Τεχνολογικό Εκπαιδευτικό Ίδρυμα
Χανίων

Πτυχιακή Εργασία:

Μελέτη Αλγορίθμων Κρυπτογράφησης Για Προστασία στο Internet

Σπουδαστής : ΦΙΛΙΟΣ ΓΕΩΡΓΙΟΣ

Εισηγητής:ΕΜΜΑΝΟΥΗΛ ΑΝΤΩΝΙΔΑΚΗΣ

Χανιά ***2003***

ΠΡΟΛΟΓΟΣ

Η ιστορία του υπολογισμού σημαδεύεται από περιόδους που αποτελείται από ενδιαφέροντα θέματα. Γενικά υπάρχει μια έντονη ανάπτυξη στην αλληλοσύνδεση computer systems μέσο networks,καθώς θα πρέπει να επικοινωνούν από το ένα σημείο στο άλλο. Οι οργανισμοί ίσως εξαρτώνται από συστήματα υπολογιστικών πληροφοριών οι οποίοι έχουν πολλές εφαρμογές και διάφορες χρησιμότητες.Η επαναστατική πρόοδος που παρατηρείται στις ηλεκτρονικές εργασίες και στο ηλεκτρονικό ταχυδρομείο, σε συνδυασμό με την ευρέως εξαπλωμένη ανάπτυξη των εφαρμογών του Internet,μας κάνει αναγκαίο την σύσταση πληροφοριών για θέματα ασφαλείας. Αφού ο κόσμος μας έχει συνδεθεί ηλεκτρονικά, χαρακτηρίστηκα όπως virus και hackers είναι μεγάλη απειλή για το δίκτυο, την ασφάλεια και την μυστικότητα.

Σκοπός αυτής της μελέτης είναι να παρέχουμε μια μελέτη στο πως μπορούμε να χειριστούμε δεδομένα με ασφαλή τρόπο μέσο όλων των network που έχουν εδραιωθεί. Για να επιτευχθεί αυτό, μια σύντομη εκτίμηση στην περιοχή της κρυπτογραφίας έχει ταυτιστεί παράλληλα με τις βελτιώσεις που γίνονται στην τεχνολογία ασφάλειας του δικτύου. Στα πρώτα κεφάλαια της μελέτης θα δούμε κάποιες βασικές αρχές συστημάτων κρυπτογράφησης και το πως αυτά μπορούν να συνεργαστούν πρακτικά και να παράγουν τα πιο ασφαλή εμπορικά και χρήσιμα προϊόντα. Επιπλέον γίνεται μια προσπάθεια να γίνει μια αναφορά σε κρυπτογραφικές επιθέσεις και απειλές στην ασφάλεια. Επίσης ένα κομμάτι της μελέτης αναφέρεται και στην εξέταση βασικών εννοιών της θεωρίας των πρώτων αριθμών και πως αυτά μπορούν να συνεργαστούν στο RSA κρυπτοσύστημα. Το θέμα της γενίκευσης των πρώτων αριθμών είναι το επόμενο θέμα που θα μελετηθεί μαζί με μία αναφορά στα υπάρχοντα πρωτεύοντα test αλγορίθμων. Μια ιδιαίτερη προσοχή δίνεται στον πρωτεύων αλγόριθμο του Rabin-Miller, που εξετάζεται με πιο εκτεταμένο τρόπο. Τέλος υπάρχει μια σειρά από tests που μας αποδεικνύει πόσο ακριβής είναι ο αλγόριθμος του Rabin-Miller.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦ 1:Security Background

ΚΕΦ 2:Κρυπτολογία και Ασφάλεια δεδομένων

ΚΕΦ 5:Πρωταρχικά Test Αλγορίθμων

ΚΕΦ 1:Security Background

1.1 Εισαγωγή

Η ανάγκη για πληροφορία στην ασφάλεια και η χρήση μυστικών επικοινωνιών σε φόρμες κωδικοποιημένων μηνυμάτων έχουν γίνει αντικείμενο μελέτης τόσο στην αρχαία όσο και στην σύγχρονη ιστορία. Ο Ιούλιος Καίσαρας ήταν ο πρώτος που διαπίστωσε την σημασία της ασφάλειας των μηνυμάτων από τα χέρια των εχθρών του υιοθετώντας ένα αραβικό σύστημα. Η στρατηγική των περαιτέρω κωδικών χρησιμοποιήθηκε και στην διάρκεια των παγκοσμίων πολέμων και στην Ευρωπαϊκή ιστορία. Για να επιτευχθούν επιτυχημένες μάχες και κατασκοπευτικά συστήματα πολλές υπηρεσίες ασφαλείας και ο στρατός, εστίασαν στο να μεταφέρουν τις υψηλής σημασίας πληροφορίες με ένα ασφαλή τρόπο. Στις μέρες λαμβανομένης της εξέλιξης της επιστήμης και της τεχνολογίας, το θέμα της ασφάλειας της πληροφορίας έχει γίνει αντικείμενο μεγάλου ενδιαφέροντος. Τα αυξανόμενα τεχνολογικά επιτεύγματα που παρατηρούνται στο χώρο των υπολογιστών, έχουν κάνει τους υπολογιστές προσιτά στην κοινωνία μας. Παρόλο που οι υπολογιστές από μόνοι τους προστατεύουν την πληροφορία που περιέχουν μπορεί να υπάρχουν «ανοιχτές πόρτες» στα περιεχόμενά τους που μερικά από αυτά να ναι εμπιστευτικά ή μυστικά.

Ο όρος «computer system» είναι μια σειρά από υπολογιστικές πηγές [1, p1].Κάθε μια πηγή είτε αλληλεπιδρά δια μέσου ενός τηλεπικοινωνιακού καναλιού, είτε περιλαμβάνει ανεξάρτητους υπολογιστές που επιδρούν μόνο αν ζητηθεί από τους χειριστές τους. Ένα computer system θεωρείται ασφαλές, όταν μπορεί και διατηρεί την μυστικότητα και την ακεραιότητα της πληροφορίας, που περιέχει, εμποδίζοντας την αναρμόδια χρήση των πηγών του. Με την εισαγωγή συστημάτων συνδρομής, διαμοιρασμένων συστημάτων και δικτύου, τα στοιχεία μεταδίδονται μεταξύ τερματικού σταθμού και υπολογιστή και μεταξύ υπολογιστή και υπολογιστή. Η εγκατάσταση των τηλεπικοινωνιακών ικανοτήτων, ανάμεσα τους τα computer systems, και η ανάγκη μεταφοράς μηνυμάτων από το ένα σημείο στο άλλο, έχει τελικά απλωθεί στην ανάγκη της χρήσης του δικτύου και της ασφάλειας των επικοινωνιών. Ο σκοπός της ασφάλειας του δικτύου είναι να προστατέψουμε την πληροφορία, που μεταδίδεται από αναρμόδιες πράξεις που θα προσπαθήσουν να την ανακόψουν ή να παρέμβουν στην πληροφορία.

1.2 Electronic Data Processing

Electronic Data Processing [EDP] έχει γίνει στις μέρες μας το βασικό χαρακτηριστικό για οργανισμούς σε δημόσιους και ιδιωτικούς τομείς. Αναμφίβολα είμαστε στην μέση μιας επανάστασης των ηλεκτρονικών business. Μεγάλα αποθέματα από ψηφιακά δεδομένα τώρα συγκεντρώνονται και τοποθετούνται σε μεγάλα computer database και μεταδίδονται μεταξύ υπολογιστών και τερματικών συσκευών τα οποία συνδέονται με σύνθετα δίκτυα τηλεπικοινωνιών. Το Internet έχει προξενήσει μια έκρηξη στις ηλεκτρονικές business και στην ηλεκτρονική δραστηριότητα του εμπορίου, θέτοντας μια καινούργια παγκόσμια κουλτούρα στις ηλεκτρονικές συναλλαγές πληροφοριών. Το Internet μπορεί να παρέχει συνεργασίες, καθώς και ευκαιρίες για ανάπτυξη ενός επιπρόσθετου καναλιού για service, παράδοση, νομιμοποιώντας επίσης άλλα περιβάλλον όπως τραπεζιτικές εργασίες, διαχείριση δημόσιου χρήματος καθώς και άλλες υπηρεσίες δικτύου. Παρόλα αυτά η ανάγκη για παροχή network access σε κινητές υπολογιστικές συσκευές έχει οδηγήσει στην χρήση των ασύρματων δικτύων. Το WAP [Wireless Application Protocol] είναι η εναλλακτική τεχνολογία που επιτρέπει στα περιεχόμενα και τις υπηρεσίες του Internet να διανεμηθούν σε κινητά τηλέφωνα καθώς και σε αλλά ασύρματα τερματικά. Το WAP επιτρέπει σε συσκευές να κάνουν online τραπεζικές συναλλαγές, χρήση e-mail και πρόσβαση στο Internet και όλα αυτά από τα κινητά τηλέφωνα.

Μια τόσο μεγάλη επανάσταση στις συναλλαγές πληροφοριών και στο networking σημαίνει ότι εταιρείες και οι χρήστες κινητών, θα πρέπει να έρθουν αντιμέτωποι με την μεγάλη πιθανότητα να πέσουν θύματα απάτης, κρυφοκοιτάγματος των e-mail, κλέψιμο στοιχείων τους καθώς επίσης ακούσιας φθοράς φακέλων από αναρμόδια άτομα. Νομοθέτες, αναγνωρίζοντας ότι η εμπιστευτικότητα και η ακεραιότητα ενός συγκεκριμένου στοιχείου πρέπει να προστατευθεί, έχουν δημιουργήσει νόμους που εμποδίζουν αυτά τα προβλήματα. Αλλά οι νόμοι από μόνοι τους δεν μπορούν να εμποδίσουν επιθέσεις ή απομάκρυνση απειλών στο data processing systems. Κατά συνέπεια η ασφάλεια στην πληροφορία είναι τώρα ένα μέγιστο θέμα που η ηλεκτρονική κοινωνία πρέπει να το αντιμετωπίσει. Ανάμεσα στα μέτρα που πρέπει να λάβουμε υπ'όψην στο να προστατέψουμε την μυστικότητα και την ακεραιότητα των computer data, είναι η κρυπτογραφία.

