειδιά δεν γίνονται

διαθέσιμα στις εφαρμογές, αντίθετα με τα αποκρυπτογραφημένα δεδομένα τα οποία είναι διαθέσιμα.

2.1.4 Στόχοι της Διαχείρισης Κλειδιών

Η διαχείριση των κλειδιών παίζει έναν σημαντικότατο ρόλο στην Κρυπτογραφία καθώς αποτελεί την βάση για ασφαλείς κρυπτογραφικές τεχνικές που προσφέρουν μυστικότητα (confidentiality), επικύρωση της ταυτότητας μιας οντότητας (entity authentication), επικύρωση της προέλευσης των δεδομένων (data origin authentication), ακεραιότητα των δεδομένων (data integrity) και βέβαια ψηφιακές υπογραφές. Ο στόχος ενός καλού κρυπτογραφικού συστήματος είναι να μειώσει στο ελάχιστο τα πολύπλοκα προβλήματα του ελέγχου ενός μεγάλου αριθμού οντοτήτων, συγκεντρώνοντας την επιτήρησή του σε ένα μικρό πλήθος στοιχείων, τα οποία είναι εύκολα ελεγχόμενα. Με τον τρόπο αυτό διατηρεί αναλλοίωτες τις σχέσεις μεταξύ των οντοτήτων όσο αφορά τα κλειδιά.

Πιο συγκεκριμένα, ένα κρυπτοσύστημα πρέπει να προστατεύει την μυστικότητα των κλειδιών που πρέπει να παραμένουν γνωστά μόνο στους κατόχους τους. Αυτά είναι τασυμμετρικά κλειδιά και τα ιδιωτικά ασύμμετρα κλειδιά. Επίσης πρέπει να προστατεύει τα κλειδιά από την αλλοίωση του παράγοντα authentication,. Δηλαδή, τα κλειδιά πρέπει να παραμένουν μοναδικώς συνδεόμενα με την ταυτότητα του κατόχου τους και η χρήση τους, στην περίπτωση των ιδιωτικών κλειδιών, να επιτρέπεται μόνο από αυτόν. Το τελευταίο αυτό σημείο είναι πολύ σημαντικό για ένα κρυπτοσύστημα, καθώς η χρήση των κλειδιών υπάγεται σε κάποιους κανόνες οι οποίοι πρέπει να ακολουθώνται αυστηρά. Δεν επιτρέπεται, για παράδειγμα κάποιος να δημιουργήσει με αθέμιτο τρόπο και να χρησιμοποιήσει το ιδιωτικό κλειδί κάποιου τρίτου, όπως και να χρησιμοποιήσει κάποιος ένα κλειδί που έχει λήξει το χρονικό διάστημα μέσα στο οποίο μπορεί να χρησιμοποιηθεί.

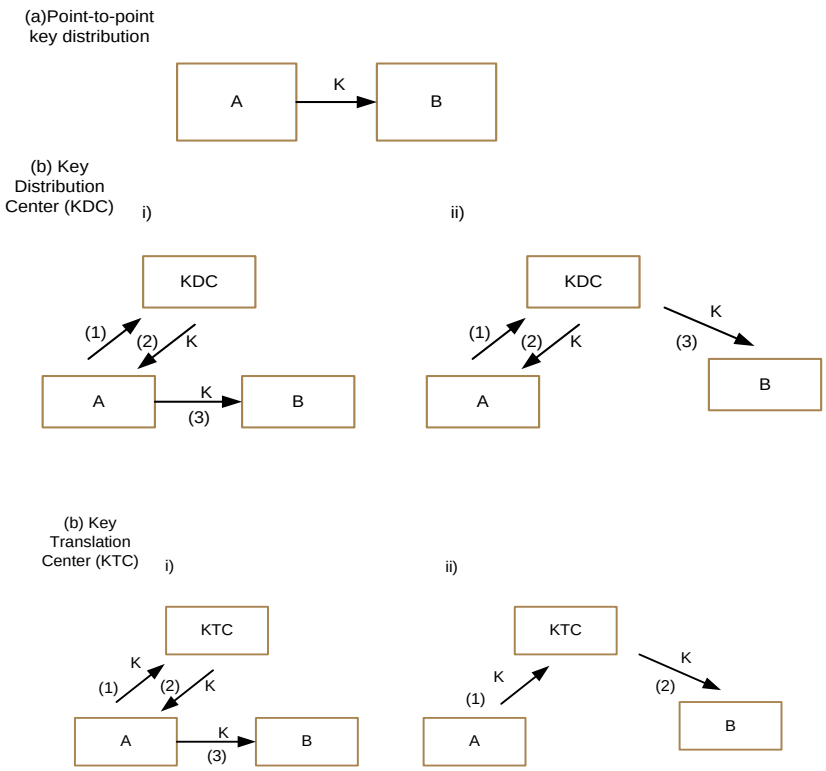
2.2 Ο ΡΟΛΟΣ ΤΩΝ TTPs (TRUSTED THIRD PARTIES)

Τα TTPs είναι απαραίτητα στοιχεία ενός ασφαλούς κρυπτογραφικού συστήματος. Ένα trusted third party είναι μία οντότητα στην οποία οι χρήστες ενός μεγάλου δικτύου εμπιστεύονται την διαχείριση των κλειδιών τους, ώστε να καθίσταται δυνατή η ασφαλής επικοινωνία μεταξύ τους. Οι ευθύνες και οι υποχρεώσεις που έχει αυτή η οντότητα σε ένα σύστημα είναι αυστηρά καθορισμένες. Βέβαια, η μορφή ενός trusted third party σε ένα συμμετρικό σύστημα κρυπτογραφίας παρουσιάζει μεγάλες διαφορές σε σχέση με αυτό ενός ασύμμετρου συστήματος. Στη συνέχεια θα αναφερθούμε ξεχωριστά για τις δύο αυτές κατηγορίες.

2.2.1 Trusted Third Party σε Δίκτυο Συμμετρικής Κρυπτογραφίας

Ας υποθέσουμε ότι έχουμε ένα δίκτυο που χρησιμοποιεί τεχνικές συμμετρικού κλειδιού με *n* πλήθος χρηστών. Αν ο κάθε χρήστης θέλει να επικοινωνήσει ξεχωριστά με τους υπόλοιπους τότε το συνολικό πλήθος των κλειδιών που θα χρειαστούν είναι *n(n-1)/2,* εφόσον κάθε ζεύγος χρηστών θα πρέπει να μοιράζεται ένα κοινό μυστικό κλειδί. Προκύπτει συνεπώς ένα σοβαρό πρόβλημα διαχείρισης των κλειδιών αφού ο αριθμός των κλειδιών είναι πολύ μεγάλος, και όσο προστίθενται νέοι χρήστες στο σύστημα ο αριθμός αυτός θα αυξάνεται συνεχώς. Οι χρήστες σε ένα τέτοιο σενάριο θα ήταν πολύ δύσκολο να αποθηκεύσουν και να διαχειριστούν τόσα πολλά κλειδιά. Το πρόβλημα αυτό λύνεται με την προσθήκη ενός κεντρικού διακομιστή κλειδιών (key server), ο οποίος αναλαμβάνει τον ρόλο ενός trusted third party. Έτσι έχουμε μία κεντρική διαχείριση κλειδιών (centralized key management).

Στο ακόλουθο σχήμα παρουσιάζονται τρία απλοποιημένα μοντέλα επικοινωνίας συμμετρικού κλειδιού, όπου K είναι το κλειδί.



Σχήμα 2.2 Μοντέλα Key Distribution (symmetric key)

Το πρώτο σχήμα, βέβαια, παρουσιάζει το πιο απλό μοντέλο, το οποίο είναι μία επικοινωνία σημείου προς σημείο (point-to-point), χωρίς να παρεμβάλλεται τίποτα μεταξύ των δύο άκρων. Το δεύτερο σχήμα παρουσιάζει μία επικοινωνία με ένα *κέντρο διανομής κλειδιού (Key Distribution Center).* Στην περίπτωση αυτή τα κέντρα αυτά (KDC) έχουν την υποχρέωση να διανέμουν νέα κλειδιά (session keys) για κάθε επικοινωνία των χρηστών. Ο κάθε χρήστης, στο μοντέλο αυτό, μοιράζεται το ίδιο μυστικό κλειδί με το KDC, το οποίο, στη συνέχεια, το χρησιμοποιεί για να κρυπτογραφήσει το νέο session κλειδί και να το στείλει στους χρήστες. Το τρίτο διάγραμμα παρουσιάζει μία επικοινωνία με *κέντρο μετάφρασης κλειδιού (Key Translation Center).* Η διαφορά του με το προηγούμενο μοντέλο είναι ότι αυτή την φορά το session key το παρέχει η μία από τις δύο πλευρές που θέλουν να επικοινωνήσουν και όχι το κέντρο KTC.

Παρατηρεί κανείς ότι το μοντέλο με KDC παρέχει κεντρικοποιημένη δημιουργία κλειδιών ενώ το μοντέλο με KTC παρέχει κατανεμημένη δημιουργία κλειδιών.

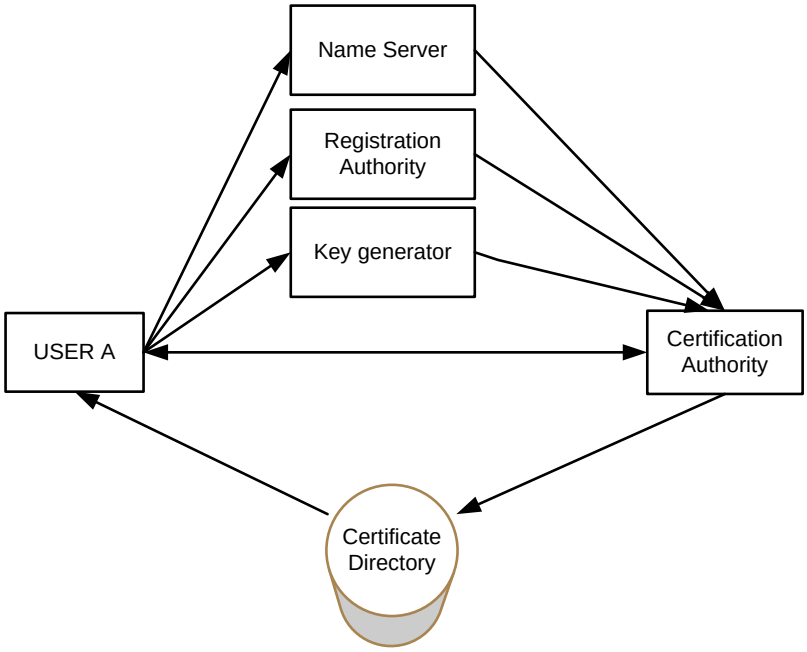
Επίσης, στην επικοινωνία point-to-point, είναι αναγκαίο ο κάθε χρήστης να μοιράζεται a priori ένα κοινό μυστικό κλειδί με τον συνομιλούντα χρήστη. Στην περίπτωση, όμως, του κεντρικοποιημένου key management, υπάρχει ένα trusted third party που όλοι εμπιστεύονται τυφλά και προϋποθέτει ότι κάθε μέλος του δικτύου μοιράζεται με αυτό ένα κοινό μυστικό κλειδί. Αυτή η κεντρικοποιημένη δομή παρέχει το πλεονέκτημα ότι τα κλειδιά, μπορούν να αποθηκεύονται πολύ αποδοτικά από τους χρήστες. Ο κάθε χρήστης, συνεπώς, πρέπει να διατηρεί μόνο ένα μυστικό κλειδί με το trusted third party, το οποίο, μάλιστα, έχει μεγάλη διάρκεια ζωής.

Τα κεντρικοποιημένα αυτά μοντέλα παρουσιάζουν, βέβαια, και κάποια μειονεκτήματα για τα οποία πρέπει να γίνει λόγος. Σε περίπτωση που γίνει επίθεση από κάποιο κακόβουλο στον κεντρικό κόμβο, διακυνδυνεύει η ασφάλεια όλου του συστήματος. Επίσης, αν τεθεί εκτός λειτουργίας ο κόμβος αυτός τότε όλες οι υπηρεσίες καταρρέουν και οι χρήστες αδυνατούν να επικοινωνήσουν μεταξύ τους με ασφάλεια. Τέλος, θα πρέπει να σημειωθεί ότι τα μοντέλα αυτά προϋποθέτουν ότι ο κεντρικός αυτός κόμβος είναι συνέχεια σε λειτουργία (on-line), γεγονός που επιβαρύνει την απόδοση του συστήματος.

2.2.2 Trusted Third Party σε Δίκτυο Κρυπτογραφίας Δημόσιου Κλειδιού

Το μοντέλο ενός δικτύου που χρησιμοποιεί κρυπτογραφία δημοσίου κλειδιού και ψηφιακά πιστοποιητικά ονομάζεται *PKI (Public Key Infrastructure)*. Μία δομή PKI αποτελείται από πρωτόκολλα, υπηρεσίες, και πρότυπα που υποστηρίζουν εφαρμογές της κρυπτογραφίας δημοσίου κλειδιού. Στο σημείο αυτό θα αναφερθούμε σε trusted third parties που είναι απαραίτητες σε μια τέτοια δομή (ενδελεχής ανάλυση του PKI γίνεται σε επόμενο κεφάλαιο).

Στο σχήμα 2.3 παρουσιάζονται οι βασικές υπηρεσίες που πρέπει να παρέχονται από εμπιστευόμενες τρίτες οντότητες (trusted third parties) και πως συνδέονται μεταξύ τους.