1.2.1 Ηλεκτρονικό Εμπόριο

1.2.1.1 Ηλεκτρονικές Συναλλαγές

Συναλλαγές χρημάτων από μια ομάδα σε μια άλλη μπορεί να επιτευχθεί με ηλεκτρονικό τρόπο.Το ηλεκτρονικό χρήμα επίσης καλείται ηλεκτρονικό ρευστό χρήμα ή ψηφιακό ρευστό χρήμα το οποίο μπορεί να είναι είτε για χρέωμα είτε για πίστωση. Με σκοπό να παρουσιάσουμε μια συναλλαγή, το ποσό του χρήματος πρέπει πρώτα να μετατραπεί σε ψηφιακό χρήμα μαζί με μια διαδικασία η οποία είναι ανάλογη στο αγόρασμα ξένου ισχύον νομίσματος. Η ηλεκτρονική εκπροσώπηση του αποθέματος μπορεί να ναι ανώνυμη ή να ναι γνωστή η ταυτότητά του. Στην παρούσα κατάσταση τυφλές υπογραφές χρησιμοποιούνται και η ταυτότητα του πελάτη δεν φανερώνεται, επειδή στις τελευταίες καταστάσεις χρησιμοποιούνται πιο γενικές μορφές υπογραφών και η ταυτότητα του πελάτη πάντα αποκαλύπτεται. Από την στιγμή που κάνει συναλλαγές με την ηλεκτρονική εκπροσώπηση ρευστού χρήματος είναι πιθανό να ξοδέψει το ίδιο ποσό χρημάτων περισσότερο από μια φορά. Έτσι περαιτέρω cash schemes έχουν εγκατασταθεί για να εμποδίσουν το διπλό ξόδεμα. Ηλεκτρονικά συστήματα εξόφλησης μπορεί να ισοδυναμούν με τις παραδοσιακές πιστωτικές κάρτες ή και τις επιταγές. Εδώ η κρυπτογραφία χρησιμοποιείται για να εμποδίσει την μετάδοση μιας τέτοιας πληροφορίας όπως το νούμερο του ποσού του πελάτη ή το ποσό των χρημάτων του. Επίσης , ψηφιακές υπογραφές έχουν αντικαταστήσει τις χειρόγραφες υπογραφές.

1.2.1.2 Πρωτόκολλο IKP

Το πρωτόκολλο Internet Keyed Payment είναι μια αρχιτεκτονική η οποία αναπτύχθηκε από τον IBM’s T.J Watson Research Center και Zurich Research εργαστήριο. Σκοπός αυτού του σχήματος είναι να παρέχει ασφάλεια στα συστήματα καταβολής τα οποία περιλαμβάνει 3 ή περισσότερες ομάδες. Συναλλαγές μεταξύ αγοραστών και πωλητών γίνεται από μια βάση «credit card» και η έγκριση εκτελείται από ένα τρίτο κομμάτι που καλείται «acquirer», όπου είναι συχνά σύστημα πιστωτικής κάρτας ή μια τράπεζα. Το κοινό κλειδί παρέχει ασφάλεια στο πρωτόκολλο.

1.2.1.3 Πρωτόκολλο SET

Το Secure Electronic Transaction πρωτόκολλο είναι μια αρχιτεκτονική αναπτυγμένη από την Visa και MasterCard. Σκοπός της είναι να παρέχει εμπόρους και πελάτες μαζί με εμπιστοσύνη για bankcard

συναλλαγές πάνω από ένα ανοικτό δίκτυο. Το SET παρέχει ασφαλής ηλεκτρονικές αγορές και παρέχει την ικανότητα αίτησης είτε έγκρισης πληρωμών είτε πιστοποιητικό ταυτότητας.

1.2.1.4 Mondex

Το Mondex είναι ένα σχήμα ηλεκτρονικού ρευστού χρήματος το οποίο μπορεί να χρησιμοποιηθεί στις καθημερινές συναλλαγές ρευστού χρήματος. Περιέχει μια μοναδική αρχιτεκτονική που την κάνει πιο λειτουργική σε σύγκριση με άλλο σχήμα ηλεκτρονικού χρήματος. Με το Mondex το τρέχων χρήμα αποθηκεύεται σε μια smartcard, η οποία είναι μια πλαστική κάρτα όπως η πιστωτική κάρτα όπου περιέχει ένα microchip για αποθήκευση πληροφοριών. Χρήματα μπορεί να μεταφερθούν από κάρτα σε κάρτα σε οποιοδήποτε ποσό σε οποιαδήποτε χρονική στιγμή. Υπάρχουν πολλά πλεονεκτήματα που παρέχει το Mondex: μπορεί να μεταφερθεί μέσο Internet ή μέσο μιας τηλεφωνικής γραμμής, το χρήμα μπορεί να κλειδωθεί στην κάρτα Mondex χρησιμοποιώντας κωδικό διαλεγμένο από τον χρήστη και το microchip περιέχει το ρεκόρ των τελευταίων 10 συναλλαγών που έχουν γίνει. Από την άλλη ένα μεγάλο μειονέκτημα είναι ότι όταν το Mondex χάσει κάποιο ποσό τότε και το απόθεμα έχει χάσει. Το σύστημα Mondex έχει γίνει παγκοσμίως δεκτό και ήδη χρησιμοποιείται σε ορισμένα σημεία του κόσμου.

1.2.1.5 Micro Συναλλαγές

Οι Micro-Συναλλαγές είναι πληρωμές όπου η αξία των συναλλαγών είναι αρκετά μικρή σε σύγκριση με τις normal συναλλαγές. Σε τέτοιες περιπτώσεις το κόστος υπολογισμού για πιο αποδοτικό χειρισμό αυτών των ποσών είναι πολύ μεγάλο. Σαν αποτέλεσμα ένα σύστημα micro συναλλαγής απαιτεί μια ‘παρτίδα’ συναλλαγών με κάποιο ρίσκο όσο αφορά την ασφάλεια.

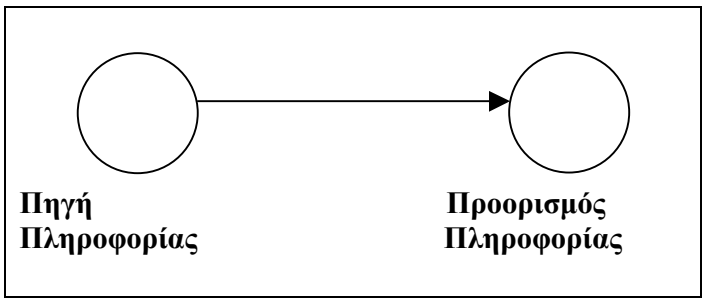
1.3 Σενάρια Επίθεσης

1.3.1 Επιθέσεις Ασφαλείας

Η εκρηκτική ανάπτυξη των συστημάτων computer και οι μεταξύ τους αλληλοσυνδέσεις μέσο δικτύων έχει αυξήσει την ανάγκη για προστασία των

πηγών πληροφοριών από οποιαδήποτε επίθεση που μπορεί να παραβιάσει την αυθεντικότητά τους. Επιπλέον λαμβάνοντας υπόψη ότι μεγάλη πλειοψηφία των οργανισμών εξαρτάται από την ασφάλεια ενσύρματης ή ασύρματης μετάδοσης της πληροφορίας. Έτσι η ανάγκη για επιβολή ασφαλείας του δικτύου έχει γίνει σήμερα κάτι σαν σταυροφορία.

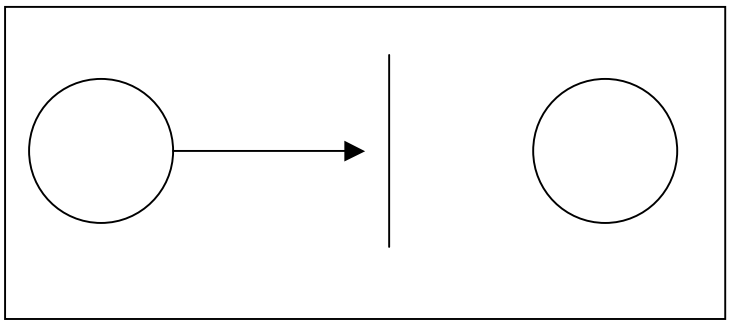
Στις μέρες μας αναφορές επιθέσεων στην ασφάλεια των υπολογιστών έχει αποδειχθεί ότι είναι πολύ απλή. Σε ένα δίκτυο ενός υπολογιστή η πληροφορία με την μορφή κειμένου, συμβόλων, απεικόνισης, μουσικής ή και ακόμη στοιχεία φωνής, μεταδίδεται από το ένα σημείο στο άλλο. Η κανονική ροή αυτής της πληροφορίας διασφαλίζεται όταν και η μυστικότητα και η ακεραιότητα είναι εγγυημένες. Μια ομαλή επικοινωνία φαίνεται στο παρακάτω σχήμα:



Σχήμα 1.1 Κανονική ροή

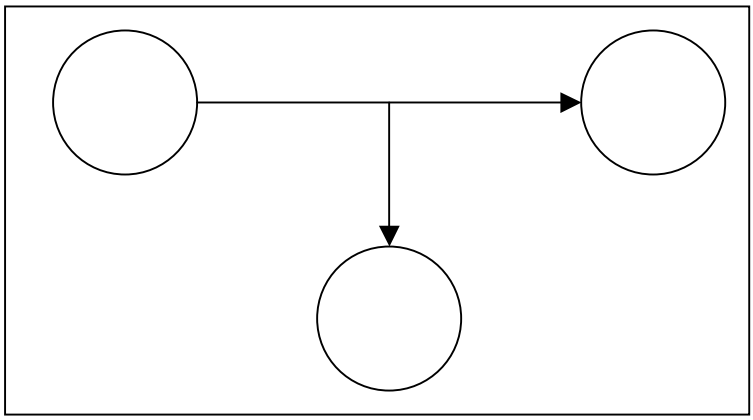
Αλλά η πιθανότητα ότι μη εξουσιοδοτημένες ενέργειες μπορεί να διακόψουν την πορεία των δεδομένων πάντα υπάρχει. Στην πραγματικότητα υπάρχουν πολλοί τρόποι κρυφοκοιτάγματος:

(α). <u>Διακοπή</u>, είναι η επίθεση όπου η πληροφορία δέχεται μια αλλοίωση και έτσι γίνεται άχρηστη. Είναι μια επίθεση ως προς την διαθεσιμότητα. Τέτοιες επιθέσεις είναι το κόψιμο της γραμμής επικοινωνίας και ελευθερώνει το σύστημα διαχείρισης φακέλου.
Το σχήμα 1.2 δείχνει τον τρόπο αυτό:



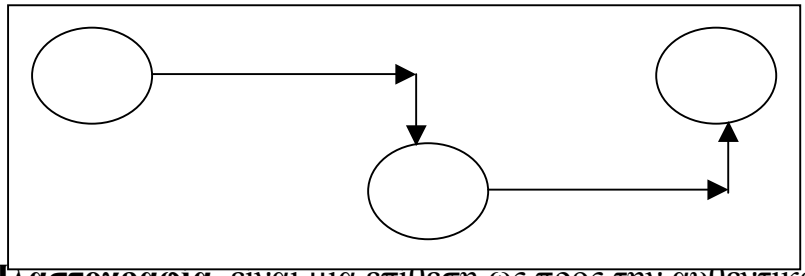
Σχήμα 1.2 Διακοπή

(β). <u>Ανακοπή πορείας</u>, είναι μια επίθεση ως προς την εμπιστοσύνη. Μια μη εξουσιοδοτημένη ομάδα η οποία έχει πρόσβαση σε μεμονωμένες εκπομπές πάνω σε μια γραμμή επικοινωνίας χρησιμοποιώντας hardwire συνδέσεις.
Το σχήμα 1.3 μας δείχνει την ανακοπή πορείας

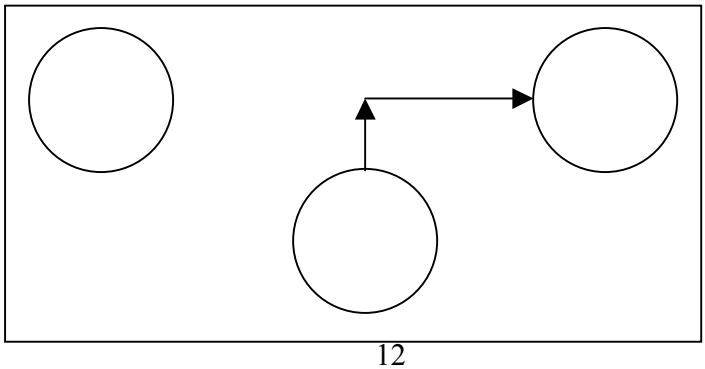


Σχήμα 1.3 Ανακοπή πορείας

(γ). <u>Μετατροπή</u>, είναι επίθεση ακεραιότητας. Με αυτόν τον τρόπο επίθεσης ο αντίπαλος όχι μόνο ανακόπτει την πορεία της εκπεμπόμενης πληροφορίας αλλά μπορεί να την μεταβάλλει την ίδια χρονική στιγμή. Το σχήμα 1.4 μας δείχνει την Μετατροπή



(δ). <u>Πλαστογραφια,</u> είναι μια επίθεση ως προς την αυθεντικότητα της πληροφορίας. Ο επιτιθέμενος απλώς μπαίνει και πλαστογραφεί την πληροφορία. Το σχήμα 1.5 μας δείχνει την πλαστογραφία



Σχήμα 1.5 Πλαστογραφία

Η ανακοπή πορείας θεωρείται «παθητική» επίθεση. Αυτή είναι μια επίθεση που περιλαμβάνει μόνο κρυφάκουσμα και όχι μετατροπή της πληροφορίας που μεταδίδεται. Η ανακοπή πορείας, η μετατροπή και η πλαστογραφία είναι απόρρητα στην κατηγορία της «παθητικής» επίθεσης. Σε μια δραστική επίθεση, ο αντίπαλος αλλάζει την εκπεμπόμενη πληροφορία ή εισάγει πληροφορία στο κανάλι μετάδοσης.

1.3.2 Έγκλημα Κυβερνοχώρου

Η οικονομική φύση του Internet σε συνδυασμό με την φιλική χρήση και την ευρέως απλωμένη ανάγκη για τις διευκολύνσεις που παρέχει το έχουν κάνει παγκοσμίως χρήσιμο. Ένας νέος ηλεκτρονικός κόσμος υψωθεί και η μεγάλη ανάγκη για εδραίωση εμπιστοσύνης στην ηλεκτρονική ασφάλεια παραμένει ακόμη μεγάλο ενδιαφέρον. Το έγκλημα του Κυβερνοχώρου έρχεται να απειλήσει την εμπιστοσύνη και την λειτουργικότητα προκαλώντας πολλές απώλειες στον κόσμο των ηλεκτρονικών business. Υπάρχουν 3 ειδών εγκλήματα Κυβερνοχώρου

(α) <u>Αυθαίρετη επίσκεψη</u>, οι αντίπαλοι προσπαθούν να ελιχθούν στο δίκτυο και να προκαλέσουν πολλές απώλειες και ζημίες.

(β) <u>Cracking,</u> συστήματα computer καταρρέουν ή προγραμματίζονται και φάκελοι τροποποιούνται έτσι ώστε να μολύνονται εύκολα από ιούς.

(γ) <u>Hacking,</u> αυτό πραγματοποιείται μέσο κάποιων συνδετικών κρίκων του Internet και σκοπός του επιτιθέμενου είναι απλώς να ικανοποιήσει την ανάγκη του για διασκέδαση.

Γενικά μια hacking επίθεση μπορεί να πραγματοποιηθεί ακολουθώντας 4 βασικά βήματα, μερικά από αυτά ίσως χρειαστεί να επαναληφθούν:

Α. Ένα hack σχέδιο σχεδιάζεται αφού ο επιτιθέμενος έχει συγκεντρώσει όσες περισσότερες πληροφορίες μπορεί για το στόχο. Αυτό μπορεί να επιτευχθεί παρουσιάζοντας μια ακολουθία μικρών επιθέσεων.

Β. Το δεύτερο βήμα είναι να κερδίσει μια αρχική πρόσβαση στο σύστημα του στόχου με ένα ευθύ ή πλάγιο τρόπο. Για να κερδίσει την

αρχική πρόσβαση, ο hacker μπορεί είτε να αναφέρεται στο σύστημα στέλνοντας mail κοριό ή να χρησιμοποιεί την μέθοδο «ftp».

Γ. Το επόμενο βήμα του hacker είναι να κερδίσει πλήρη πρόσβαση στο σύστημα. Με σκοπό να δημιουργήσει μια κατάλληλη ευκαιρία για πλήρη πρόσβαση, ο επιτιθέμενος μπορεί να χρησιμοποιεί περαιτέρω ιούς ή να εκμεταλλευθεί κάποιο πλεονέκτημα αδυναμίας που παρουσιάζει το σύστημα, που έχει ανακαλύψει ο ίδιος ότι το σύστημα φαίνεται να έχει. Σε αυτό το στάδιο ο hacker εύκολα μπορεί να συμβιβαστεί με την μυστικότητα και το ιδιωτικό περιβάλλον του συστήματος.

Δ. Το τελευταίο βήμα είναι να μετακινήσει όλες τις πιθανές ανιχνεύσεις που μπορεί να προσκομιστούν στη επίθεση και ταυτόχρονα να εγκαταστήσει ‘πίσω πόρτες ‘ για περαιτέρω επιθέσεις. Όταν ολοκληρωθεί και αυτό το βήμα, τότε ο hacker μπορεί να αναφέρει ότι το σύστημα είναι δικό του.

Παρόλο που έχουν γίνει μεγάλες προωθήσεις στο θέμα της προστασίας του δικτύου, η απειλή για το έγκλημα του Κυβερνοχώρου και το hacking είναι ακόμη ζωντανό. Αναφορές των Κυβερνοτρομοκρατών έρχονται να μας δείξουν ότι η ασφάλεια είναι τρωτή:

- Κατά την διάρκεια του πολέμου στον κόλπο, Δανοί hackers έκλεψαν πληροφορίες για κινήσεις Αμερικανικών στρατευμάτων από τους υπολογιστές του Αμερικάνικου Υπουργείου Εθνικής Άμυνας και προσπάθησαν να το πουλήσουν σε Ιρακινούς, που σκέφτηκαν ότι ήταν απάτη και αρνήθηκαν.

- Το Μάρτιο του 1997 μια 15 άχρονη από την Κροατία εισχώρησε στους υπολογιστές της Αμερικάνικης Αεροπορίας στο Guam.

- Το 1997 και 1998 ένας νεαρός Ισραηλινός που αυτοαποκαλούταν “The Analyzer”, εισέβαλε στους υπολογιστές του Αμερικάνικου Πενταγώνου με την βοήθεια εφήβων από την Καλιφόρνια. Ο Ehud Tenebaum κατηγορήθηκε στην Ιερουσαλήμ τον Φεβρουάριο του 1999 για κατασκοπεία και για προξένηση βλαβών στα συστήματα υπολογιστών.

- Τον Φεβρουάριο του 1999, άγνωστοι hackers πήραν τον έλεγχο ενός Βρετανικού δορυφόρου επικοινωνιών και απαίτησαν χρήματα για να επιστρέψουν τον έλεγχο του δορυφόρου. Αυτό το γεγονός ο Βρετανικός στρατός το αρνήθηκε.

- Ο Πρόεδρος Κλίντον ανακοίνωσε ότι τον Φεβρουάριο του 1999 1.46 δισεκατομμύρια $ συμφωνήθηκαν για την προστασία του

κυβερνητικού συστήματος. Ιδιαίτερα αφορά το Πεντάγωνο, τον πιο ισχυρό στρατό του κόσμου. Το Υπουργείο Αμύνης αναγνωρίζει ότι γίνονται 60 με 80 επιθέσεις τη μέρα, παρόλο που υπάρχουν αναφορές για πολύ περισσότερες.

● Σύμφωνα με το British Broadcasting Corp. ένας hacker υπερφόρτωσε ένα δορυφόρο της NASA και απείλησε να αποδιοργανώσει τις επικοινωνίες με τους αστροναύτες κατά την διάρκεια μιας αποστολής τον Σεπτέμβριο του 1997. Η NASA αρνήθηκε αυτή την αναφορά και δέχθηκε ότι υπήρχε μια δια διακοπή στην επικοινωνία, από επίθεση hacker, αλλά σε στιγμή που δεν απειλήθηκαν οι ζωές του πληρώματος.