Σχήμα 2.3 Third party services

Η πιο σημαντική οντότητα είναι η *Αρχή Πιστοποίησης (Certification Authority).* Η αρχή αυτή είναι υπεύθυνη για την πιστοποίηση της αυθεντικότητας των κλειδιών του συστήματος. Για να το πετύχει αυτό δημιουργεί ψηφιακά πιστοποιητικά που συνδέουν μοναδικά την ταυτότητα ενός χρήστη με το δημόσιο κλειδί του, διαχειρίζεται τους σειριακούς αριθμούς των πιστοποιητικών και επικαλείται την ανάκλησή τους, όταν συντρέχουν συγκεκριμένες καταστάσεις. Η οντότητα του *διακομιστή ονοματοδοσίας (name server)* δημιουργεί και διαχειρίζεται τα ονόματα που χρησιμοποιούν οι χρήστες μέσα στο δίκτυο, τα οποία είναι μοναδικά για κάθε χρήστη. Επίσης, σημαντικός είναι ο ρόλος της *Αρχής Εγγραφής (Registration Authority).* Αποτελεί ουσιαστικά την διεπαφή μεταξύ του χρήστη και της αρχής πιστοποίησης, καθώς είναι υπεύθυνη για την πιστοποίηση της ταυτότητας των χρηστών για λογαριασμό της αρχής πιστοποίησης. Επίσης μεταφέρει τα ψηφιακά πιστοποιητικά για λογαριασμό της αρχής πιστοποίησης στους χρήστες.

Η *γεννήτρια κλειδιών (key generator)* δημιουργεί τα ζεύγη δημόσιου-ιδιωτικού κλειδιού, τα συμμετρικά μυστικά κλειδιά ή τους κωδικούς ασφαλείας (passwords). Η οντότητα αυτή μπορεί, να είναι ανεξάρτητη ή να αποτελεί μέρος της

αρχιτεκτονικής του χρήστη ή της Αρχής Πιστοποίησης (Certification Authority). Τέλος, υπάρχει και μία δομή η οποία χρησιμεύει ως βάση δεδομένων για τα πιστοποιητικά και ονομάζεται αρχείο πιστοποιητικών (certificate directory). Λειτουργεί ως διακομιστής πρόσβασης μόνο για ανάγνωση(read-access server), ώστε οι χρήστες να βρίσκουν τα πιστοποιητικά που τους ενδιαφέρουν, και τα πιστοποιητικά ανανεώνονται από την Αρχή Πιστοποίησης (CA).

2.3 ΣΥΓΚΡΙΣΗ ΤΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΛΕΙΔΙΩΝ ΜΕ ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ Ή ΣΥΜΜΕΤΡΙΚΟΥ ΚΛΕΙΔΙΟΥ

Η επιλογή ανάμεσα σε κρυπτογραφία δημόσιου και συμμετρικού κλειδιού για ένα πρωτόκολο, εξαρτάται κυρίως από τις απαιτήσεις ασφάλειας που πρέπει να εξασφαλίζονται στο δίκτυο. Οι σύγχρονες εφαρμογές key management υλοποιούν κυρίως υβριδικά πρωτόκολα, τα οποία χρησιμοποιούν τεχνικές ασύμμετρης και συμμετρικής κρυπτογραφίας. Αυτό συμβαίνει ώστε οι εφαρμογές αυτές να εκμεταλλεύονται παράλληλα τα πλεονεκτήματα και των δύο μεθόδων κρυπτογραφίας. Η πιο αποδοτική επιλογή είναι να επιλεχθούν τεχνικές συμμετρικής κρυπτογραφίας για την κρυπτογράφηση των δεδομένων και την εξασφάλιση της ακεραιότητας τους, και τεχνικές δημοσίου κλειδιού για τις ψηφιακές υπογραφές και το key management που προσφέρουν.

Πέρα όμως από την πρακτική θεώρηση, αν συγκρίνει κάποιος μεταξύ τους τις δύο τεχνικές κρυπτογραφίας, σε σχέση με το key management που προσφέρουν, μπορεί εύκολα να παρατηρήσει ότι οι τεχνικές δημοσίου κλειδιού παρουσιάζουν κάποια πλεονεκτήματα έναντι των συμμετρικών. Πρωταρχικά, προσφέρουν ένα

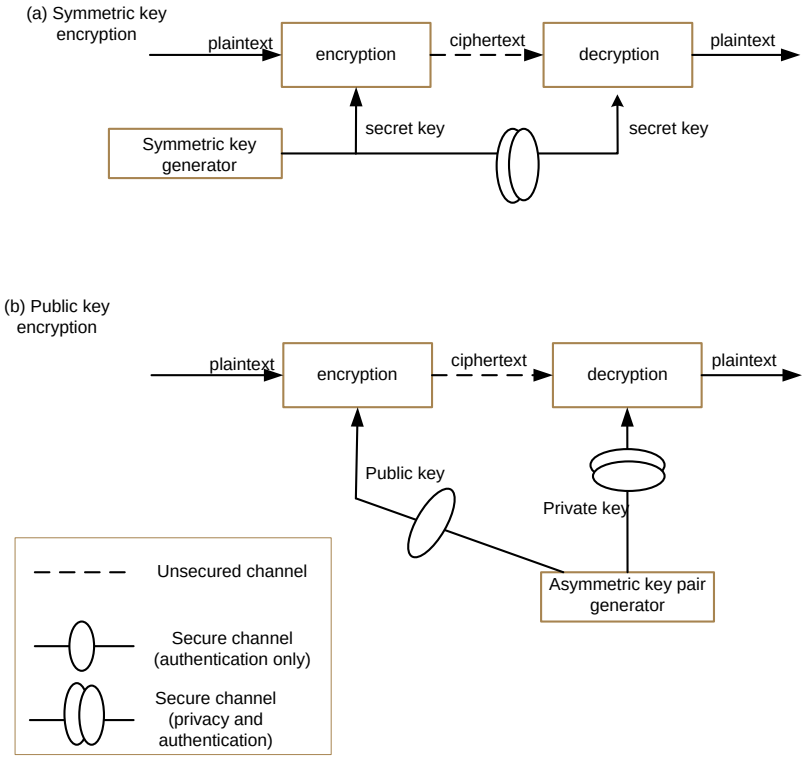
απλοποιημένο σύστημα διαχείρισης των κλειδιών. Αυτό εξηγείται από το γεγονός ότι, για να κρυπτογραφήσει κάποιος ένα μήνυμα, απαιτείται μόνο η γνώση του δημόσιου κλειδιού του παραλήπτη. Συνεπώς ο παράγοντας της μυστικότητας του κλειδιού, που απαιτείται στην περίπτωση συμμετρικής κρυπτογραφίας, δεν υπάρχει και απομένει μόνο ο έλεγχος για την πιστοποίηση της αυθεντικότητας του κλειδιού (authentication). Ο ακόλουθος πίνακας παρουσιάζει συνοπτικά τις προδιαγραφές ασφάλειας που υποστηρίζουν τα κλειδιά της συμμετρικής και ασύμμετρης κρυπτογραφίας.

	Συμμετρικά κλειδιά		Ασύμμετρα κλειδιά	
	Μυστικότητα (Secrecy)	Αυθεντικότητα (Authenticity)	Μυστικότητα (Secrecy)	Αυθεντικότητα (Authenticity)
Κλειδί Κρυπτογράφησης (Encryption key)	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
Κλειδί Αποκρυπτογράφησης (Decryption key)	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ

Πινακας 2.2 Προδιαγραφές Ασφάλειας συμμετρικής και ασύμμετρης κρυπτογραφίας

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, σε δίκτυο με συμμετρική κρυπτογραφία, είναι αναγκαία η ύπαρξη ενός on-line εμπιστευόμενου server, ο οποίος διανέμει στους χρήστες τα κλειδιά τα οποία είναι αναγκαία για την επικοινωνία τους. Στην περίπτωση όμως που έχουμε ασύμμετρη κρυπτογραφία, ο εξυπηρετητής αυτός μπορεί να αντικατασταθεί από έναν ο οποίος είναι off-line. Αυτό το γεγονός αποτελεί πλεονέκτημα γιατί το δίκτυο καθίσταται επεκτάσιμο και μπορεί να υποστηρίξει μεγάλο αριθμό χρηστών.

Τέλος, ένα ακόμη πλεονέκτημα των ασύμμετρων έναντι των συμμετρικών τεχνικών, είναι ότι παρέχουν την απαραίτητη λειτουργικότητα με πολύ μικρότερο κόστος, καθώς εκπληρώνουν απαιτήσεις όπως non-repudiation, με τις ψηφιακές υπογραφές, και αυθεντικότητα προέλευσης δεδομένων (data origin authentication). Αντίθετα, σε συστήματα με συμμετρικά κλειδιά, η επίτευξη αυτών των στόχων θα απαιτούσε επιπλέον εγκατάσταση κάποιων trusted third parties και υλικού ασφάλειας. Στην εικόνα 2.5 που ακολουθεί παρουσιάζεται η σύγκριση των δύο τεχνικών όσο αφορά το επίπεδο key management που προσφέρει η κάθε μία.

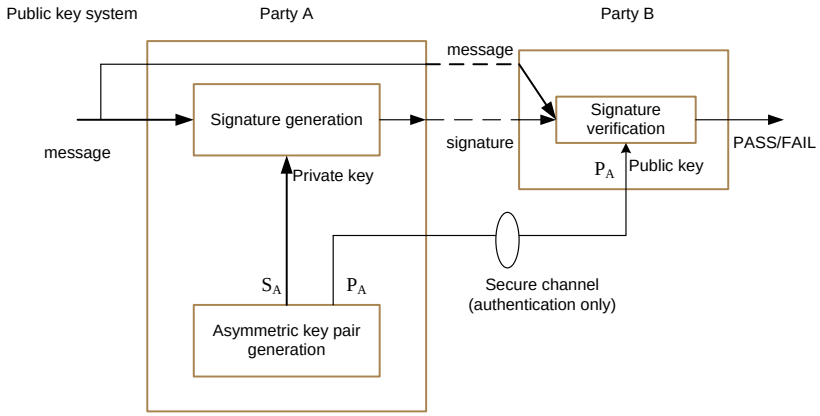


Σχήμα 2.5 Key Management συμμετρικής Κρυπτογραφίας και Κρυπτογραφίας δημοσίου κλειδιού

2.4 ΤΕΧΝΙΚΕΣ ΔΙΑΝΟΜΗΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Σε ένα κρυπτοσύστημα δημοσίου κλειδιού θα πρέπει να εξασφαλίζεται το αίτημα των χρηστών να παραλαμβάνουν τα δημόσια κλειδιά με τρόπο απόλυτα ασφαλή, ώστε να μπορέσουν να ξεκινήσουν μια επικοινωνία. Τα πρωτόκολλα που υλοποιούν κρυπτογραφία δημόσιου κλειδιού συνηθίζεται να περιγράφονται έχοντας εξασφαλισμένο το παραπάνω αίτημα. Αυτό δίνει την δυνατότητα να σχεδιαστούν πολλές εναλλακτικές μέθοδοι διανομής των δημόσιων κλειδιών [1].

Η πιο απλή από αυτές είναι η από *άκρο-σε-άκρο μετάδοση* (point-to-point delivery) του δημόσιου κλειδιού πάνω από ένα κανάλι επικοινωνίας που εμπιστεύονται οι χρήστες. Το κανάλι μπορεί να μεταφραστεί σε μία χέρι με χέρι ανταλλαγή του κλειδιού (άμεση φυσική επαφή), ή σε αποστολή του μέσω courier, και πρέπει να εξασφαλίζει την ακεραιότητα και την αυθεντικότητα των δεδομένων. Πολύ πιθανό βέβαια είναι το γεγονός το κανάλι της μετάδοσης να είναι μία μη έμπιστη ηλεκτρονική γραμμή Στην περίπτωση αυτή πρέπει να μεταδοθούν δεδομένα τα οποία πιστοποιούν την αυθεντικότητα του κλειδιού. Τα επιπλέον δεδομένα συνήθως είναι ένα message digest από μία hash συνάρτηση. Υπάρχουν, βέβαια, κάποια μειονεκτήματα απο την χρήση της παραπάνω μεθόδου, εκ των οποίων τα σημαντικότερα είναι η απώλεια σημαντικού χρόνου λόγω καθυστέρησης και το κόστος ενός απολύτως ασφαλούς καναλιού επικοινωνίας. Η συγκεκριμένη μέθοδος παρουσιάζεται σχηματικά στην εικόνα 2.6.



Εικόνα 2.6 Key Management σε κρυπτοσύστημα χωρίς TTP's

Μια άλλη περίπτωση διανομής κλειδιού είναι η άμεση πρόσβαση των χρηστών σε μία δομή δεδομένων που έχουν καταχωρηθεί τα δημόσια κλειδιά (public key registry). Η δομή αυτή είναι συνήθως υπό τον έλεγχο μιας trusted third party οντότητας (πχ CA) και σχεδιάζεται με τέτοιο τρόπο ώστε να περιέχει το όνομα και το αυθεντικό δημόσιο κλειδί για κάθε χρήστη (το ψηφιακό πιστοποιητικό προσφέρεται για τον παραπάνω σχεδιασμό). Οι χρήστες παραλαμβάνουν τα κλειδιά άμεσα από αυτή την δομή, χωρίς να παρεμβάλλεται καμία άλλη οντότητα.