Όπως καταλαβαίνουμε, παράνομες δραστηριότητες στο Internet είναι παγκόσμιες και οι επιπτώσεις πολύ ζωτικές, ιδιαίτερα όταν top-secret πληροφορίες απειλούνται ή ακόμη περισσότερο όταν απειλούνται ανθρώπινες ζωές.

1.3.3 WAP και Επιδράσεις

Με την βοήθεια των WAP κινητών τηλεφώνων, οι χρήστες μπορούν και εξοπλίζονται με την ικανότητα να έχουν πρόσβαση σε διευκολύνσεις του Internet, σε υπηρεσίες του e-mail, ή ακόμη και για ηλεκτρονικές συναλλαγές. Από την άλλη ασύρματες επικοινωνίες δεδομένων συστήνουν την υπόθεση μη ανιχνεύσιμου κρυφακούσματος. Ισχύοντα WAP τερματικά δεν μπορούν να μολυνθούν εύκολα από τους παραδοσιακούς ιούς, αλλά από τότε που έγιναν περισσότερο λειτουργικά περαιτέρω τρωτά σημεία θα εμφανιστούν.

1.4 Ηλεκτρονικός κόσμος σε δράση

Το χαμηλό κόστος του Internet σε συνδυασμό με την ευκολία που κάνει κανείς συναλλαγές έχουν φέρει τις ηλεκτρονικές business σε μια εκρηκτική αύξηση. Το ηλεκτρονικό mail είναι η πιο διαδεδομένη μορφή αίτησης και έτσι, η ασφάλεια της εμπιστοσύνης και της αυθεντικότητας είναι ένα θέμα με μεγάλο ενδιαφέρον. Το PGP (Pretty Good Privacy) και S/MIME (Secure/Multipurpose Internet Mail Extension) αναπτύχθηκαν για να αντιμετωπίζουν θέματα ασφαλείας των mail.Επίσης η μεγάλη χρήση του World Wide Web και οι ασύρματες επικοινωνίες, φέρνει νέες εκτιμήσεις στο Web και στην ασφάλεια κινητής τηλεφωνίας. Η ασφάλεια στο επίπεδο IP (Internet Protocol), που είναι και το βασικό στοιχείο, είναι επίσης αυξανομένου ενδιαφέροντος. Με σκοπό να αντιμετωπιστεί αυτή η βαριά ανάγκη για ηλεκτρονική ασφάλεια, ένας μεγάλος αριθμός από εταιρείες που

παρέχουν προϊόντα για ασφάλεια έχουν πάρει τα μέτρα τους. Εταιρείες όπως η Baltimore, iD2, Telcordia, Trintech, Microsoft, IBM, Entrust και Certicom, δουλεύουν με σκοπό την ηλεκτρονική ασφάλεια και τα προϊόντα τους υπόσχονται πολλά σε ότι αφορά τις επιθέσεις (περισσότερα στο κεφ 3). Την ίδια στιγμή επαγγελματικές κοινωνίες, ινστιτούτα ερευνών και υπηρεσίες παρουσιάζουν διάφορες έρευνες στο πως μπορούν να προστατέψουν το επικοινωνιακό δίκτυο. Το Internet Crimes Group Inc. εγκαθιστά μια νέα προσπάθεια στην έρευνα για την παρεμπόδιση ή ακόμη για την ανακάλυψη των επιθέσεων και των ανάρμοστων δραστηριοτήτων. Όλες αυτές οι εταιρείες εργάζονται πάνω σε βάσεις κρυπτογραφικών μεθόδων και εφαρμογών, με σκοπό να βρουν τρόπους να προστατέψουν το software και άλλες ψηφιακές δραστηριότητες. Χωρίς αμφιβολία έχουν πολλά να υποσχεθούν για την μάχη ενάντια στις επιθέσεις στο δίκτυο και σε άλλες απειλές στο μέλλον.

1.5 Επίλογος

Η εγκατάσταση των τηλεπικοινωνιακών δικτύων μέσο καναλιών έχει πλέον ευρέως επεκταθεί. Μεμονωμένες εταιρείες και οργανισμοί είναι μέλη του ηλεκτρονικού κόσμου που γενικά βρίσκεται σε πρόοδο. Το Internet καθιστά την ανάπτυξη των ηλεκτρονικών business, ηλεκτρονικό εμπόριο και τις ηλεκτρονικές συναλλαγές. Επιπλέον ηλεκτρονικές συναλλαγές, πληρωμές ή ακόμη πρόσβαση σε υπηρεσίες του Internet μέσο συσκευών WAP μπορεί εύκολα να πραγματοποιηθεί. Η είσοδος του ηλεκτρονικού χρήματος μαζί με το special cash schemes γνωστά ως Mondex, χρησιμοποιούνται για να κάνουν τις καθημερινές συναλλαγές πιο λειτουργικές. Υιοθετώντας ειδικά πρωτόκολλα διαφυλάσσουν την ασφάλεια των ηλεκτρονικών συναλλαγών. Αυτά τα πρωτόκολλα είναι αρχιτεκτονικές που σκοπό έχουν την ασφάλεια στις ηλεκτρονικές συναλλαγές και πληρωμές.

Η βαριά ανάπτυξη των εφαρμογών του Internet έρχεται αντιμέτωπη με ένα μεγάλο αριθμό απειλών που αφορούν την ασφάλεια. Η αυθαίρετη επίσκεψη, το hacking και cracking είναι οι πιο κοινές έννοιες επίθεσης στο Internet. Από τότε που τύπος τέτοιου εγκλήματος μπορεί να προκαλέσει μεγάλες απώλειες στον ηλεκτρονικό επιχειρηματικό κόσμο, η προστασία της ηλεκτρονικής ασφάλειας έχει γίνει θέμα πρωτίστης σημασίας. Με στόχο να βοηθηθεί η προσπάθεια αντιμετώπισης του εγκλήματος του κυβερνοχώρου, νέα προϊόντα ασφαλείας έχουν εμφανιστεί και νέες εταιρείες και υπηρεσίες έχουν συγκροτηθεί.

Στα επόμενα κεφάλαια θα μελετηθούν έννοιες όπως κρυπτογραφία, κρυπτοανάλυση και κρυπτοσυστήματα.

ΚΕΦ 2: Κρυπτολογία Και Ασφάλεια Δεδομένων

2.1 Εισαγωγή

Η ασφάλεια της ηλεκτρονικής πληροφορίας είναι χωρίς καμία αμφιβολία το πιο συχνά μελετημένο θέμα από τότε που οι επικοινωνίες γίνονται μέσο δικτύων. Με σκοπό να προστατέψουμε την ασφάλεια των δεδομένων, η επιστήμη της κρυπτογραφίας έρχεται να εισάγει ένα σχήμα απόκρυψης δεδομένων. Ειδικά συστήματα κρυπτογράφησης και αλγορίθμων έχουν εφευρεθεί. Μέχρι τώρα πολλά πλεονεκτήματα έχουν παρουσιαστεί από ειδικούς κρυπτογραφικούς αλγόριθμους, αλλά η απειλή της κρυπτοανάλυσης ακόμη υπάρχει. Σε αυτό το κεφάλαιο παρέχει μια σύντομη περιγραφή από έννοιες και τεχνικές που υποστηρίζουν την θεωρεία των κρυπτογραφικών συστημάτων. Και η συμβατική κρυπτογράφηση και το δημόσιο κλειδί κρυπτογραφίας θα εξετασθούν σε βάθος. Τέλος μια αναφορά γίνεται επίσης σε χρήσιμες έννοιες επίθεσης για κάθε διαφορετικό αλγόριθμο, μαζί με προτάσεις που αφορούν πως τέτοιες απειλές μπορούν άλλοτε να τις αποφεύγουμε και άλλοτε να τις εξολοθρεύουμε.

2.2 Κρυπτογραφία Και Βασικές αρχές

2.2.1 Βασικές Έννοιες

2.2.1.1 Κρυπτογραφία

Κρυπτογραφία ή κρυπτολογία, από την αρχαία Ελληνική λέξη κρυφογράψιμο, είναι μια αρχαία επιστήμη όπου ο αποστολέας κωδικοποιεί την πληροφορία έτσι ώστε αν ανακοπή η πορεία του προς τον δέκτη τότε ο εισβολέας δεν μπορεί να καταλάβει το περιεχόμενο του. Χάρη στην ανάπτυξη των υπολογιστών και των τηλεπικοινωνιακών δεσμών μεταξύ αυτών δεδομένα μπορούν να μεταφερθούν από το ένα σημείο στο άλλο. Παρεπιπτώντος τα δεδομένα γίνονται πιο τρωτά σε μη εξουσιοδοτημένες προσβάσεις, μετατροπές και κρυφοκοιτάγματα. Η Κρυπτολογία έρχεται να στραφεί προς αυτά τα προβλήματα και να δώσει πληροφορίες για την ασφάλειά και την ιδιωτικότητά τους. Η ανάπτυξη των μοντέρνων

υπολογιστών και η εμφάνιση ειδικών επιστημόνων που μελετάνε σε βάθος την κρυπτολογία, σε έννοιες που δεν ήταν και τόσο ορατές στο παρελθόν.

Η Κρυπτογραφία θεωρείται ότι έχει πολλές μορφές. Μπορεί να χρησιμοποιηθεί με σκοπό την επιβεβαίωση της ταυτότητας ενός μακρινού χρήστη και τελικά να του παρέχει πρόσβαση στο σύστημα. Επίσης συχνά ζητείται η παροχή γνησιότητας: το γνήσιο του μηνύματος θα πρέπει να επιβεβαιώνεται. Ακεραιότητα: ο δέκτης θα πρέπεί να μπορεί να ελέγχει αν η πληροφορία έχει προσβληθεί όταν μεταδίδονταν. Μη απόρριψη:ο αποστολέας δεν θα πρέπει να αρνείται ότι έστειλε το μήνυμα.