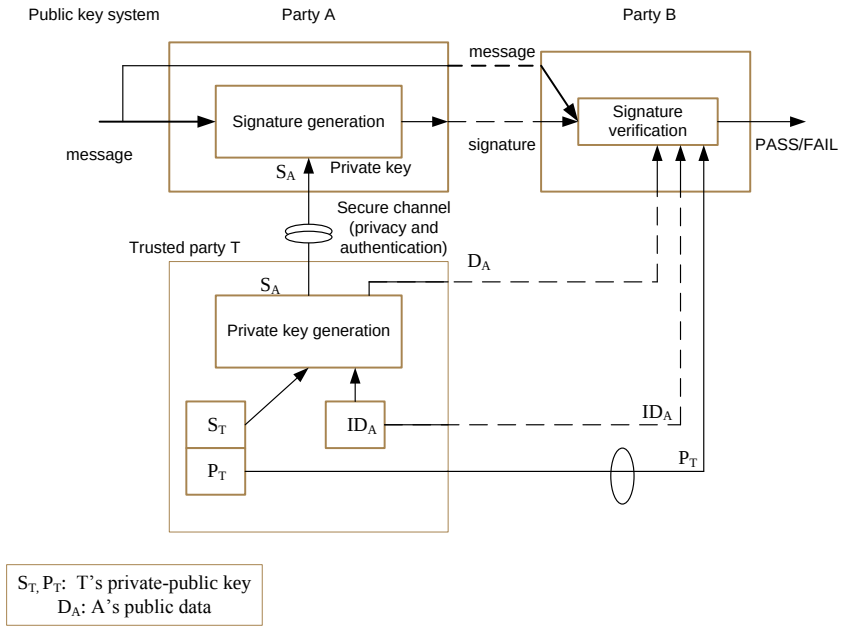
Μια παραλλαγή της παραπάνω μεθόδου είναι η χρήση ενός on-line διακομιστή, τον οποίο εμπιστεύονται οι χρήστες (on-line trusted server). Ο διακομιστής αυτός δέχεται αιτήσεις από τους χρήστες και τους στέλνει τα κλειδιά, διαχειριζόμενος μία δομή όμοια με αυτή που περιγράφηκε προηγουμένως. Βέβαια, για να εξασφαλιστεί η ασφαλής μετάδοση, ο διακομιστήςυπογράφει τα δεδομένα που αποστέλει και ο παραλήπτης κάνει την επιβεβαίωσηαυτών. Δύο δυσκολίες που πρέπει να αντιμετωπιστούν σε αυτό το σενάριο είναι :

α) το γεγονός ότι ο διακομιστής πρέπει να είναι συνεχώς on-line για να εξυπηρετεί τους χρήστες

β) υπάρχει πιθναότητα το σύστημα να υπερχειλίσει από αιτήσεις και ο διακομιστής να τις εξυπηρετεί με μεγάλη καθυστέρηση (φαινόμενο bottleneck)

Τέλος, το πιο αποδοτικό σενάριο διανομής κλειδιών είναι αυτό που περιλαμβάνει μία trusted third party οντότητα, η οποία είναι off-line και ονομάζεται Αρχή Πιστοποίησης (Certification Authority) και τα ψηφιακά πιστοποιητικά. Ο κάθε

χρήστης επικοινωνεί με την CA, η οποία καταχωρεί το δημόσιο κλειδί του δημιουργώντας ένα ψηφιακό πιστοποιητικό. Ο χρήστης λαμβάνει το πιστοποιητικό και το επικυρώνει επιβεβαιώνοντας την ψηφιακή υπογραφή που έχει συμπεριλάβει σε αυτό, ηΑρχή Πιστοποίησης. Συνεπώς οι χρήστες παίρνουν τα δημόσια κλειδιά που τους ενδιαφέρουν ανταλλάσσοντας ψηφιακά πιστοποιητικά μεταξύ τους. Στην εικόνα 2.7 παρουσιάζεται σχηματικά αυτό το σενάριο. Πάνω σε αυτό το σενάριο έχει βασιστεί εξ'ολοκλήρου η αρχιτεκτονική του PKI (Public Key Infrastructure), η οποία έχει εξαπλωθεί σήμερα στα δίκτυα [3]. Αναφερόμαστε σε αυτή αναλυτικά στο επόμενο κεφάλαιο.



Σχημα 2.7 Key Management με trusted third parties

ΚΕΦΑΛΑΙΟ 3: ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΙΚΤΥΟΥ ΜΕ ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ- PUBLIC KEY INFRASTRUCTURE

3.1 ΓΕΝΙΚΗ ΠΕΡΙΓΡΑΦΗ ΤΟΥ PUBLIC KEY INFRASTRUCTURE

Το Public Key Infrastructure είναι μία δομή που αποτελείται από πρωτόκολλα, υπηρεσίες, και πρότυπα που υποστηρίζουν εφαρμογές της κρυπτογραφίας δημοσίου κλειδιού. Ο ρόλος του είναι να διαχειρίζεται δημόσια κλειδιά με την χρήση ψηφιακών πιστοποιητικών και να προσφέρει την ομαλή λειτουργία και επικοινωνία μεταξύ των οντοτήτων που το απαρτίζουν. Ένα PKI εκδίδει, διαχειρίζεται και ανακαλεί πιστοποιητικά δημοσίου κλειδιού, τα οποία περιέχουν ψηφιακές υπογραφές, επιτρέποντας σε απομακρυσμένες οντότητες να πιστοποιούν την αυθεντικότητα, η μία της άλλης. Είναι, συνεπώς, αυτονόητο ότι μία δομή PKI πρέπει να παρέχει τις απαραίτητες προυποθέσεις για την έκδοση νόμιμων ψηφιακών πιστοποιητικών δημοσίου κλειδιού.

Ο κύριος στόχος είναι ο σχεδιασμός μιας δομής η οποία να επιτρέπει στους χρήστες να καθιερώνουν πιστοποιημένες «διαδρομές» (certification paths), οι οποίες περιλαμβάνουν πάνω από ένα δημόσιο κλειδί. Η δημιουργία των «διαδρομών» αυτών, οι οποίες ονομάζονται αλυσίδες εμπιστοσύνης, επαφίεται στις Αρχές Πιστοποίησης (Certification Authorities). Η αλυσίδα αυτή είναι, ουσιαστικά, μία σειρά διαδοχικών CAs, οι οποίες έχουν ως υποχρέωση την δημιουργία, αρχειοθέτηση και ανάκληση των ψηφιακών πιστοποιητικών.

Μία αρχικτεκτονική PKI έχει πολλά επίπεδα εμπιστοσύνης ανάμεσα στις οντότητες που την αποτελούν (levels of trust). Σε ένα ιεραρχικό μοντέλο, το μέγιστο επίπεδο εμπιστοσύνης κατέχει ένα root CA, τον οποίο εμπιστεύονται όλοι οι υπόλοιποι κόμβοι της δομής. Η εμπιστοσύνη μεταβιβάζεται από την ριζική Αρχή Πιστοποίησης (root CA) στις κατώτερης βαθμίδας CAs, τις οποίες πιστοποιεί.

Πιο συγκεκριμένα, οι CAs πιστοποιούν την ταυτότητα μιας οντότητας (ένα μοναδικό όνομα για κάθε μία) και το δημόσιο κλειδί της. Επίσης εκτελούν διαδικασίες πιστοποίησης των χρηστών (user authentication) και είναι υπεύθυνες να

κρατούν το δημόσιο κλειδί με το αντίστοιχο όνομα του κάθε χρήστη. Είναι, συνεπώς αυτονόητο το γεγονός ότι μια CA πρέπει να είναι εμπιστευόμενη οντότητα, η οποία πιστοποιεί δημόσια κλειδιά, δημιουργεί πιστοποιητικά αυτών τα οποία τα διανέμει και, τέλος, διανέμει *Λίστες Ανάκλησης Πιστοποιητικών (Certificate Revocation Lists)*.

Η αρχιτεκτονική ενός συστήματος PKI απαρτίζεται από ένα σύνολο κανόνων οι οποίοι μπορεί να προσαρμόζονται αναλόγως με τις σχέσεις εμπιστοσύνης που θέλει κάποιος να εγκαθιδρύσει σε ένα δίκτυο. Σήμερα δεν υπάρχει ένας επικρατών σχεδιασμός PKI, αλλά ένας συνδυασμός πολλών, που ο καθένας υπακούει σε διαφορετικές πολιτικές ασφάλειας και εμπιστοσύνης. Είναι, συνεπώς, αποδεκτές πολλές Αρχές Πιστοποίησης ταυτόχρονα σαν root CAs, και όχι μία μοναδική. Υπάρχει ένα παγκόσμιο PKI, το οποίο διαχωρίζεται σε επιμέρους δίκτυα PKI (παρόμοια με τα WAN της δεκαετίας του ‘80) με διαφορετικά επίπεδα εμπιστοσύνης και profiles χρηστών.

Συνοπτικά, μπορούμε να πούμε ότι ο στόχος μίας αρχιτεκτονικής PKI είναι η διασφάλιση απαιτήσεων ασφάλειας όπως η πιστοποίηση η ταυτότητα (identification), η πιστοποίηση της αυθεντικότητας (authentification) και του ελέγχου πρόσβασης στα δεδομένα (access control).

3.2 ΕΠΙΠΕΔΑ ΕΜΠΙΣΤΟΣΥΝΗΣ ΣΕ ΕΝΑ PKI ΣΥΣΤΗΜΑ

Προτού αρχίσουμε να αναλύουμε τους λειτουργικούς ρόλους και την πολιτική των οντοτήτων που αποτελούν ένα PKI σύστημα, θα αναφερθούμε στα μοντέλα εμπιστοσύνης που χαρακτηρίζουν ένα τέτοιο σύστημα. Υπάρχουν πολλοί τρόποι για να καθοριστούν και να εφαρμοσθούν οι σχέσεις εμπιστοσύνης ανάμεσα στις Αρχές Πιστοποίησης (CAs) ενός κρυπτοσυστήματος δημοσίου κλειδιού. Ο σχεδιασμός ενός τέτοιου δικτύου σχέσεων ονομάζεται *μοντέλο εμπιστοσύνης (trust model)* ή *τοπολογία πιστοποίησης (certification topology)*. Οι σχέσεις αυτές καθορίζονται από ένα σύνολο κανόνων, σύμφωνα με τους οποίους υποδεικνύεται ο τρόπος που μπορεί ένα πιστοποιητικό, που έχει εκδοθεί από μια CA, να χρησιμοποιηθεί και να επικυρωθεί από οντότητες οι οποίες ανήκουν σε χώρους αρμοδιότητας άλλων CAs.

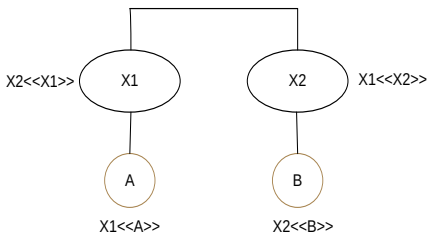
Αρχικά, όμως, πρέπει να αναφερθούμε στη σημαντική έννοια των αλυσίδων από πιστοποιητικά (certificate chains), προτού προχωρήσουμε σε ανάλυση των διαφόρων trust models.

3.2.1 Αλυσίδες Πιστοποιητικών (Certificate chains) – Διαδρομή Πιστοποίησης (Certification Path) – Cross Certification

Για να πάρει ένας χρήστης Α το αυθεντικό δημόσιο κλειδί μιας άλλης οντότητας Β πρέπει να έχει στην κατοχή του ένα πιστοποιημένο αντίγραφο του δημοσίου κλειδιού της CA. Με το δημόσιο κλειδί της CA μπορεί να επικυρώσει την υπογραφή που περιέχει το πιστοποιητικό που έχει εκδόσει η CA για το δημόσιο κλειδί του Β. Στην περίπτωση πολλών Αρχών Πιστοποίησης CAs, ο χρήστης μπορεί να βρεθεί σε κατάσταση να θέλει να πάρει ένα πιστοποιημένο δημόσιο κλειδί μιας οντότητας, η οποία δεν πιστοποιείται από την CA που ο ίδιος εμπιστεύεται. Τότε θα πρέπει να δημιουργήσει μία αλυσίδα πιστοποιητικών (certificate chain) που αρχίζει από το δημόσιο κλειδί της CA που ο ίδιος εμπιστεύεται και καταλήγει στο δημόσιο κλειδί που θέλει να πάρει. Ο στόχος του, λοιπόν, είναι να βρει μία διαδοχή πιστοποιητικών που αντιστοιχούν σε μία κατευθυνόμενη διαδρομή (certification path), η οποία αρχίζει από τον κόμβο τη; CA, το δημόσιο κλειδί της οποίου ο χρήστης εμπιστεύεται a priori, και καταλήγει στην CA, η οποία έχει υπογράψει το πιστοποιητικό του δημόσιου κλειδιού που ο χρήστης θέλει να πάρει.

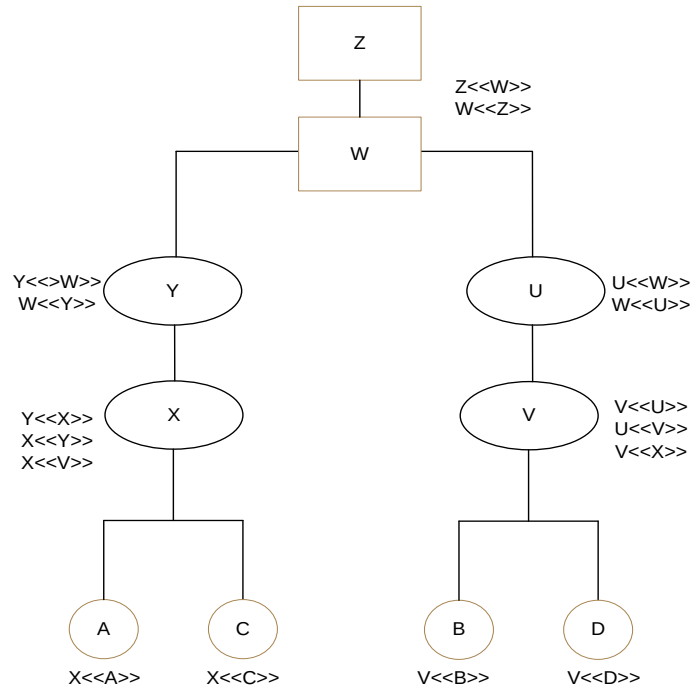
Θα προσπαθήσουμε να περιγράψουμε κάποια σενάρια certification chains με διαγραμματικό τρόπο. Ας υποθέσουμε ότι υπάρχουν δύο χρήστες Α και Β και ότι το πιστοποιητικό συμβολίζεται ως εξής :

$X << A >>$, το οποίο σημαίνει ότι το πιστοποιητικό του Α εκδόθηκε από την Αρχή Πιστοποίησης X. Στην εικόνα 3.1 παρουσιάζεται ένα δίκτυο, όπου X_1 και X_2 είναι δύο CAs.