Η μεγάλη χρήση των πηγών των υπολογιστών που περιέχουν ιδιωτικές πληροφορίες μαζί με την αυξανόμενη χρήση των δικτύων, συνιστούν την βάση ψαξίματος τεχνικών κρυπτογραφίας. Αρχικά οι μη-κρυπτογράφησης στρατηγικές, όπως η συμπίεση δεδομένων που ανακαλύφθηκε με σκοπό να αυξήσει το μέγεθος της πληροφορίας και να την κάνει λιγότερο τρωτή σε διεισδύσεις. Ο βαθμός ασφαλείας που αποκτιέται υιοθετώντας τέτοιες έννοιες δεν ήταν τόσο ικανοποιητικές έτσι εμφανίστηκε η κρυπτογράφηση. Μαζί με τα δεδομένα κρυπτογράφησης κωδικοποιείται στην αρχή η πληροφορία και αποκωδικοποιείται στον δέκτη. Με αυτόν τον τρόπο το πρόβλημα της ανακοπής της πορείας της πληροφορίας απομακρύνεται σημαντικά.

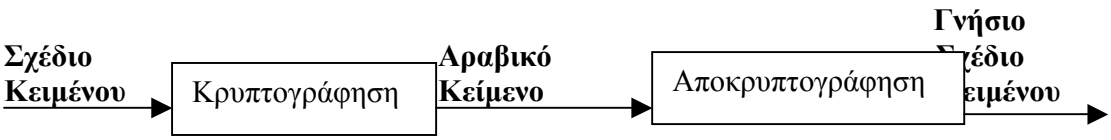
Τον Αύγουστο του 1974, το ινστιτούτο Computer Science and Technology, του National Bureau of Standards (NBS), παρατήρησαν την προφανή και επείγουσα ανάγκη για προστασία των δεδομένων της κυβέρνησης και του ιδιωτικού τομέα και ότι η encryption είναι η μόνη έννοια για προστασία των δεδομένων επικοινωνίας και μια χρήσιμη έννοια για την προστασία αποθηκευμένων δεδομένων. Τον Αύγουστο του 1974 η γνωστή εταιρεία International Business Machines (IBM), υποτάχθηκε σε έναν υποψήφιο αλγόριθμο. Το NBS δέχθηκε βοήθεια από την National Security Agency (NSA), όπου βρήκε δεκτή μόνο τον αλγόριθμο που πήρε από την IBM. Αυτός ο αλγόριθμος ήταν η βάση, για την προτεινόμενη Data Encryption Standard (DES). Τον Ιούλιο του 1997, το DES δοκιμάστηκε και σαν Federal Information Processing Standard (FIPS). Εκτός από το ομοσπονδιακό τμήμα και άλλες υπηρεσίες το Standard μπορούσε να υιοθετηθεί και να χρησιμοποιηθεί από οργανισμούς. Για αυτό τον λόγο το NSB παρείχε τον ιδιωτικό τομέα μαζί με έναν κρυπτογραφικό αλγόριθμο, που είχε ανακαλυφθεί μετά από έντονες προσπάθειες γι σχεδιασμό και επιβεβαίωσης του DES. Επίσης το DES χρησιμοποιήθηκε και από το American National Standards Institute (ANSI).

2.2.1.2 Αλγόριθμοι Κρυπτογράφησης

Ο βασικός σκοπός της κρυπτογραφίας είναι να επινοήσει διαδικασίες μετατροπής μηνυμάτων σε κρυπτογράμματα. Για να επιτευχθεί αυτό χρησιμοποιούνται είτε συστήματα κωδικοποίησης είτε αραβικά συστήματα.

Ένα σύστημα κωδικοποίησης περιλαμβάνει την αντικατάσταση κωδικών λέξεων με τις λέξεις του μηνύματος. Το σύστημα αυτό απαιτεί να υπάρχει ένα βιβλίο με τις κωδικοποιημένες μεταφραζόμενες λέξεις ή φράσεις ή ακόμη και ολόκληρων προτάσεων με το ισοδύναμο κρυπτόγραμμα. Αν το μέγεθος των μηνυμάτων που πρόκειται να μετατραπεί εξαρτάται από το βιβλίο κωδικών, τότε η χρήση τους είναι περιορισμένη.

Σε ένα αραβικό σύστημα είναι πιθανό να μετατραπεί σε κρυπτογράφημα ή κρυπτογραφικό μήνυμα ή κείμενο, σε ένα ενδιάμεσο τύπο γνωστό σαν κρυπτογράφημα όπου η πληροφορία είναι παρόν αλλά κρυμμένη. Ακολουθώντας την κρυπτογράφηση και αποκρυπτογράφηση ο δέκτης ψάχνει να βρει το κρυμμένο μήνυμα. Η κρυπτογράφηση και αποκρυπτογράφηση φαίνεται στο σχήμα 2.1

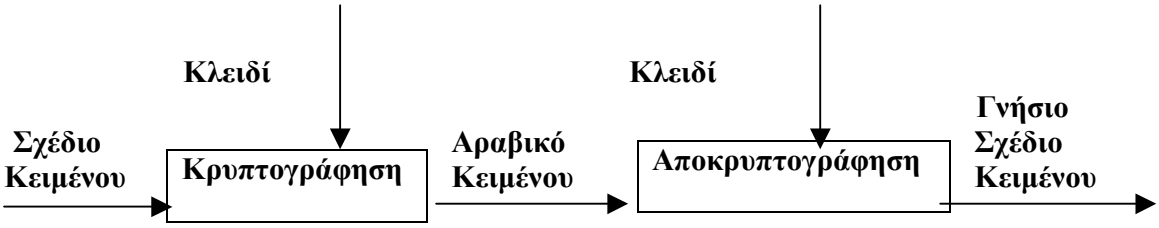


Ο χαρακτήρας Μ χρησιμοποιείται για να δείξει το σχέδιο κειμένου και το C για το κρυπτογραφημένο κείμενο. Η λειτουργία του Ε ενεργεί πάνω στο Μ για να παραχθεί το C:E(M)=C. Στην διαδικασία της αποκρυπτογράφησης γίνεται η αντίστροφη διαδικασία και η λειτουργία της αποκρυπτογράφησης εφαρμόζεται στο κρυπτογραφημένο κείμενο που περιέχει το αρχικό μήνυμα:D(C)=M. Αφού σκοπός της διαδικασίας της κρυπτογράφησης και αποκρυπτογράφησης είναι να ανακαλύπτουν το μήνυμα τότε η επόμενη λειτουργία κρατά το αρχικό μήνυμα: D(E(M))=M.

Στην μοντέρνα κρυπτογραφία η διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης παρουσιάζονται με την βοήθεια ενός κλειδιού του K. Το κλειδί μπορεί να ναι οποιοδήποτε μέσα από ένα μεγάλο εύρος αξιών που καλείται κλειδί-διάστημα. Ανάλογα με τον τρόπο που χρησιμοποιείται το κλειδί, έχουμε 2 ειδών κρυπτογραφικούς αλγόριθμους: τους συμβατικούς ή συμμετρικούς και τους ασυμμετρικούς ή κοινό κλειδί.

Στους συμβατικούς αλγόριθμους τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης είτε είναι κοινά, ή , αν διαφορετικά, είναι τέτοια ώστε κάθε κλειδί μπορεί εύκολα να υπολογιστεί από το άλλο. Έτσι όταν τα

κλειδιά είναι όμοια τότε οι λειτουργίες που γίνονται είναι οι εξής: $E_K(M)=C$, $D_K(C)=M$, και $D_K(E_K(M))=M$. Όταν χρησιμοποιούνται διαφορετικά κλειδιά K_1 και K_2 οι λειτουργίες γίνονται: $E_{K1}(M)=C$, $D_{K2}(C)=M$ και $D_{K2}(E_{K1}(M))=M$. Ένα παράδειγμα συμβατικού αλγορίθμου είναι το DES. Γενικά ο συμβατικός αλγόριθμος παρουσιάζεται όπως το παρακάτω σχέδιο:



Σχήμα 2.2 Ένα Κλειδί Κρυπτογράφησης

Από την άλλη μεριά, το κοινό κλειδί των αλγορίθμων, το κλειδί κρυπτογράφησης είναι διαφορετικό από το κλειδί αποκρυπτογράφησης. Επιπλέον, το κλειδί αποκρυπτογράφησης δεν μπορεί να υπολογιστεί από το κλειδί κρυπτογράφησης. Το κλειδί κρυπτογράφησης, λέγεται και κοινό κλειδί και το αποκρυπτογράφησης λέγεται μυστικό. Το πιο γνωστό κοινό κλειδί αλγορίθμων είναι το RSA και θα εξετασθεί αργότερα.

Το μήκος ενός κρυπτογραφικού αλγόριθμου μας δείχνει το πόσο δύσκολο είναι να σπαστεί το αραβικό σύστημα και να αναγνωριστεί η κρυπτογραφημένη πληροφορία. Για να συμβεί αυτό το κλειδί πρέπει να επιλεχθεί τυχαία και να χρησιμοποιηθεί μόνο μια φορά. Επίσης το μήκος του κλειδιού πρέπει να είναι ικανό ή και καλύτερο από το μήκος του σχεδίου του κειμένου που θα κρυπτογραφηθεί. Υπάρχουν 2 τρόποι να σχεδιαστεί ένας κρυπτοαναλυτικός αλγόριθμος. Ο πρώτος περιλαμβάνει μεθόδους λύσεων χρήσιμες για τον επιτιθέμενο και καθορίζει έναν αριθμό κανόνων που χαλά αυτές τις μεθόδους. Ο δεύτερος βασίζεται στην κατασκευή αλγορίθμων που για να σπαστούν απαιτείται η λύση ενός γνωστού προβλήματος, αλλά δύσκολο να λυθεί. Ο DES αλγόριθμος σχεδιάστηκε υιοθετώντας την πρώτη προσέγγιση, ενώ μερικά κοινά κλειδιά σχεδιάστηκαν με βάση την δεύτερη προσέγγιση.