Σχήμα 3.1 Μοντέλο ιεραρχίας X.509 πιστοποιητικών

Ο χρήστης *A* χρησιμοποιεί μία αλυσίδα πιστοποιητικών για να πάρει το δημόσιο κλειδί του χρήστη *B*. Η αλυσίδα αυτή είναι της μορφής: $X_1 <<X_2>> X_2 <<B>>$. Αντίστοιχα, για να πάρει ο *B* το δημόσιο κλειδί του *A,* η αλυσίδα θα είναι : $X_2 <<X_1>> X_1 <<A>>$. Η ίδια λογική μπορεί να εμφανίζεται και σε τοπολογίες που έχουν περισσότερες από δύο CAs. Είναι, βέβαια, υποχρεωτικό το γεγονός ότι κάθε CA πρέπει να διατηρεί ένα αρχείο με τα πιστοποιητικά που την συνδέουν με σχέσεις εμπιστοσύνης με τις άλλες CAs. Με τον τρόπο αυτό ο χρήστης θα μπορεί να δημιουργεί ένα certificate path που θα τον οδηγεί στο πιστοποιητικό του χρήστη, το κλειδί του οποίου θέλει να λάβει. Στην εικόνα 3.2 παρουσιάζεται μία ιεραρχία από CAs. Στα κουτιά, δίπλα από τις CAs (οι οποίεςβρίσκονται μέσα στους ελλειπτικούς κύκλους) βρίσκονται τα πιστοποιητικά που βεβαιώνουν τις σχέσεις εμπιστοσύνης ανάμεσά τους (πχ το ζεύγος $\{X <<Y>>, Y <<X>>\}$). Ένα τέτοιο ζεύγος, το οποίο επιτρέπει σε ένα χρήστη τη δημιουργία certification path και προς τις δύο κατευθύνσεις, ονομάζεται cross-certificate pair. Στο ίδιο σχήμα, οι χρήστες παρουσιάζονται μέσα σε τέσσερις κύκλους.

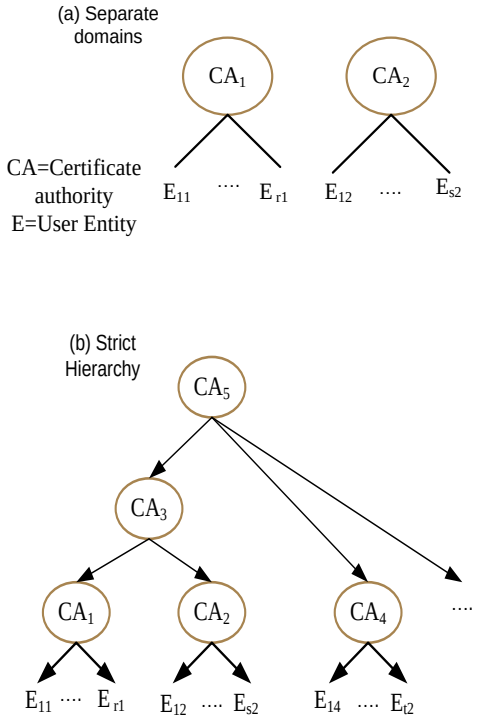


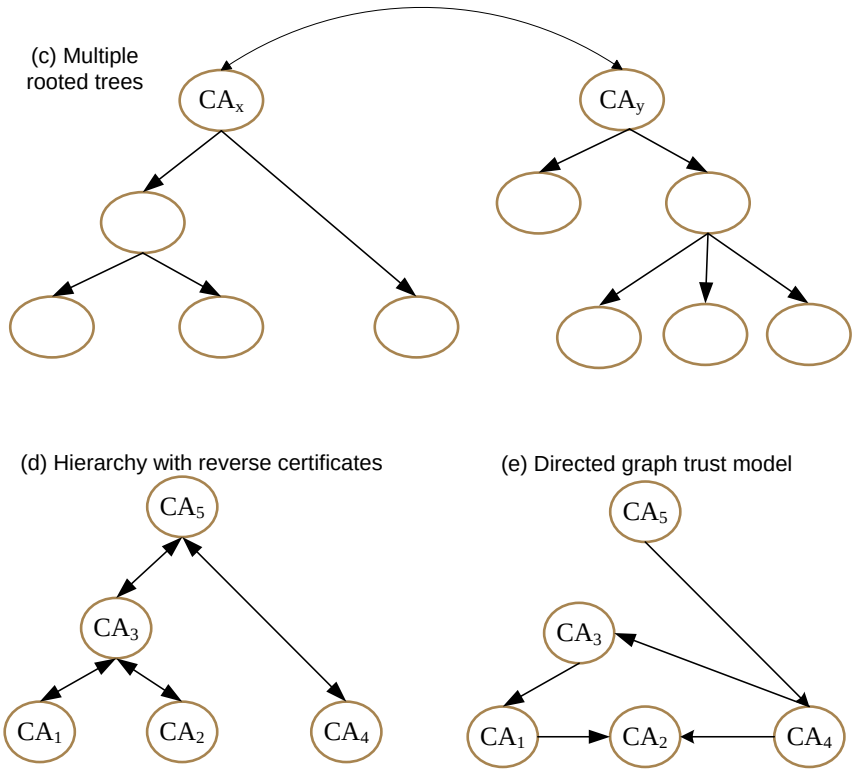
Σχήμα 3.2 Μοντέλο ιεραρχίας X.509 πιστοποιητικών

Συνεπώς, ο Α, για να πάρει το δημόσιο κλειδί του Β, θα ακολουθήσει την εξής διαδρομή πιστοποιητικών : *X <<Y>>, Y <<W>>,W <<U>>,U <<V>>,V <<B>>*. Μόλις ο Α λάβει τα πιστοποιητικά αυτά, θα κάνει ένα αλυσιδωτό verification, κάθε φορά με το προηγούμενο δημόσιο κλειδί της αλυσίδας, μέχρι να φτάσει στο δημόσιο κλειδί του Β. Εάν θελήσει να στείλει στον Β υπογεγραμμένα μηνύματα, τότε ο Β πρέπει να πάρει το δημόσιο κλειδί του Α ακολουθώντας το εξής certification path : *V <<U>>, U <<W>>, W <<Y>>, Y <<X>>, X <<A>>*. Ο Β μπορεί να λάβει τα πιστοποιητικά αυτά από τα αποθετήρια των CAs ή να του τα παρέχει ο Α σαν αρχικό μήνυμα.

3.2.2 Περιγραφή σεναρίων για μοντέλα εμπιστοσύνης

Στο ακόλουθο σχήμα παρουσιάζονται διάφορα μοντέλα εμπιστοσύνης που πετυχαίνουν, με διαφορετικό τρόπο το καθένα, πιστοποίηση των οντοτήτων.





Εικόνα 3.3 Trust Models για Πιστοποίηση

Στις περιπτώσεις απλών δικτύων δημοσίου κλειδιού, έχουμε την ύπαρξη μιας μόνο Αρχής Πιστοποίησης (CA). Όταν τα δίκτυα είναι μεγαλύτερα, τότε είναι αναγκαία η ύπαρξη περισσότερων της μιας CA για την εξυπηρέτηση των χρηστών. Στην περίπτωση αυτή, πρέπει να οριστούν αυστηρά οι σχέσεις εμπιστοσύνης μεταξύ των CAs, ώστε οι χρήστες που υπάγονται σε διαφορετικές CAs να μπορούν να επικοινωνήσουν κρυπτογραφικά μεταξύ τους. Θα μπορούσαμε να πούμε ότι δύο διαφορετικές CAs προσδιορίζουν ξεχωριστές περιοχές ασφάλειας (security domains), όπως φαίνεται στο διάγραμμα α) του σχήματος. Οι σχέσεις εμπιστοσύνης ανάμεσά τους είναι ανύπαρκτες και οι χρήστες που ανήκουν στη μια περιοχή δεν μπορούν να πιστοποιήσουν την αυθεντικότητα των πιστοποιητικών που υπάγονται σε μια άλλη. Το σενάριο αυτό, συνεπώς, δεν περιλαμβάνει σχέσεις εμπιστοσύνης μεταξύ διαφορετικών περιοχών και ονομάζεται σενάριο εμπιστοσύνης με ξεχωριστές περιοχές (trust with separate domains).

Η πρώτη λύση που επινοήθηκε για την έλλειψη κρυπτογραφικής διαλειτουργικότητας μεταξύ ξεχωριστών περιοχών είναι αυτή του μοντέλου αυστηρής ιεραρχίας, που απεικονίζεται στο σχήμα 3.3.b. Σε αυτό, κάθε οντότητα έχει αρχικά το δημόσιο κλειδί του κόμβου-ρίζας (πχ. Η οντότητα E_1 έχει το δημόσιο κλειδί του CA_5 , αντί αυτό του CA_1 του σχήματος α)). Αυτό το σενάριο είναι ένα κεντρικοποιημένο μοντέλο εμπιστοσύνης και ονομάζεται *rooted chain model*.

Συνδυάζοντας πολλά τέτοια κεντρικοποιημένα μοντέλα δημιουργείται ένα μοντέλο πολλαπλών ριζών (*multiple rooted model*) , όπως αυτό του σχήματος 3.3.c. Στην περίπτωση αυτή, επιτρέπεται η χρήση cross-certification μεταξύ των ριζών, που συμβολίζεται με ένα βέλος δύο κατευθύνσεων. Συγκεκριμένα, το βέλος που κατευθύνεται από το CA_x στο CA_y συμβολίζει το πιστοποιητικό του δημοσίου κλειδιού του CA_y, το οποίο έχει δημιουργήσει το CA_x. Έτσι οι οντότητες που υπάγονται στο CA_x, μπορούν να συνδέονται με σχέσεις εμπιστοσύνης με τις οντότητες κάτω από το CA_y, χάρη στη σύνδεση των δύο root CAs με πιστοποιητικά. Αντίστοιχα, το ίδιο συμβαίνει και με τις οντότητες που υπάγονται στο CA_y. Θα πρέπει να σημειωθεί ότι σε ένα αυστηρά ιεραρχικό μοντέλο, η κάθε οντότητα ανήκει σε μια μόνο περιοχή (domain), η οποία καθορίζεται από την root CA. Έτσι, στο προηγούμενο παράδειγμα, παρά το γεγονός ότι η CA_1 υπογράφει το πιστοποιητικό του E_1 , ο E_1 εμπιστεύεται άμεσα μόνο την CA_5, η οποία είναι η ρίζα. Αντίθετα, την οντότητα CA_1, ο E_1 την εμπιστεύεται έμμεσα μέσω της ρίζας CA_5.

Αυτό το αυστηρά ιεραρχικό μοντέλο παρουσιάζει κάποια μειονεκτήματα, τα οποία παρατίθενται ακολούθως :

- όλες οι σχέσεις εμπιστοσύνης του συστήματος εξαρτώνται από το root key
- αλυσίδες πιστοποιητικών είναι απαραίτητες ακόμη και στην απλή περίπτωση δύο μόνο οντοτήτων κάτω από ένα CA
- οι αλυσίδες πιστοποιητικών γίνονται πολύ μεγάλες στο μήκος όσο μεγαλώνει το βάθος του δέντρου της ιεραρχίας

Μια λύση για την αντιμετώπιση των παραπάνω μειονεκτημάτων είναι μία παραλλαγή του μοντέλου που εφαρμόστηκε από οργανισμούς και εταιρείες, η οποία υποδεικνύει ότι οι σχέσεις εμπιστοσύνης δεν αρχίζουν από την root CA αλλά από τον τοπικό κόμβο, δηλαδή από την CA η οποία εκδίδει το πιστοποιητικό της οντότητας. Ένα τέτοιο μοντέλο θα αναλύσουμε στην συνέχεια.

3.2.2.1 Μοντέλο ιεραρχίας με αντίστροφα πιστοποιητικά (reverse certificate hierarchy)

Ένα πιο γενικό μοντέλο ιεραρχίας είναι το *μοντέλο ιεραρχίας με αντίστροφα πιστοποιητικά (reverse certificate hierarchy)*, το οποίο παρουσιάζεται στο σχήμα 3.3.d. Το μοντέλο αυτό παρουσιάζει πολλές ομοιότητες με αυτό της αυστηρής ιεραρχίας, με την εξής όμως διαφοροποίηση: κάθε CA η οποία βρίσκεται χαμηλά στην ιεραρχία εκδίδει πιστοποιητικά και για τα δημόσια κλειδιά του αμέσως ανώτερου κόμβου CA, της γονικής CA δηλαδή. Στην περίπτωση αυτή έχουμε δύο τύπους πιστοποητικών, το forward και το reverse certificate. Το forward πιστοποιητικό εκδίδεται από μια CA για πιστοποιήσει το δημόσιο κλειδί μιας CA που είναι αμέσως κατώτερη στην ιεραρχία, ενώ το ακριβώς αντίθετο είναι ένα reverse certificate.

Στο σενάριο αυτό, ο κάθε χρήστης ξεκινά έχοντας το δημόσιο κλειδί της CA που έχει εκδόσει το δικό του πιστοποιητικό και όχι της root CA. Συνεπώς, όλες οι αλυσίδες εμπιστοσύνης ξεκινούν από την κοντινότερη Αρχή Πιστοποίησης σε κάθε οντότητα. Η κοντινότερη διαδρομή πιστοποίησης μεταξύ δύο οντοτήτων A και B, είναι αυτή που ξεκινά από τον κόμβο του A, συνεχίζει προς τα πάνω στο δέντρο μέχρι τον λιγότερο μακρινό κοινό πρόγονο του A και B (least common ancestor), και συνεχίζει την πορεία, προς τα κάτω στο δέντρο, μέχρι τον B. Συμπεραίνουμε λοιπόν πως το σενάριο αυτό είναι πολύ πιο αποδοτικό από εκείνο της αυστηρής ιεραρχίας και μπορεί να υποστηρίξει μεγάλο αριθμό οντοτήτων.

Ένα μειονέκτημα που προκύπτει είναι το γεγονός ότι δημιουργούνται μεγάλες αλυσίδες πιστοποιητικών μεταξύ οντοτήτων που υπάγονται σε διαφορετικά CAs, παρόλο που αυτές μπορεί να επικοινωνούν μεταξύ τους πολύ συχνά (πχ. οι οντότητες CA_1 και CA_4 στο σχήμα 3.3.d). Η κατάσταση αυτή μπορεί να εξομαλυνθεί επιτρέποντας τις δύο οντότητες να αναπτύξουν μεταξύ τους άμεσες σχέσεις πιστοποίησης (cross-certification), χωρίς να επικοινωνούν στο δέντρο της ιεραρχίας. Πάνω στην σκέψη αυτή βασίζεται η πιο ελεύθερη και γενικευμένη ερμηνεία για τις σχέσεις εμπιστοσύνης ενός δικτύου και σχηματικά παρουσιάζεται σαν ένας κατευθυνόμενος γράφος, όπως στο σχήμα 3.3.e. Το μοντέλο αυτό ονομάζεται *μοντέλο εμπιστοσύνης κατευθυνόμενου γράφου (directed graph trust model)*. Οι CAs παρουσιάζονται ως κόμβοι και οι σχέσεις εμπιστοσύνης ως κατευθυνόμενες γραμμές που ενώνουν μεταξύ τους τους κόμβους.

Το μοντέλο αυτό είναι ένα *κατανεμημένο* μοντέλο εμπιστοσύνης, καθώς δεν υπάρχει κανένας κεντρικός κόμβος ή ρίζα, οπότε κάθε CA μπορεί να κάνει πιστοποίηση με cross-certification μια άλλη, και κάθε οντότητα χρήστη ξεκινά έχοντας στην κατοχή της το δημόσιο κλειδί της CA που την πιστοποιεί.

3.3 ΛΕΙΤΟΥΡΓΙΚΟΙ ΡΟΛΟΙ ΤΩΝ ΟΝΤΟΤΗΤΩΝ ΕΝΟΣ PKI ΣΥΣΤΗΜΑΤΟΣ

Στο κεφάλαιο αυτό περιγράφουμε τις οντότητες που απαρτίζουν ένα σύστημα PKI και τις βασικότερες λειτουργικές διαδικασίες με τις οποίες είναι επιφορτισμένες.

3.3.1 Αρχή Αποδοχής Πολιτικής (Policy Approval Authority)

Η οντότητα PAA αποτελεί την ρίζα της αρχιτεκτονικής PKI. Η Αρχή αυτή είναι γνωστή σε όλες τις υπόλοιπες οντότητες του δικτύου και καθορίζει τα πλαίσια μέσα στα οποία κινούνται και επικοινωνούν μεταξύ τους οι οντότητες αυτές (χρήστες, CAs και άλλες αρχές). Είναι, επίσης, υπεύθυνη για την επίβλεψη των πολιτικών που ακολουθούν αρχές οι οποίες είναι κατώτερες στην ιεραρχία από αυτή. Οι κυριότερες από τις λειτουργίες της είναι οι εξής :

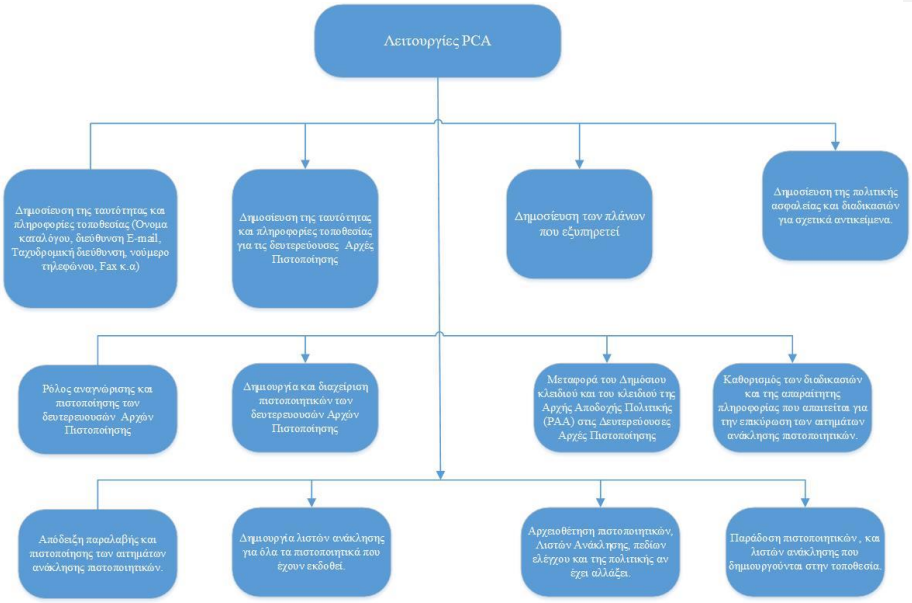
- καθορίζει τις πολιτικές και τις διαδικασίες που πρέπει να ακολουθούν οντότητες όπως CAs, PCAs (Policy Certification Authorities), ORAs (Organizational Registration Authorities)
- εκδίδει πιστοποιητικά για τις PCAs, κάνει την αναγνώριση (identification) και την ταυτοποίηση (authentication) αυτών, λαμβάνει και επικυρώνει αιτήσεις για νέες πολιτικές από τις Αρχές αυτές

- Κρατά αρχείο όλων των πιστοποιητικών και των λιστών Ανάκλησης αυτών (CRLs) που έχει εκδόσει κατά καιρούς

Είναι λοιπόν εμφανές ότι η αρχή PAA αποτελεί την κεντρική διεύθυνση ενός PKI συστήματος και ορίζει όλες τις πολιτικές που θα ακολουθηθούν από τις υπόλοιπες οντότητες.

3.3.2 Αρχή Πολιτικής για την Πιστοποίηση (Policy Certification Authority)

Η Αρχή αυτή βρίσκεται στο δεύτερο υψηλότερο επίπεδο της PKI ιεραρχίας, κάτω από την PAA. Ο ρόλος της είναι η περιγραφή των χαρακτηριστικών των χρηστών που υπάγονται σε αυτή και οι αρμοδιότητές της επεκτείνονται σε θέματα πιστοποίησης αλλά και πολιτικών ασφάλειας που θα ακολουθηθούν. Στο σχήμα 3.4 παρουσιάζονται σχηματικά οι ρόλοι αυτής της αρχής.



Σχήμα 3.4 Λειτουργίες PCA οντότητας Πηγή: Certificate-Based Key Management", Internet Activities Board, February 1993

Comment [IB1]: Αυτό το δέντρο να γραφτεί στην ελληνική γλώσσα γιατί πέραν της γλώσσας δεν έχει καλή ευκρίνεια. (να γραφτεί και η πηγή προέλευσης από όπου το πήρες.

Συνοπτικά οι διαδικασίες με τις οποίες είναι επιφορτισμένη μια PCA είναι οι εξής :

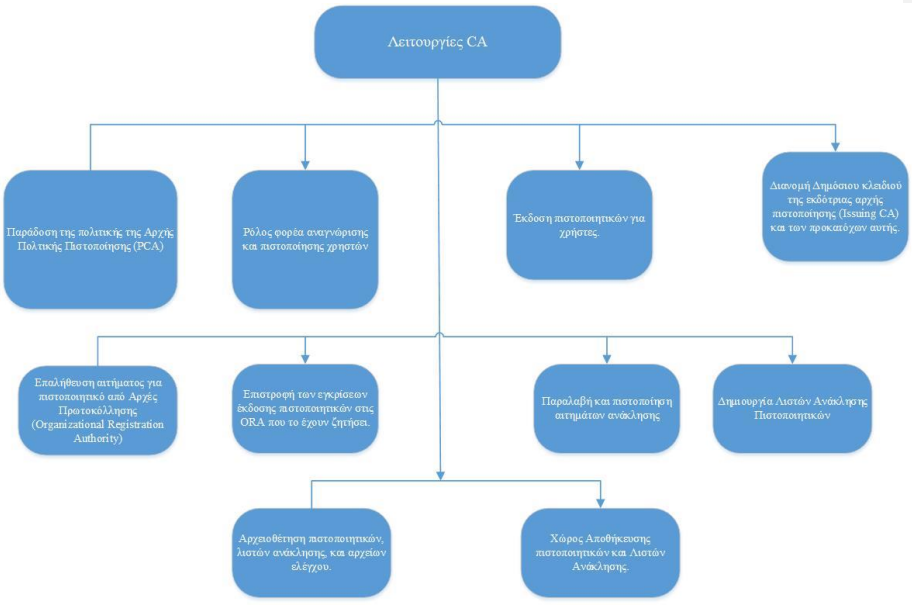
- Εκδίδει την ταυτότητα (identification) και πληροφορίες που χαρακτηρίζουν την ίδια (πχ. το directory name, την διεύθυνση e-mail, τον αριθμό

τηλεφώνου) αλλά και των CAs που βρίσκονται στις κατώτερες βαθμίδες. Επίσης εκδίδει και διαχειρίζεται και τα πιστοποιητικά των CAs

- Εκδίδει τις πολιτικές ασφάλειας και τις διαδικασίες που αφορούν τον έλεγχο της εγκυρότητας των αιτήσεων ανάκλησης πιστοποιητικών
- Δημοσιεύει το δημόσιο κλειδί της και εκδίδει CRLs για τα πιστοποιητικά που έχει εκδόσει

3.3.3 Αρχή Πιστοποίησης (Certification Authority)

Στην αμέσως κατώτερη βαθμίδα ιεραρχίας από αυτή των PCAs βρίσκονται οι Αρχές Πιστοποίησης (CAs). Οι οντότητες αυτές δεν έχουν την δυνατότητα να ορίζουν μόνες τους την πολιτική που θα ακολουθήσουν, και δρουν σύμφωνα με τις εντολές που ορίζονται από τις PCAs. Μια CA μπορεί να έχει οποιοδήποτε συνδυασμό χρηστών και ORAs (Organizational Registration Authorities), την ταυτότητα των οποίων πιστοποιεί. Στο ακόλουθο σχήμα παρουσιάζεται διαγραμματικά ο ρόλος και οι λειτουργίες μιας CA.



Σχήμα 3.5 Λειτουργίες CA οντότητας. Πηγή: Certificate-Based Key Management", Internet Activities Board, February 1993

Comment [IB2]: Όπως προηγουμένως

Παρατηρούμε ότι ο βασικός ρόλος μιας CA είναι η δημιουργία, η δημοσίευση, η ανάκληση και η αρχειοθέτηση των πιστοποιητικών δημοσίου κλειδιού, που «διασυνδέουν» μοναδικά την ταυτότητα του χρήστη με το δημόσιο κλειδί του. Ο ρόλος τους καθίσταται θεμελιώδης για την ασφαλή λειτουργία ενός PKI συστήματος, καθώς παρέχουν ασφαλή διανομή των δημόσιων κλειδιών. Έχουν, λοιπόν, την δυνατότητα να πιστοποιούν κλειδιά χρηστών σύμφωνα με την πολιτική που ορίζουν οι αρχές PCA και PAA, ακόμη και να πιστοποιούν κλειδιά που ανήκουν σε άλλες CAs. Διασφαλίζουν, επίσης, ότι όλοι οι παράμετροι των κλειδιών συμφωνούν με τα επιτρεπτά όρια που ορίζουν οι PCAs. Επιβαρύνονται με την δημιουργία λιστών ανάκλησης (CRLs) των πιστοποιητικών που έχουν εκδόσει, και, βέβαια, διατηρούν αρχείο των λιστών αυτών και των πιστοποιητικών.

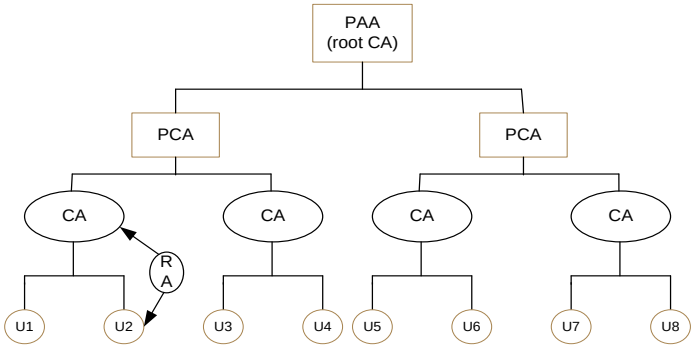
3.3.4 Αρχή Οργάνωσης των Εγγραφών (Organisational Registration Authority)

Η Αρχή αυτή αποτελεί, ουσιαστικά, το interface μεταξύ του χρήστη και του CA. Ο βασικός της ρόλος είναι να κάνει την αναγνώριση (identification) και ταυτοποίηση (authentication) του χρήστη για λογαριασμό της CA, και να του παραδίδει το πιστοποιητικό που εξέδωσε το CA. Η πορεία των ενεργειών που ακολουθεί είναι η εξής: αφού πιστοποιήσει την αυθεντικότητα ενός χρήστη, μεταδίδει μία υπογεγραμμένη αίτηση πιστοποιητικού στην υπεύθυνη CA. Στη συνέχεια, παραλαμβάνει το πιστοποιητικό από την CA και το μεταδίδει στον χρήστη. Επίσης, πρέπει σε τακτά χρονικά διαστήματα να ενημερώνει το CA για περιπτώσεις ανάκλησης πιστοποιητικών. Τέλος, είναι αναγκαίο να κρατά αρχείο των πιστοποιητικών ώστε να μπορεί να επιβεβαιώνει ψηφιακές υπογραφές των χρηστών.