2.2.1.3 Μπλοκ και Ροή Κρυπτογραφικού Συστήματος

Με ένα μπλοκ κρυπτογραφικό σύστημα δεδομένα κρυπτογραφούνται και αποκρυπτογραφούνται σε μπλοκ, που το μήκος τους είναι προκαθορισμένο από τον σχεδιαστή του αλγορίθμου. Έστω το M είναι το σχέδιο κειμένου. Ένα μπλοκ αραβικό σύστημα ‘σπάει’ το M σε άλλα διαδοχικά μπλοκ M_1,M_2....και κρυπτογραφεί κάθε ένα M_1 με το ίδιο κλειδί

Κ. Αυτό γίνεται ως εξής: $E_K(M)=E_K(M_1)\ E_K(M_2)$….. Κάθε μπλοκ είναι ένα μήκος τυπικών χαρακτήρων.

Η χρήση του αλγορίθμου ροής κρυπτογραφικού συστήματος καθορίζει το μήκος των δεδομένων που πρόκειται να κρυπτογραφηθούν και αποκρυπτογραφηθούν. Το σύστημα 'σπάει' το μήνυμα Μ σε διαδοχικούς χαρακτήρες ή bits m_1, m_2….. και κρυπτογραφεί κάθε ένα m_i μαζί με το στοιχείο k_i μιας ροής κλειδιών $K=k_1k_2$….; και αυτό είναι $E_k(M)=E_{k1}(m_1)E_{k2}(m_2)$

Και οι 2 συμβατικοί αλγόριθμοι και οι αλγόριθμοι δημοσίων κλειδιών καλύπτονται κάτω από την περιοχή των μπλοκ κρυπτογραφ- ικών συστημάτων.

2.3 Στεγανογραφία

Στεγανογραφία είναι μια τεχνική κρυμμένης πληροφορίας ξεχωριστής από την έννοια της κρυπτογραφίας. Αυτή εξυπηρετεί να κρύβει μυστικά μηνύματα σε άλλα μηνύματα, με τέτοιο τρόπο που η ύπαρξη του μυστικού είναι καλά κρυμμένη. Για παράδειγμα, η ακολουθία των πρώτων γραμμάτων της κάθε λέξης του συνολικού μηνύματος μας δείχνει το κρυμμένο μήνυμα. Ιστορικά πολλές άλλες τεχνικές έχουν χρησιμοποιηθεί. Παρακάτω ακολουθούν μερικά παραδείγματα:

- → **Μαρκάρισμα χαρακτήρων:** Διαλεγμένα γράμματα εκτυπωμένων ή γραμμένων κειμένων γράφονται όλα με μολύβι. Τα μαρκαρισμένα δεν φαίνονται εκτός αν το χαρτί το κρατάμε με κάποια γωνία στο φως.
- → **Αόρατη μελάνη:** Ένας αριθμός από υλικά μπορεί να χρησιμοποιηθεί για γράψιμο αλλά να μην αφήνει εμφανή ίχνη μέχρι να θερμανθεί ή με κάποιο χημικό το χαρτί.
- → **Τρύπημα καρφίτσας**: Μικρά τρυπήματα καρφίτσας σε επιλεγμένα γράμματα συχνά όχι εμφανίσιμα εκτός αν κρατάμε το χαρτί μπροστά από το φως.
- → **Διορθωτική κορδέλα γραφομηχανής:** Χρησιμοποιείται μεταξύ τυπωμένων γραμμών μαζί με μια μαύρη κορδέλα, όπου τα αποτελέσματα της εγγραφής μαζί με την διορθωτική κορδέλα είναι ορατά μόνο στο ισχυρό φως.

Η στενογραφία σε σύγκριση με την κρυπτογραφία έχει έναν αριθμό μειονεκτημάτων. Απαιτεί πολλά για να κρύψει μερικά bits

πληροφορίας και όταν το σύστημα αποκαλύπτεται στην ουσία μετά είναι άχρηστο.

2.4 Κρυπτογραφήματα

Ένα κρυπτοσύστημα χωρίζεται σε 2 είδη: στο κρυπτογράφημα αντικατάστασης και στο κρυπτογράφημα μετάθεσης.

2.4.1 Κρυπτογραφήματα Αντικατάστασης

Ένα κρυπτογράφημα αντικατάστασης είναι αυτό όπου τα γράμματα του σχεδίου του κειμένου αντικαθίστανται από άλλα γράμματα ή από νούμερα ή από σύμβολα. Αν το σχέδιο κειμένου αποτελείται από ακολουθία bits, τότε η αντικατάσταση περιλαμβάνει αντικατάσταση των προτύπων bit του κειμένου από πρότυπα bit κρυπτοκειμένου.

2.4.1.1 Μονοαλφαβητικά κρυπτογραφήματα

Η πιο γνωστή χρήση του κρυπτογραφήματος ήταν από τον Ιούλιο Καίσαρα. Αυτό το κρυπτογράφημα αντικαθιστά γράμματα του κειμένου με γράμματα που βρίσκονται 3 θέσεις πιο κάτω στην αλφάβητο. Αυτό είναι γνωστό σαν μονοαλφαβητικό κρυπτογράφημα. Στο σχήμα δίνεται ένα κανονικό σχέδιο κειμένου και ακριβώς από κάτω το κρυπτοκείμενο:

Κείμενο: **ABCDEFGHIJKLMNOPQRSTUVWXYZ**
Κρυπτοκείμενο: **DEFGHIJKLMNOPQRTSUVWXYZABC**

Τα μεταβαλλόμενα νούμερα που χρησιμοποιούνται για να μετατρέψουν ένα σχέδιο κειμένου σε κρυπτοκείμενο αναφέρονται συνήθως ως κλειδί. Το μειονέκτημα είναι ενός τέτοιου συστήματος είναι ότι ένα μπορεί να δεχτεί μεγάλη επίθεση απλώς δοκιμάζοντας τα 25 πιθανά κλειδιά. Ένας άλλος τρόπος είναι δοκιμάζοντας την λειτουργικότητα της χρησιμοποιούμενης γλώσσας όταν η φύση του σχεδίου του κειμένου είναι γνωστή. Η επίθεση αυτή είναι γνωστή και σαν συχνότητα ανάλυσης. Μια τέτοια επίθεση συχνότητας ανάλυσης μπορεί να γίνει μόνο με το απλό τρέξιμο ενός προγράμματος το οποίο μας δείχνει την συγγενική συχνότητα των γραμμάτων του μηνύματος.

2.4.1.2 Πολυαλφαβιτικό Κρυπτογράφημα

Τα πολυαλφαβητικά κρυπτογραφήματα είναι οι πιο δυνατοί τύποι κρυπτογραφημάτων αντικατάστασης. Σε τέτοια συστήματα το σχέδιο κειμένου κρυπτογραφείται χρησιμοποιώντας κάθε φορά διαφορετικοί μονοαλφαβητική αντικατάσταση. Ένα σύνολο κανόνων μονοαλφαβητικής αντικατάστασης δημιουργείται και ένα συγκεκριμένο κλειδί καθορίζει ποιοι κανόνες θα χρησιμοποιούνται κάθε φορά. Ένας από τους πιο απλούς τύπους κρυπτογραφήματος είναι ο Vigenere. Σε αυτό το κρυπτογράφημα το σύνολο των κανόνων αντικατάστασης αποτελείται από 26 Caesar κρυπτογραφήματα, μαζί με μεταβάσεις από 0 σε 25. Κάθε κρυπτογράφημα μαρτυράτε από ένα κλειδί γράμμα, το οποίο είναι το γράμμα του κρυπτοκειμένου το οποίο αντικαθιστά το γράμμα a του σχεδίου κειμένου. Έτσι το κρυπτογράφημα Caesar μαζί με μια μετάβαση από 3 ενδείκνυται να ναι το κλειδί d. Για να βοηθηθεί αυτή η λειτουργικότητα αυτού του σχήματος κατασκευάστηκε ένα καλούπι γνωστό και σαν πλαστική εικόνα Vigenere. Κάθε ένα από τα 26 κρυπτογραφήματα είναι απλωμένα οριζόντια μαζί με το κάθε γράμμα κλειδί του κρυπτογραφήματος στα αριστερά του. Ένα κανονικό αλφάβητο για το σχέδιο κειμένου τρέχει κατά μήκος της κορυφής. Η πορεία της κρυπτογράφησης είναι απλή: Δίνεται ένα γράμμα κλειδί x και ένα γράμμα σχεδίου κειμένου y, το γράμμα κρυπτοκειμένου θα βρίσκεται στην γραμμή με επιγραφή x και στην στήλη με επιγραφή y. Σε αυτή την περίπτωση το κρυπτοκείμενο θα ναι V. Με σκοπό να κρυπτογραφήσουμε ένα μήνυμα, ένα κλειδί με μήκος ίδιο με το μήκος του μηνύματος απαιτείται. Για παράδειγμα αν η λέξη κλειδί είναι ABC και το μήνυμα JOHN IS GOOD τότε το κρυπτοκείμενο θα ναι το ακόλουθο:

Σχέδιο Κειμένου:	**JOHN IS GOOD**
Κλειδί:	**ABCA BC ABCA**
Κρυπτοκείμενο:	**JPJN JU GPQD**

Η αποκρυπτογράφηση είναι εξίσου απλή. Η λέξη κλειδί ξανά αναγνωρίζει την γραμμή. Η θέση του γράμματος του κρυπτοκειμένου καθορίζει την στήλη και το γράμμα του σχεδίου του κειμένου είναι στην κορυφή της στήλης.

Σε αντίθεση με τα μονοαλφαβητικά κρυπτογραφήματα, τα πολυαλφαβητικά δεν είναι και τόσο τρωτά στις επιθέσεις συχνοτήτων

ανάλυσης. Αλλά το σύστημα μπορεί να σπαστεί σε περίπτωση που ο επιτιθέμενος μαντέψει σωστά το μήκος του κλειδιού. Ένας τρόπος εξάλειψης της ηρεμίας μια επίθεσης είναι να χρησιμοποιούμε μη επαναλαμβανόμενα κλειδιά. Το Vigenere προτείνει ένα σύστημα αυτόματου κλειδιού όπου το τρέχων κλειδί είναι μια ακολουθία της λέξης κλειδί και του σχεδίου κειμένου.