3.3.5 Ιεραρχική δομή των PKI οντοτήτων

Στο σημείο αυτό θα προσπαθήσουμε να δόσουμε κάποια παραδείγματα αρχιτεκτονικής των συστημάτων PKI , βασιζόμενοι στα επίπεδα εμπιστοσύνης που χαρακτηρίζουν τις σχέσεις των οντοτήτων που τα αποτελούν. Ο πρωταρχικός στόχος μιας PKI αρχιτεκτονικής είναι να επιτρέψει στον κάθε χρήστη να δημιουργήσει αλυσίδες εμπιστοσύνης, οι οποίες να μην έχουν μήκος μεγαλύτερο

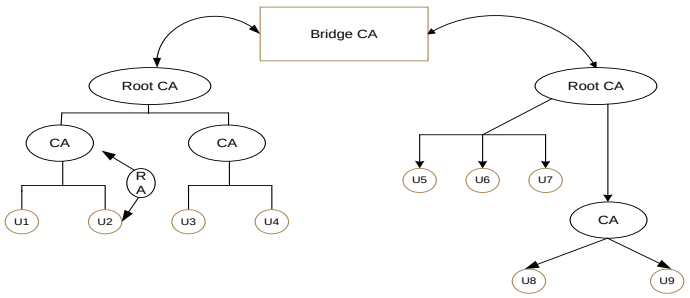
από ένα λογικό αριθμό πιστοποιητικών. Στην εικόνα 3.6 παρουσιάζεται μία δενδρική δομή ενός PKI συστήματος.



Σχήμα 3.6 Δενδρική δομή σε ένα PKI σύστημα

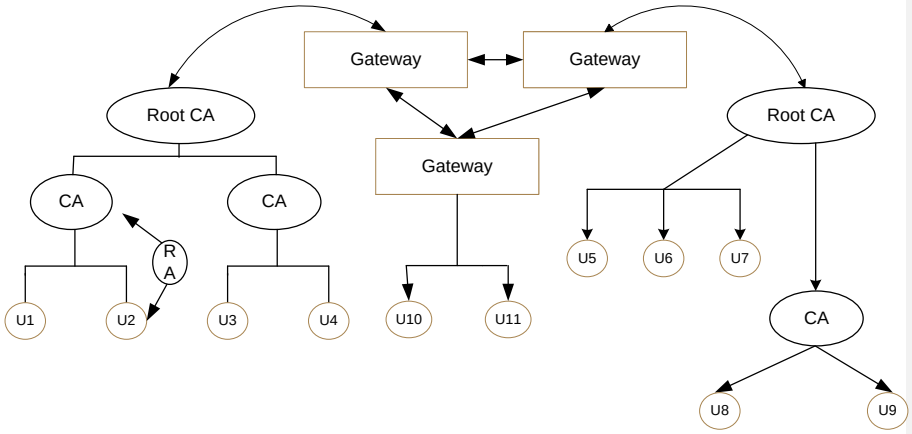
Παρατηρούμε ότι οι σχέσεις εμπιστοσύνης ακολουθούν μία αυστηρή δενδρική ιεραρχία με βάση μία θεμελιώδη Αρχή , η οποία μπορεί να είναι PAA ή PCA , και η οποία είναι το αρχικό σημείο αναφοράς των σχέσεων εμπιστοσύνης για κάθε οντότητα. Κάθε CA πιστοποιεί τα δημόσια κλειδιά των χρηστών που υπάγονται σε αυτή. Επίσης, γίνεται η διανομή, σε όλες τις PKI οντότητες, του δημοσίου κλειδιού της root CA, και με τον τρόπο αυτό κάθε οντότητα συνδέεται με την root CA με μία μοναδική διαδρομή εμπιστοσύνης.

Ανάλογα με τις απαιτήσεις ασφάλειας και απόδοσης που μπορεί να θέτει ένα δίκτυο, μπορούν να συνδυαστούν μεταξύ τους διαφορετικοί τύποι ιεραρχίας των οντοτήτων. Υπάρχει η επιλογή της χρήσης μιας CA-γέφυρας και η επιλογή του άμεσου cross-certification των root CAs. Στο ακόλουθο σχήμα παρουσιάζεται ένας συνδυασμός ιεραρχικής δενδρικής δομής με μια πιο αυθαίρετη, με την χρήση μιας γέφυρας CA.



Σχήμα 3.7 Δομή με CA γέφυρα

Με μία πιο αυθαίρετη δομή μπορούμε να έχουμε την σύνδεση των οντοτήτων μεταξύ τους με περισσότερες από μία αλυσίδες εμπιστοσύνης. Το πρωτόκολλο PGP (Pretty Good Privacy) χρησιμοποιεί μία δομή mesh, ώστε κάθε οντότητα να λειτουργεί σαν μια ξεχωριστή CA. Επίσης, η χρήση αρχιτεκτονικών με γέφυρες (gateway structures) χρησιμοποιείται όλο και περισσότερο σε εφαρμογές προσωπικών δικτύων VPNs. Στην εικόνα 3.8 απεικονίζεται μία τέτοια δομή με τρεις gateway CAs που πιστοποιούνται μεταξύ τους. Τέτοιες οριζόντιες δομές παρουσιάζουν μεγάλη ανθεκτικότητα σε επιθέσεις καθώς δρομολογούν τις διαδρομές εμπιστοσύνης των οντοτήτων μέσω οριζόντιας οδού.



Εικόνα 3.8 Δομή με gateway CAs

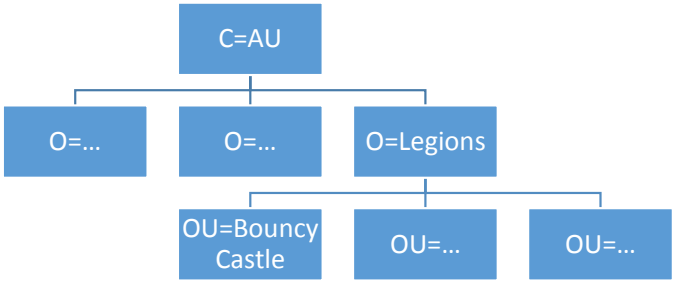
3.4 ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ X.509

Πριν αναφερθούμε αναλυτικά στις μορφές (formats) των πιστοποιητικών X.509 είναι αναγκαίο να παρουσιαστεί σύντομα η δομή X.500 και τα *διακεκριμένα ονόματα (Distinguished Names)*, καθώς και η δομή σύνταξης ASN.1 που βοηθά στην περιγραφή αντικειμένων.

3.4.1 Abstract Syntax Notation 1 (ASN.1) και X.500 Directory structure

Η ASN.1 σύνταξη προέκυψε από τα πρότυπα της ISO και της ITU-T (International Telecommunications Union) κατά την διάρκεια της ανάπτυξης των προτύπων που αφορούσαν την διασύνδεση συστημάτων OSI (Open Systems Interconnection). Ο πρωταρχικός στόχος ήταν η δημιουργία ενός συνοπτικού σημειολογικού τρόπου περιγραφής αντικειμένων που περιλαμβάνουν τα πρωτόκολλα. Σήμερα χρησιμοποιείται ευρέως για την περιγραφή κωδικοποίησης κλειδιών, ασφαλών πρωτοκόλλων, και παραμέτρων των αλγορίθμων που χρησιμοποιούνται [1]. Το βασικό πρότυπο που καθορίζει την σύνταξη ASN.1 είναι το X.680 και στη συνέχεια την χρησιμοποιούμε για να περιγράψουμε αντικείμενα όπως τα πιστοποιητικά και τα X.500 διακεκριμένα ονόματα (Distinguished Names).

Η έννοια του *διαεκριμένου ονόματος (distinguished name)*, ή αλλιώς DN, προτάθηκε στο X.501 του OSI για να περιγράψει την δομή X.500. Η βασική ιδέα του X.500 directory είναι η δημιουργία μιας ιεραρχίας, όπως αυτής του σχήματος 3.9, όπου κάθε επίπεδο χαρακτηρίζεται μοναδικά με ένα *σχετικό διακριτό όνομα (relative distinguished name)*, ή αλλιώς RDN.



Εικόνα 3.9 X.500 Directory Structure

Ολόκληρη η διαδρομή από την βάση του δέντρου ονομάζεται *distinguished name (DN)* και αποτελείται από την διαδοχή των RDNs. Σύμφωνα με την ASN.1, ένα DN περιγράφεται ως εξής :

DistinguishedName ::= RDNSequence

RDNSequence :: = SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET SIZE (1..MAX) OF AttributeTypeAndValue

AttributeTypeAndValue ::= SEQUENCE {

Συνεπώς, σύμφωνα με την εικόνα 3.9 και με την ASN.1 σύνταξη, ένα DN είναι string χαρακτήρων όπως το ακόλουθο:

"CN=www.bouncycastle.org, OU=Bouncy Castle, O=Legions, C=AU"

3.4.2 Γενικά για τα πιστοποιητικά X.509

Όπως είναι γνωστό, τα ψηφιακά πιστοποιητικά, ή ακριβέστερα τα πιστοποιητικά δημοσίου κλειδιού, παρέχουν ένα μηχανισμό σε μία οντότητα ώστε να μπορέσει να εγγυηθεί ότι ένα συγκεκριμένο δημόσιο κλειδί ανήκει μοναδικά σε ένα χρήστη ή σε μία δομή (πχ. CA). Κάθε πιστοποιητικό συνδέεται με ένα ιδιωτικό κλειδί , και μία αλυσίδα πιστοποιητικών είναι μία διαδοχή αυτών, όπου, το ιδιωτικό κλειδί καθενός από αυτά έχει χρησιμοποιηθεί για να υπογράψει το επόμενο πιστοποιητικό που ακολουθεί στην λίστα. Το πρώτο πιστοποιητικό της αλυσίδας, το οποίο ονομάζεται root certificate, είναι συνήθως υπογεγραμμένο από την οντότητα που κατέχει το ζεύγος κλειδιών που αυτό πιστοποιεί, είναι δηλαδή self-signed. Το τελευταίο πιστοποιητικό της αλυσίδας παρέχει την πιστοποίηση του δημόσιου κλειδιού της οντότητας και, δεδομένου ότι μια άλλη οντότητα εμπιστεύεται το root certificate, το δημόσιο κλειδί θεωρείται αυθεντικό γι' αυτή. Σύμφωνα με την ιεραρχία PKI, η αρχή που εκδίδει τα πιστοποιητικά και αποτελεί το βασικό «εκτελεστικό» όργανο της πολιτικής PKI, ονομάζεται Αρχή Πιστοποίησης (Certification Authority).

Η επικρατέστερη μορφή πιστοποιητικών είναι το X.509 και έχει καθοριστεί ως το Διεθνές Πρότυπο Πιστοποιητικών X.509 της ένωσης ITU-T (International Telecommunications Union) [2] ή ISO/IEC/ITU 9594-8, και δημοσιεύτηκε για

πρώτη φορά το 1988 σαν μέρος του X.500 directory. Η πρώτη αυτή μορφή του πιστοποιητικού ονομάστηκε έκδοση 1 (v1) και στηριζόταν πάνω στην εξής ιδέα : μπορούσε κάποιος να χρησιμοποιήσει το DN της οντότητας που έχει εκδόσει ένα πιστοποιητικό και να δημιουργήσει μία αλυσίδα πιστοποιητικών που οδηγούν στο root της ιεραρχίας. Το στοιχείο αυτό, όμως, θεωρήθηκε πολύ περιοριστικό και το 1993 παρουσιάστηκε το πιστοποιητικό X.509 έκδοση 2, το οποίο εισήγαγε την έννοια του *παράγοντα μοναδικής αναγνώρισης (unique identifier)* του εκδότη και του κατόχου του πιστοποιητικού. Αυτό βοήθησε την επαναχρησιμοποίηση των DNs διατηρώντας ατόφια την δομή του X.500 directory. Τελικά, και αυτή η πρόταση κατέρρευσε και τελικά επικράτησε το πιστοποιητικό X.509 έκδοση 3 (από το 1996 και μετά), με το οποίο παρουσιάστηκε η έννοια των *επεκτάσεων* του πιστοποιητικού, οι οποίες ονομάζονται *certificate extensions*. Με τον τρόπο αυτό εισήχθηκαν καινοτομίες όπως η χρήση του κλειδιού που απελευθέρωσε τελείως την έννοια των αλυσίδων εμπιστοσύνης μέσα σε ένα PKI σύστημα. Έτσι, ανάλογα με τις απαιτήσεις που θέτει κάποιος, μπορούμε να δημιουργήσουμε ένα μοντέλο με αυστηρή ιεραρχία των οντοτήτων είτε ένα δίκτυο «ιστού» εμπιστοσύνης μεταξύ τους.

Σήμερα έχει επικρατήσει πλήρως η χρήση πιστοποιητικών X.509 version 3, υπάρχουν ωστόσο και κάποια πιστοποιητικά έκδοσης 1 που είναι κυρίως αυτο-υπογεγραμμένα πιστοποιητικά από root οντότητες. Τα X.509 πιστοποιητικά χρησιμοποιούνται σε πολλά πρωτόκολλα όπως στο S/MIME για ασφάλεια ηλεκτρονικού ταχυδρομείου, στο IPSec για ασφάλεια επιπέδου δικτύου, στα SSL/TLS για ασφάλεια επιπέδου μεταφοράς.

Η δομή ASN.1 του X.509 ψηφιακού πιστοποιητικού παρατίθεται στην συνέχεια. Οι σημαντικές πληροφορίες βρίσκονται στο πεδίο tbsCertificate, το οποίο περιέχει τις λεπτομέρειες που περιγράφουν τον εκδότη του πιστοποιητικού (issuer) καθώς και τον κάτοχο (subject). Η δομή ASN.1 του tbsCertificate παρατίθεται ακολούθως.

```
Certificate  ::=  SEQUENCE  {
                  tbsCertificate          TBSCertificate,
                  signatureAlgorithm      AlgorithmIdentifier,
                  signatureValue          BIT STRING
                                  }
```

ASN.1 Definition of *Certificate*

```
TBSCertificate    ::=    SEQUENCE    {
                  version          [0]  EXPLICIT Version DEFAULT  v1,
                  serialNumber              CertificateSerialNumber,
                  signature                 AlgorithmIdentifier,
                  issuer                     Name,
                  validity                  Validity,
                  subject                   Name,
                  subjectPublicKeyInfo      SubjectPublicKeyInfo,
                  issuerUniqueID    [1]     IMPLICIT UniqueIdentifier OPTIONAL,
                                            ----  If present , version shall be v2 or v3
                  subjectUniqueID   [1]     IMPLICIT UniqueIdentifier OPTIONAL,
                                            ----  If present , version shall be v2 or v3
                  issuerUniqueID    [1]     IMPLICIT Extensions  OPTIONAL,
                                            ----  If present , version shall be v3
                                       }

Name  ::  =  CHOICE { RDNSequence }
```

ASN.1 Definition of *TBSCertificate*

Στην συνέχεια θα περιγράψουμε με συνοπτικό τρόπο τα V.1 και V.2 πιστοποιητικά, δίνοντας μεγαλύτερη έμφαση στο V.3.

3.4.3 Ψηφιακό Πιστοποιητικό X.509 έκδοση 1

Η δομή του πιστοποιητικού X.509 έκδοση 1 περικλείει πληροφορίες που αφορούν τον ιδιοκτήτη του δημοσίου κλειδιού και την αρχή Πιστοποίησης που το εξέδοσε. Κάποια από τα πεδία του είναι ο αριθμός της έκδοσης, ένας σειριακός αριθμός, η υπογραφή και ο αλγόριθμος αυτής που χρησιμοποίησε η CA, τα ονόματα του εκδότη και του κατόχου, το χρονικό διάστημα εγκυρότητάς του και, βέβαια, το δημόσιο κλειδί του κατόχου. Στο παρακάτω σχήμα παρουσιάζεται το πιστοποιητικό έκδοσης 1 με τα πεδία του.

Certificate fields	Interpretation of contents
Version	Version of certificate format
Serial number	Certificate serial number
Signature algorithm	Signature algorithm identifier for certificate issuer's signature

Issuer	CA's X.500 name
Validity period	Start and expiry dates/times
Subject name	Subject X.500 name
Subject public key information	Algorithm identifier and subject public-key value
Issuer's signature	Certificate Authority's digital signature

Εικόνα 3.10 X.509 v1 Certificate format

3.4.4 Ψηφιακό Πιστοποιητικό X.509 έκδοση 2

Όπως αναφέρθηκε προηγουμένως, το Ψηφιακό Πιστοποιητικό X.509 έκδοση 1 παρουσιάζει περιορισμούς που αφορούν την χρήση του. Το Ψηφιακό Πιστοποιητικό X.509 έκδοση 2 (v2), που περιέχεται στο RFC 1422 περιέχει δύο πεδία ακόμη, που περιέχουν δύο μοναδικούς συντελεστές αναγνώρισης, ένα για τον εκδότη και ένα για τον κάτοχο του πιστοποιητικού (issuer unique identifier και subject unique identifier). Τα πεδία αυτά είναι σημαντικά γιατί επιτρέπουν την χρησιμοποίηση του ίδιου ονόματος μετά από κάποιο χρονικό διάστημα, εξασφαλίζοντας ότι οι οντότητες που έχουν κοινό όνομα θα διακρίνονται ως ξεχωριστές από τα μέλη του δικτύου. Τα υπόλοιπα πεδία είναι ακριβώς τα ίδια με αυτά του πιστοποιητικού έκδοσης 1.

3.4.5 Ψηφιακό Πιστοποιητικό X.509 έκδοση 3

Το Ψηφιακό Πιστοποιητικό X.509 έκδοση 3 (v3) δημοσιεύτηκε από την ISO/IEC/ITU και την ANSI X9 για να ξεπεραστούν δυσκολίες που προέκυπταν από τις παλαιότερες εκδόσεις και για να ικανοποιηθούν νέες απαιτήσεις. Τον Ιούνιο του 1996 ολοκληρώθηκε το πρότυπο της τρίτης έκδοσης του X.509 πιστοποιητικού και αποτελείτο από 11 πεδία (εικόνα 3.11). Η διαφορά του από τις προηγούμενες εκδόσεις είναι ότι περιλαμβάνει ένα νέο πεδίο, το οποίο ονομάζεται πεδίο προεκτάσεων (extensions field), στο οποίο περιγράφονται χαρακτηριστικά του πιστοποιητικού που επεκτείνουν σε πολύ μεγαλύτερο βαθμό την χρήση του. Πιο συγκεκριμένα, οι επεκτάσεις αυτές μεταφέρουν δεδομένα όπως

συμπληρωματική πληροφορία για την ταυτότητα του κατόχου, περιορισμοί στην διαδρομή πιστοποίησης, πληροφορία για τα χαρακτηριστικά του κλειδιού και γενικότερα για την πολιτική που ακολουθείται. Είναι, λοιπόν, εμφανές ότι οι επεκτάσεις του πιστοποιητικού παρέχουν μεθόδους ώστε το πιστοποιητικό να περιγράφει με σαφέστατο τρόπο τα όρια μέσα στα οποία ο κάτοχος μπορεί να χρησιμοποιήσει το κλειδί του, την χρήση του κλειδιού από μία τρίτη οντότητα και, γενικότερα, την διαχείριση των σχέσεων πιστοποίησης μέσα στην ιεραρχία PKI.

Certificate fields	Interpretations of contents
v1=v2=v3 (for seven fields)	Version, serial number, signature algorithm, issuer, validity period, subject name, subject public-key information
v2=v3 (for two fields)	Issuer unique identifier Subject unique identifier
Extensions (v3)	Key and policy information
v1=v2=v3 (for the last field)	Issuer's signature

Εικόνα 3.11 X.509 v3 Certificate format

3.4.5.1 Προεκτάσεις X.509 (X.509 Extensions)

Κάθε προέκταση αποτελείται από ένα object identifier (OID) και μία δομή ASN.1. Όπως διαφαίνεται στην δομή ASN.1 που παρατίθεται πιο κάτω, το OID περιέχεται στο πεδίο extnID, προσδιορίζοντας τον τύπο της προέκτασης και τον

τρόπο που πρέπει να ερμηνεύσει κάποιος τα bytes στο πεδίο extnValue. Το πεδίο critical, που είναι ένας boolean, διευκρινίζει αν η εφαρμογή που προσπαθεί να διαβάσει το πιστοποιητικό θα πρέπει να είναι σε θέση να κατανοεί τον τύπο της επέκτασης. Τέλος, το πεδίο extnValue περιέχει μία DER κωδικοποίηση του τύπου της επέκτασης (Distinguished Encoding Rules).

```
Extensions   ::  SEQUENCE SIZE (1..MAX) OF Extension

Extension    ::  SEQUENCE  {
                       extnID      OBJECT IDENTIFIER,
                       critical       BOOLEAN DEFAULT FALSE,
                       extnValue  OCTET STRING
                                }
```

ASN.1 Definition of *Extensions*

Οι επεκτάσεις χωρίζονται σε τέσσερεις ομάδες, ανάλογα με το τι περιγράφουν.Αυτές είναι οι εξής :

- Extensions με πληροφορία που αφορά το κλειδί και την πολιτική
- Extensions με attributes του εκδότη και του κατόχου
- Extensions με περιορισμούς σε σχέση με το certification path
- Extensions με πληροφορία που αφορά τις λίστες ανάκλησης πιστοποιητικών (CRLs)

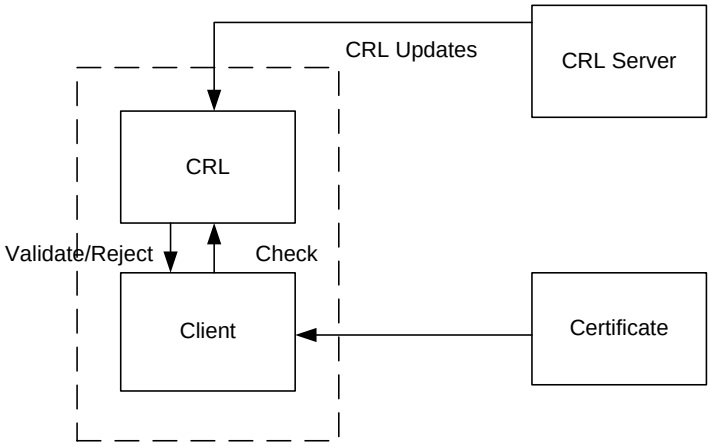
Στην πρώτη κατηγορία, η κυριότερη προέκταση είναι η KeyUsage, στην οποία ορίζονται οι χρήσεις που μπορεί να έχει το κλειδί. Περιλαμβάνει πεδία όπως digitalSignature για το αν το κλειδί θα χρησιμοποιείται για ψηφιακές υπογραφές, keyEncipherment για το αν θα κρυπτογραφεί άλλα κλειδιά, keyAgreement για το αν θα συμμετέχει σε αντίστοιχη διαδικασία και, τέλος, crlSign για το αν θα υπογράφει CRLs. Στην δεύτερη κατηγορία, η κυριότερη προέκταση είναι η SubjectAltName, η οποία δίνει την δυνατότητα στον κάτοχο του δημοσίου κλειδιού να είναι γνωστός και με άλλα ονόματα. Στην κατηγορία που αφορά τους περιορισμούς, η κυριότερη προέκταση είναι η BasicConstraints, με την οποία μπορούμε να ορίσουμε αν ο κάτοχος του πιστοποιητικού είναι Certificate Authority ή απλή οντότητα. Επίσης μπορεί να οριστεί ο αριθμός των πιστοποιητικών που μπορούν να έπονται αυτού που έχει την επέκταση. Με τον

τρόπο αυτό ορίζουμε το μήκος του Certificate path που ακολουθεί το πιστοποιητικό. Τέλος, στην τελευταία κατηγορία υπάγονται προεκτάσεις που αφορούν τον τρόπο με τον οποίο μπορεί κάποιος να λάβει CRL πληροφορίες για το πιστοποιητικό.

3.5 ΛΙΣΤΕΣ ΑΝΑΚΛΗΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ (CRLs) ΚΑΙ PATH VALIDATION

Η βασική μέθοδος για την διαχείριση των πιστοποιητικών που έχουν ανακληθεί είναι η χρήση των Λιστών Ανάκλησης Πιστοποιητικών (Certificate Revocation Lists). Τα πιστοποιητικά μπορεί να ανακληθούν για πολλούς λόγους, όπως η περίπτωση να ανακληθεί από την CA επειδή έχει λήξει το χρονικό διάστημα που μπορεί αυτό να χρησιμοποιηθεί. Ένας πιο σημαντικός λόγος ανάκλησης του πιστοποιητικού είναι η περίπτωση που κάποιος κακόβουλος έχει ανακτήσει το ιδιωτικό κλειδί που συνδέεται με αυτό.

Οι λίστες CRLs χρησιμοποιούνται σε μεγάλη ποικιλία από εφαρμογές και περιβάλλοντα καλύπτοντας διαλειτουργικά προβλήματα και απαιτήσεις ασφάλειας. Συνεπώς, όπως κάποιος χρησιμοποιεί ένα root certificate για να πιστοποιήσει την εγκυρότητα των πιστοποιητικών που δέχεται, με τον ίδιο τρόπο «διαβάζει» την λίστα CRL του root certificate για να δει ποια από αυτά τα πιστοποιητικά έχουν ανακληθεί. Στο επόμενο σχήμα παρουσιάζεται ο τρόπος διανομής μιας τέτοιας λίστας. Όπως είναι φανερό, διανέμεται από ένα server και ο χρήστης την κρατά και ελέγχει τα πιστοποιητικά που δέχεται.



Εικόνα 3.12 CRL distribution

Η δομή X.509 CRL έχει καθοριστεί στο πρότυπο ISO/IEC/ITU, και έχει εξελιχθεί σημαντικά από το 1998 που πρωτοεμφανίστηκε, όπως και με τη δομή του πιστοποιητικού X.509. Πιο συγκεκριμένα, όταν προστέθηκαν οι επεκτάσεις στη δομή του πιστοποιητικού και δημιουργήθηκε το πιστοποιητικό X.509 v3, ο ίδιος μηχανισμός προστέθηκε και στις CRL λίστες για να δημιουργηθεί η X.509 v2 CRL. Έτσι, τα κυριότερα πεδία του X.509 v2 CRL είναι η έκδοσή του (version), η υπογραφή (signature), το όνομα του εκδότη (issuer name), τα ανακληθέντα πιστοποιητικά (revoked certificates) και πληροφορίες για τις ανανεώσεις της λίστας (updates).