2.4.2 Κρυπτογραφήματα Μετακίνησης

Τα κρυπτογραφήματα μετακίνησης ακολουθούν ειδικές τεχνικές στις οποίες το κανονικό πρότυπο των χαρακτήρων αλλάζει. Ένα απλό παράδειγμα ενός κρυπτογραφήματος μετακίνησης μπορεί να περιλαμβάνει αντιστροφή του μηνύματος ή τη διαίρεσή του σε ζευγάρια και ανταλλαγή αυτών. Γενικά οι τεχνικές που υιοθετούνται είναι: αντιστροφή μηνύματος, γεωμετρικά πρότυπα, μετακίνηση διαδρομής και κιονοειδής μετακίνηση.

Αφού τα γράμματα του κρυπτοκειμένου είναι είναι τα ίδια σαν αυτά του σχεδίου κειμένου, μια ανάλυση συχνότητας γράμματος καθιστά ικανή επίθεση στο κρυπτογράφημα μετακίνησης. Με σκοπό να εξαλείψουμε μια επιτυχή επίθεση, μια δεύτερη μετάθεση του κρυπτοκειμένου προτείνεται. Γενικά τα κρυπτογραφήματα μετακίνησης είναι τρωτά σε κρυπτοανάλυση και μπορεί να απαιτεί μηνύματα με καθορισμένο μήκος. Γι' αυτό τα κρυπτογραφήματα αντικατάστασης είναι πιο πολύ εξαπλωμένα.

2.4.3 Ρότορες

Οι Ρότορες είναι ταξινομημένοι σε κατηγορίες όπου τα διάφορα στάδιά της κρυπτογράφησης χρησιμοποιούνται για εφαρμογή. Η μηχανή αποτελείται από ένα σύνολο στρεφόμενων κυλίνδρων μέσα από τα οποία μπορούν να περνάνε ηλεκτρικοί παλμοί. Κάθε ρότορας είναι μια αυθαίρετη μετάθεση του αλφαβήτου και έχει 26 pins εισόδου και 26 pins εξόδου, μαζί με εσωτερική καλωδίωση που συνδέει κάθε pin εισόδου με κατάλληλο pin εξόδου. Κάθε ρότορας εφαρμόζει μια εκδοχή του κρυπτογραφήματος Vigenere και κάθε ρότορας παρουσιάζει μια απλή αντικατάσταση. Η ισχύς αυτών των μηχανών εξαρτάται από την χρήση πολλαπλών κυλίνδρων, στους οποίους τα pins εξόδου του ενός κυλίνδρου συνδέονται με τα pins εισόδου του αμέσως επόμενου. Για παράδειγμα σε ένα 4-rotor machine ο πρώτος ρότορας μπορεί να αντικαταστήσει το 'F' με το 'A', ο δεύτερος το 'Y' με το 'F', ο τρίτος το 'E' με το 'Y' και ο τρίτος το 'C' με το 'E'. Σε αυτή την μηχανή το 'C' θα ναι η έξοδος του κρυπτοκειμένου. Έτσι μερικοί από τους Ρότορες μετακινούνται και έτσι την επόμενη φορά οι αντικαταστάσεις θα ναι διαφορετικές. Η κρυπτοανάλυση στους Ρότορες δεν

είναι εύκολο κεφάλαιο και γίνεται ακόμη λιγότερο ορατό όταν κάθε ρότορας έχει διαφορετικό αριθμό θέσεων.

Η πιο γνωστή συσκευή ρότορα είναι η Enigma. Η Enigma χρησιμοποιήθηκε από τους Γερμανούς στον 2ο παγκόσμιο πόλεμο για στρατιωτικούς σκοπούς. Είχε 3 Ρότορες, διαλεγμένους από ένα σύνολο των 5, ένα πώμα χαρτονιού που μετάλλασσε ελαφρά το σχέδιο κειμένου, και ένα ρότορα απεικόνισης που έκανε κάθε ρότορα να ενεργεί στο γράμμα του σχεδίου κειμένου 2 φορές. Μετά από πολλές προσπάθειες και επιθέσεις μια ομάδα Πολωνών κρυπτογράφων κατάφερε να σπάσει το Γερμανικό Enigma.

2.5 Θεωρητικές Πληροφορίες Για Το Background

Το κομμάτι αυτό αναφέρεται σε κύρια σημεία της θεωρίας πληροφοριών και τον τρόπο που αυτές μπορούν να χρησιμοποιηθούν στην περιοχή της κρυπτογραφίας.

2.5.1 Εντροπία Και Αβεβαιότητα

Η θεωρεία της πληροφορίας μετρά το ποσό της πληροφορίας σε ένα μήνυμα από το ελάχιστο αριθμό bits που χρειάζεται για να κωδικοποιήσει όλες τις πιθανές έννοιες του μηνύματος, υποθέτοντας όλα τα εξίσου όμοια μηνύματα. Η περιοχή sex σε μια βάση δεδομένων, για παράδειγμα, περιέχει μόνο ένα bit πληροφορίας, γιατί μπορεί να κωδικοποιηθεί με ένα bit (το αρσενικό παριστάνεται με το ‘0’ και το θηλυκό με το ‘1’). Αν η περιοχή παριστάνεται από χαρακτήρα ASCII κωδικοποιώντας τους χαρακτήρες strings ‘MALE’ και ‘FEMALE’, θα χρειαστεί περισσότερος χώρος αλλά θα περιέχει το ίδιο ποσό πληροφορίας. Η εντροπία του μηνύματος M, που σημειώνεται ως H(M) μετρά το ποσό της πληροφορίας του μηνύματος. Στην περίπτωσή μας η πληροφορία του μηνύματος δείχνει ότι το sex θα ναι 1 bit. Γενικά η εντροπία του μηνύματος που μετριέται σε bits είναι $\log_2 n$ όπου n ο αριθμός των πιθανών εννοιών.

Η εντροπία του μηνύματος μπορεί επίσης και να χρησιμοποιηθεί και σαν μέτρο για την ‘ αβεβαιότητα’. Αυτή είναι ο αριθμός των bits που χρειάζονται για να ανακτηθούν όταν το μήνυμα έχει παραποιηθεί κατά την διάρκεια της μετάδοσης ή είναι κρυμμένο σε κρυπτοκείμενο. Για παράδειγμα αν το σχέδιο κειμένου είναι είτε ‘MALE’ ή ‘FEMALE’ και το κρυπτοκείμενο είναι ‘W$GH3F’ τότε η αβεβαιότητα του κρυπτοκειμένου

θα ναι 1. Σε περίπτωση που η κρυπτοανάλυση ξέρει το ‘sex’ του σχεδίου κειμένου τότε θα χρειαστεί μόνο ένα bit για να αναγνωρίσει το σχέδιο κειμένου.

2.5.2 Πλεονασμός

Για μια δοσμένη γλώσσα, η αναλογία της γλώσσας για μηνύματα με μήκος N οροθετείται από **r=H(M)/N**. Αυτό μετρά τον μέσο όρο bits των αριθμών πληροφορίας σε κάθε χαρακτήρα. Για μεγάλο N, το r εκτιμάται για Αγγλικό εύρος από 1.0 bits/γράμμα σε 1.5 bits/γράμμα.

Η καλύτερη αναλογία της γλώσσας είναι ο μέγιστος αριθμός των bits της πληροφορίας που μπορεί να κωδικοποιηθεί σε κάθε χαρακτήρα, παίρνοντας όλες τις πιθανές αναλογίες ομοιότητας των χαρακτήρων. Αν υπάρχουν L χαρακτήρες στην γλώσσα τότε η καλύτερη αναλογία γλώσσας είναι: $R=\log_2 L$. Αυτή είναι η μέγιστη εντροπία των μεμονωμένων χαρακτήρων. Για Αγγλικά, $R=\log_2 26=4.7$ bits/γράμμα.

Ο ‘Πλεονασμός D’ μιας γλώσσας με εύρος r και απόλυτο εύρος R ισοδυναμεί με D=R-r. Για την Αγγλική γλώσσα το D=3.4bits/γράμμα, που σημαίνει ότι κάθε Αγγλικό γράμμα περιέχει 3.4 bits περιττή πληροφορία. Αυτή η βεβαιότητα οφείλεται στην συχνότητα στην οποία διπλά γράμματα, διαγράμματα, τριγράμματα και η-γράμματα καταστρέφονται.

2.5.3 Άριστη Μυστικότητα

Η άριστη μυστικότητα ενός κρυπτοσυστήματος είναι ένα κομμάτι που χρησιμοποιείται για να δείξει ότι το κρυπτοκείμενο δεν φανερώνει καμία πληροφορία όσον αφορά το σχέδιο κειμένου. Ο Claude Shannon υποστηρίζει ότι θεωρητικά αυτό δεν είναι πιθανό, αν το κλειδί είναι τουλάχιστο σαν το μήνυμα και κανένα κλειδί να μη ν έχει ξαναχρησιμοποιηθεί. Πρακτικά το κρυπτοκείμενο τις περισσότερες φορές παράγει μερικούς τύπους από πληροφορία για το σχέδιο κειμένου. Έτσι η πιθανότητα για κρυπτοανάλυση γίνεται ακόμη πιο δύσκολη.

2.5.4 Unicity Distance

Δοσμένου του κλειδιού K για κρυπτοκείμενο C, η unicity distance καθορίζεται από την ποσότητα του κρυπτοκειμένου που χρειάζεται για να καθορίσει το μοναδικό κλειδί. Τα περισσότερα κρυπτοσυστήματα είναι πολύπλοκα στο να υπολογίσουν την unicity distance, αλλά είναι πιθανό να την βρουν κατά προσέγγιση και αυτό μπορεί να βοηθήσει στην αξιολόγηση της ασφάλειας σε ένα συγκεκριμένο σύστημα. Με μαθηματικούς όρους η

unicity distance N καθορίζει την ποσότητα του κειμένου που χρειάζεται για να σπάσει το κρυπτογράφημα, δίνεται από μια formula που πρότεινε ο Claude Shannon: N=H(K) / D, όπου H(K)=$\log_2$ (K), είναι η εντροπία του κλειδιού σε bits και D η αβεβαιότητα της γλώσσας.

Χρησιμοποιώντας τον αλγόριθμο DES, που κρυπτογραφεί 64-bits block και 56 bits κλειδιών η unicity distance θα ναι:

N=56 / 3.2= 17.5 χαρακτήρες.

Διπλασιάζοντας το μέγεθος του κλειδιού σε 112 bits θα διπλασιαστεί και η unicity distance σε 35 χαρακτήρες.