Τέλος, υπάρχει και πεδίο το οποίο περιλαμβάνει τις επεκτάσεις που μπορεί να πάρει η CRL (extensions field). Με τον τρόπο αυτό συνδέονται περισσότερες πληροφορίες με την λίστα, όπως συμβαίνει και με τις επεκτάσεις του πιστοποιητικού X.509 v3 .

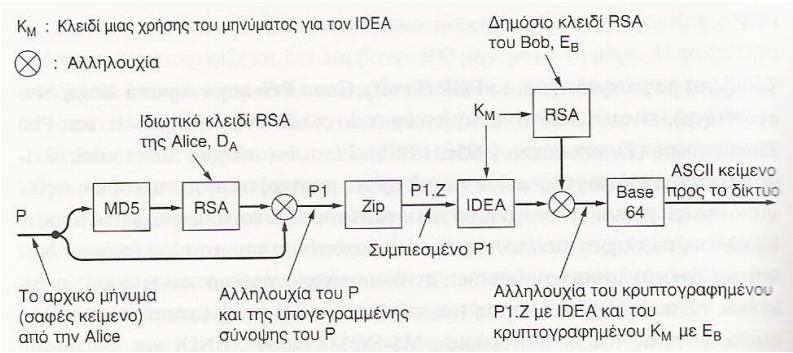
3.6 ΠΡΩΤΟΚΟΛΛΟ PRETTY GOOD PRIVACY (PGP)

Το πρωτόκολο PGP δημιουργήθηκε από τον Phil Zimmermann και δόθηκε στην δημοσιότητα το 1995. Είναι ένα πλήρες πακέτο ασφάλειας που παρέχει μυστικότητα, πιστοποίηση αυθεντικότητας, ψηφιακές υπογραφές και συμπίεση σε εύχρηστη μορφή. Το πλήρες πακέτο, συμπεριλαμβανομένου και του πηγαίου κώδικα, διατίθεται δωρεάν μέσω του Internet και άλλων εμπορικών δικτύων. Εξαιτίας της ποιότητάς τους, της μηδενικής του τιμής και της εύκολης διαθεσιμότητάς του σε πλατφόρμες Windows, Unix και Macintosh, χρησιμοποιείται σήμερα ευρέως.

3.6.1 Λειτουργία του PGP

Αυτό που χαρακτηρίζει την λειτουργία του PGP είναι το γεγονός ότι συνδυάζει τα πλεονεκτήματα της ασύμμετρης κρυπτογραφίας και της κρυπτογραφίας δημόσιου κλειδιού. Είναι συνεπώς ένα υβριδικό κρυπτοσύστημα.

Ας υποθέσουμε ότι ένας χρήστης θέλει να κρυπτογραφήσει ένα plaintext με PGP. Αρχικά το PGP συμπιέζει το μήνυμα. Με τον τρόπο αυτό μειώνονται τα patterns που εμφανίζονται στο plaintext και που ένας κακόβουλος μπορεί να εκμεταλλευτεί, και αυξάνεται σημαντικά η κρυπτογραφική ασφάλεια. Στην συνέχεια δημιουργείται ένα κλειδί συνόδου (session key), το οποίο είναι μοναδικό μυστικό κλειδί για κάθε session. Για την δημιουργία του κλειδιού αυτού χρησιμοποιείται συνήθως ο συμμετρικός αλγόριθμος IDEA και το κλειδί έχει μήκος 128 bits. Το session key κρυπτογραφεί το plaintext και δημιουργείται το κρυπτογραφημένο μήνυμα ciphertext. Στην συνέχεια, το session key κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη και, τέλος, μεταδίδεται το ciphertext μαζί με το κρυπτογραφημένο session key. Το ακόλουθο σχήμα παρουσιάζει την διαδικασία κρυπτογράφησης του PGP.



Εικόνα 3.13 Το PGP σε λειτουργία αποστολής μηνύματος

Η διαδικασία αποκρυπτογράφησης είναι ακριβώς η αντίστροφη με αυτή της κρυπτογράφησης. Ο παραλήπτης του μηνύματος χρησιμοποιεί το ιδιωτικό του κλειδί για να αποκρυπτογραφήσει το session key, το οποίο χρησιμοποιείται στην συνέχεια από το PGP για να αποκρυπτογραφήσαει με την σειρά του το ciphertext.

Ο συνδυασμός των δύο μεθόδων κρυπτογράφησης είναι σημαντικός καθώς περιλαμβάνει την ταχύτητα με την οποία κρυπτογραφούν οι συμμετρικοί αλγόριθμοι και την αξιοπιστία της κρυπτογραφίας δημοσίου κλειδιού. Χάρη στην τελευταία, άλλωστε, εκμεταλλευόμαστε το πλεονέκτημα της διαχείρησης και διανομής των κλειδιών που μπορεί να προσφέρει, εξασφαλίζοντας μεγάλο βαθμό ασφάλειας.

3.6.2 Διαχείρηση κλειδιών στο PGP (Key Management)

Η διαχείριση κλειδιών έχει γίνει αντικείμενο μεγάλης προσοχής στο PGP, αφού αποτελεί την αχίλλειο πτέρνα των συστημάτων ασφαλείας. Ο κάθε χρήστης τηρεί δύο δομές δεδομένων τοπικά : έναν δακτύλιο ιδιωτικών κλειδιών και ένα δημοσίων. Ο δακτύλιος ιδιωτικών κλειδιών (private key ring) περιέχει ένα ή περισσότερα ζεύγη ιδιωτικού-δημοσίου κλειδιού. Ο λόγος για τον οποίο υποστηρίζονται πολλαπλά ζεύγη για κάθε χρήστη είναι να μπορούν οι χρήστες να αλλάζουν τα δημόσια κλειδιά τους περιοδικά ή όταν κάποιο φαίνεται να έχει υπονομευθεί, χωρίς να ακυρώσουν τα μηνύματα που εκείνη την στιγμή βρίσκονται στο στάδιο της ετοιμασίας ή μεταφοράς. Κάθε ζεύγος συνδέεται με μια ταυτότητα, ώστε ο αποστολέας ενός μηνύματος να μπορεί να πει στον

αποδέκτη, ποιο δημόσιο κλειδί χρησιμοποιήθηκε κατά την κρυπτογράφησή του. Οι ταυτότητες στο μήνυμα αποτελούνται από τα 64 bit χαμηλής τάξης του δημοσίου κλειδιού. Είναι ευθύνη των χρηστών να αποφεύγουν τις συγκρούσεις ταυτοτήτων των δημόσιων κλειδιών τους. Τα ιδιωτικά κλειδιά στο δίσκο κρυπτογραφούνται με την χρήση μιας ειδικής (αυθαίρετα μεγάλης) συνθηματικής φράσης (passphrase) για την προστασία τους. Ο δακτύλιος δημόσιων κλειδιών (public key ring) περιέχει τα δημόσια κλειδιά αυτών με τους οποίους αλληλογραφεί ο χρήστης. Κάθε καταχώρηση στον δακτύλιο αυτό περιέχει όχι μόνο το δημόσιο κλειδί, αλλά επίσης και την ταυτότητα 64 bit του και μία ενδειξη του πόσο πολύ εμπιστεύεται το κλειδί ο χρήστης.

3.6.3 Επίπεδα εμπιστοσύνης στο PGP (Levels of trust)

Το μοντέλο εμπιστοσύνης που υιοθετεί το PGP είναι αυτό του *web of trust (δίκτυο εμπιστοσύνης)*. Αυτό συνδυάζει το ιεραρχικό μοντέλο εμπιστοσύνης (αλυσίδας πιστοποιητικών μέχρι το root certificate), με αυτό της άμεσης εμπιστοσύνης σε ένα πιστοποιητικό. Σε ένα περιβάλλον PGP ο κάθε χρήστης μπορεί να λειτουργήσει σαν μία Αρχή Πιστοποίησης (Certificate Authority) και να εκδόσει πιστοποιητικό για το δημόσιο κλειδί μιας άλλης οντότητας. Αυτό όμως το πιστοποιητικό μπορεί να το εμπιστευτεί ένας τρίτος αν και εφόσον εμπιστεύεται τον εκδότη του. Για τον λόγο αυτό, ο κάθε χρήστης αποθηκεύει πληροφορίες στον δακτύλιο δημοσίου κλειδιού του που αφορούν τα εξής :

- αν θεωρεί ότι εμπιστεύεται ένα κλειδί ή όχι
- το επίπεδο εμπιστοσύνης (level of trust) που θεωρεί ότι έχει ένα κλειδί, τον βαθμό εμπιστοσύνης, δηλαδή, που έχει στον ιδιοκτήτη του κλειδιού ώστε να υπογράφει πιστοποιητικά τρίτων

Συνεπώς ο κάθε χρήστης δημιουργεί ένα ιστορικό εμπιστοσύνης για τους άλλους χρήστες, θεωρώντας ότι κάποιοι δίνουν έγκυρες υπογραφές και άλλοι όχι.

Ο υψηλότερος βαθμός εμπιστοσύνης είναι αυτός της εμπιστοσύνης του χρήστη στο δικό του ζεύγος κλειδιών, και ονομάζεται *αδιαπραγμάτευτη εμπιστοσύνη (implicit trust)*. Όσο αφορά τα επίπεδα εμπιστοσύνης στο κλειδί ενός τρίτου, αυτά είναι τρια : η απόλυτη εμπιστοσύνη (complete trust), η επιφυλακτική εμπιστοσύνη (marginal trust), και η μη εμπιστοσύνη (no trust). Αντίστοιχα, υπάρχουν και τρεις

διαβαθμίσεις που χαρακτηρίζουν την εγκυρότητα (validity) ενός κλειδιού (valid, marginally valid και invalid).

Συνεπώς, για να ορίσει ένας χρήστης ότι εμπιστεύεται μια οντότητα ως trusted third party, πρέπει να θεωρεί το κλειδί της έγκυρο (valid key), είτε επειδή αυτό είναι υπογεγραμμένο από τον ίδιο είτε από άλλη trusted third party οντότητα, και μετά να ορίσει το level of trust στο οποίο θεωρεί ότι ανήκει ο κάτοχος του κλειδιού αυτού. Το πρωτόκολλο PGP θεωρεί ότι ένα κλειδί είναι έγκυρο όταν έχει ο χρήστης στην κατοχή του ένα πιστοποιητικό το οποίο είναι υπογεγραμμένο με κλειδί το οποίο θεωρείται απολύτως εμπιστευόμενο (completely trusted key), ή όταν έχει στην διάθεσή του δύο πιστοποιητικά τα οποία είναι υπογεγραμμένα με κλειδιά τα οποία θεωρούνται επιφυλακτικώς εμπιστευόμενα (marginally trusted keys).

3.7 ΣΥΜΠΕΡΑΣΜΑΤΑ

Σήμερα η χρήση ψηφιακών πιστοποιητικών είναι ευρέως διαδεδομένη. Πολλές καθημερινές μας συναλλαγές (όπως η ηλεκτρονική τραπεζική – ebanking, ηλεκτρονικές συναλλαγές με το δημόσιο κ.α), χρησιμοποιούν τα ψηφιακά πιστοποιητικά για την ασφάλεια των συναλλαγών.

Αποτελούν δε την μόνη αξιόπιστη λύση για την ταυτόχρονη πιστοποίηση της προέλευσης και την διασφάλιση της ακεραιότητας της διακινούμενης πληροφορίας μέσω διαδικτύου. Όμως παρά την μεγάλη χρησιμότητα και ασφάλεια που παρέχουν, παρατηρείται ένας φόβος από την μεριά των δυνητικών χρηστών σχετικά με την χρήση, την ασφάλεια και την νομική αναγνώριση αυτών. Ο φόβος αυτός πηγάζει από την έλλειψη ενημέρωσης πάνω σε θέματα ψηφιακών πιστοποιητικών, κρυπτογράφησης και των εφαρμογών τους (ψηφιακές υπογραφές, smart cards, e-tokens κ.α.).

Για αυτό τον λόγο θα πρέπει να καταβληθούν προσπάθειες ενημέρωσης των χρηστών για τα πλεονεκτήματα χρήσης των τεχνολογιών αυτών.

Ο χρήστης θα πρέπει να ενημερώνεται διεξοδικά για τους όρους χρήσης των κρυπτογραφικών κελιδιών, των πιστοποιητικών και των συναφών υπηρεσιών του παρόχου υπηρεσιών πιστοποίησης. Τα εκδοθέντα ψηφιακά πιστοποιητικά θα πρέπει να χρησιμοποιούνται αποκλειστικά για τον σκοπό τον οποίο εκδόθηκαν, σύμφωνα με την εκάστοτε δήλωση πρακτικής. Φυσικά κάθε χρήστης θα πρέπει να προβαίνει στις απαραίτητες προφυλάξεις των ιδιωτικών κλειδιών ώστε να αποτρέψει την αποκάλυψη ή ακόμη και την απώλειά τους. Αν δε, υποψιαστεί την έκθεση των ιδιωτικών κλειδιών του σε μη εξουσιοδοτημένα άτομα, θα πρέπει να ζητά αμέσως την ανάκλησή του πιστοποιητικού.

Μέχρι σήμερα, η χρήση ψηφιακών πιστοποιητικών δεν είναι παντού υποχρεωτική και εξαρτάται από τον φορέα για το αν θα την χρησιμοποιήσει ή όχι. Αν όμως θέλουμε πραγματική ασφάλεια, η χρήση πιστοποιητικών πρέπει να εφαρμοστεί ευρέως.

3.8 ΒΙΒΛΙΟΓΡΑΦΙΑ

[1]: D.Hook, "Beginning Cryptography with Java", Wiley, 2005

[2]: S.Kent, "RFC 1422:Privacy Enhancement for Internet Electronic Mail, Part 2: Certificate-Based Key Management", Internet Activities Board, February 1993