2.5.5 Μπέρδεμα Και Διάδοση

Ο Claude Shannon πρότεινε 2-μεθόδους-για κρυπτογράφηση με σκοπό να ανατρέψει επιθέσεις που βασίζονται σε στατιστική ανάλυση: μπέρδεμα και διάδοση.

Το Μπέρδεμα περιλαμβάνει σύνθετες αντικαταστάσεις που κάνουν τις σχέσεις μεταξύ του κρυπτοκειμένου και του κλειδιού κρυπτογράφησης όσο το δυνατό πιο πολύπλοκο. Με αυτόν τον τρόπο είναι πιθανό ο επιτιθέμενος να μην μπορεί να αποκτήσει το κλειδί ακόμη και αν καταφέρει να αποκτήσει κάποιες πληροφορίες στις στατιστικές του κρυπτοκειμένου.

Η Διάδοση περιλαμβάνει μετασχηματισμούς που διαλύει τις στατιστικές κυριότητες του σχεδίου κειμένου κατά μήκος του κρυπτοκειμένου. Αυτό επιτυγχάνεται με το να επηρεάσουμε το κάθε ψηφίο του κρυπτοκειμένου, από πολλά ψηφία του σχεδίου κειμένου. Με αυτόν τον τρόπο, η διάδοση προσπαθεί να κάνει την σχέση μεταξύ σχεδίου κειμένου και κρυπτοκειμένου όσο το δυνατό πιο πολύπλοκη με σκοπό να εμποδίσει τις προσπάθειες εντοπισμού του κλειδιού.

2.6 Συμβατικοί Αλγόριθμοι

2.6.1 Τύποι Δεδομένων Κρυπτογράφησης

Οι τύποι δεδομένων κρυπτογράφησης DES (Data Encryption Standard) υιοθετήθηκε το 1977 από το NBS και έγινε η βάση για τα πιο ευρέως χρησιμοποιούμενα κρυπτοσυστήματα. Από τότε που έγινε αυτή η

πρόταση έχουν γίνει πολλές εντατικές έρευνες όσο αναφορά την ασφάλεια. Οι όροι υπαγορεύουν ότι θα πρέπει να γίνεται αναθεώρηση κάθε 5 χρόνια. Αυτό δεν ήταν αποτέλεσμα κάποιας υποψίας ότι τα πρότυπα έχουν σπαστεί, αλλά μπορούσε να συμβεί σύντομα χάρη στην αύξηση των ικανοτήτων των μοντέρνων υπολογιστών. Μέχρι στιγμής, το software του DES έχει πιστοποιηθεί και ο αλγόριθμος χρησιμοποιείται ευρέως σε εφαρμογές.

2.6.1.1 Overview

Το DES είναι ένα block κρυπτογραφίας με την έννοια ότι κρυπτογραφεί block δεδομένων. Στο DES το μέγεθος του block είναι 64 bits. Καθώς είναι ένας συμμετρικός αλγόριθμος χρειάζεται 64 bit block σχεδίου κειμένου, το κρυπτογραφεί χρησιμοποιώντας ένα κλειδί σε 64 bit κρυπτοκειμένου και μετά η αποκρυπτογράφηση γίνεται χρησιμοποιώντας το ίδιο κλειδί. Το μήκος του κλειδιού που χρησιμοποιείται είναι 56 bits. Στην πιο απλή εκδοχή, το DES θεωρείται ότι είναι συνδυασμός 2 απλών κρυπτογραφικών τεχνικών προτεινόμενοι από τον Shannon: μπέρδεμα και διάδοση. Ένας και μόνο συνδυασμός αυτών των τεχνικών, η αντικατάσταση ακολουθείται από παραλλαγές, γνωστές σαν ‘round’. Το DES εφαρμόζει τον ίδιο συνδυασμό τεχνικών σε κάθε block σχεδίου κειμένου 16 φορές, κατά συνέπεια έχει 16 rounds. Για την κρυπτογράφηση ενός block DES γίνονται τα παρακάτω:

→ Το block του σχεδίου κειμένου μετά από αρχική παραλλαγή όπου τα 64 bit ξανατακτοποιούνται, χωρίζονται στην μέση, το δεξί μισό και το αριστερό μισό κάθε ένα 32 bit.
→ Τότε οι 16 rounds ξεκινάνε και κάθε ένας από αυτούς παρουσιάζει έναν αριθμό σύντομων λειτουργιών που καλείται function ‘F’ όπου τα δεδομένα συνδυάζονται με το κλειδί. Η λειτουργία ‘F’ δημιουργείται από τα παρακάτω:

1. Τα bit του κλειδιού μετακινούνται και τότε 48 από τα 56 επιλέγονται.

2. Το δεξί μισό του block του σχεδίου κειμένου περνά μέσα από μια ανάπτυξη συνδυασμών και αυξάνεται από 32 σε 48 bits.

3. Το αυξανόμενο σχέδιο κειμένου γίνεται XOR με την χρήση ενός κλειδιού μετακίνησης και στέλνεται μέσα από 8 S-boxes παράγωντας 32 νέα bits.

4. Άλλη μια μετάθεση παίρνει μέρος.

→ Η έξοδος της λειτουργίας F γίνεται XOR με το αριστερό μισό.

→ Το αποτέλεσμα γίνεται το νέο δεξί μισό και το παλιό δεξί γίνεται το νέο αριστερό μισό.
→ Μετά το τέλος του 16 ου round το δεξί και αριστερό μισό ενώνονται και η έξοδος πηγαίνει για νέα μετάθεση. Αυτή η μετάθεση θα ναι η αντιστροφή της αρχικής μετάθεσης.

2.6.1.2 Κλειδί DES

Όπως έχουμε πει το DES χρησιμοποιεί ένα κλειδί με μήκος 56 bits. Με τέτοιοι κλειδί υπάρχουν 2^{56} πιθανά κλειδιά που είναι κατά προσέγγιση $7.2 * 10^{16}$ κλειδιά. Έτσι μια μεγάλη δύναμη επίθεσης με προσπάθεια δοκιμής όλων των πιθανών κλειδιών φαίνεται αδύνατο.
Αν δεχθούμε αυτό ο μισός μέσος όρος του διαστήματος κλειδιού πρέπει να ερευνηθεί, μια μηχανή που παρουσιάζει ένα DES κρυπτογράφησης ανά microsecond, θα χρειαστεί περισσότερο από 1000 χρόνια να σπάσει το κρυπτογράφημα.

Το 56 bit κλειδί DES λαμβάνεται από ένα κλειδί εισόδου 64 bit. Αυτό λαμβάνεται από μια τεχνική κλειδιού μετάθεσης, το οποίο μετακινεί την αναλογία των bits και ξανατακτοποιεί τα εναπομείναντα bit. Αφού παραχθεί και το 56_o κλειδί, κάθε γύρος των 16 DES rounds θα χρησιμοποιεί ένα διαφορετικό 48 bit 'subkey'. Σε κάθε γύρο το κλειδί χωρίζεται σε 2 μισά των 28 bit το κάθε ένα. Μετά το κάθε ένα από αυτά τα μισά μετακινείται αριστερά κατά μια ή δυο θέσεις ανάλογα με τον γύρο. Ο αριθμός των bits μετακινείται ανά γύρο αν η κρυπτογράφηση γίνεται όπως παρακάτω:

Κλειδί μετακίνησης ανά γύρο

Γύρος	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
#of shifts	**1**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**1**

Μετά την μετακίνηση του κλειδιού μόνο 48 από τα 56 bits θα διαλεχτούν. Η λειτουργία αυτή που κάνει αυτή την επιλογή καλείται 'μετάθεση συμπίεσης.

2.6.1.3 Αποκρυπτογράφηση

Μια πολύ ενδιαφέρουσα ιδιότητα του αλγορίθμου DES είναι ότι η διαδικασία της αποκρυπτογράφησης είναι παρόμοια με της κρυπτογράφησης. Η μοναδική διαφορά μεταξύ των 2 έγκειται στην σειρά που πρέπει να ακολουθηθεί στα κλειδιά που χρησιμοποιούνται. Το ένα μπορεί να χρησιμοποιεί τα ίδια κλειδιά όπως το ένα στην φάση της κρυπτογράφησης με την μόνη διαφορά ότι πρέπει να χρησιμοποιείται με αντίστροφη φορά. Έτσι αν σε κάθε round τα κλειδιά για την

κρυπτογράφηση είναι K1,K2,.....,K_{16}, της αποκρυπτογράφησης τα κλειδιά θα ναι K_{16},.....,K_2,K_1. Το κλειδί τώρα μετακινείται στα δεξιά αντί για τα αριστερά και τα νούμερα των θέσεων μετακίνησης καθορίζονται στο διάγραμμα που ακολουθεί:

Κλειδί μετακίνησης ανά γύρο																
Γύρος	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
#of shifts	**0**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**1**

Όπως βλέπουμε το πρώτο κλειδί δε θα πρεπε να μετακινηθεί καθόλου καθώς αυτό θα ναι το κλειδί που θα χρησιμοποιηθεί στην κρυπτογράφηση.

2.6.1.4 Boxes

Στον αλγόριθμο DES η διαδικασία της αντικατάστασης εκτελείται από 8 διαφορετικά boxes ή S-boxes και η διαδικασία της μετάθεσης από box μετάθεσης ή 'P-box'.

Ένα S-box μπορεί να θεωρείται σαν ένα box, το οποίο δέχεται 6 bit σαν είσοδο και μετά από ένα αριθμό bit αντικατάστασης και μετατροπών, μόνο 4 bit παράγονται σαν έξοδος. Ένα πολύ σημαντικό χαρακτηριστικό του S-box, είναι ότι αν ένα συμπλήρωμα είναι μιας εισόδου του S-box, τότε τουλάχιστον 2 bits εξόδου θα αλλάξουν. Στην ουσία οποιαδήποτε αλλαγή στην είσοδο του S-box θα χει σαν αποτέλεσμα τυχαία αλλαγή στην έξοδο.

Ένα P-box μπορούμε να το βλέπουμε σαν ένα απλό box, το οποίο παίρνει σαν είσοδο δεδομένα, εφαρμόζει μετάθεση σε αυτά και επιστρέφει τα μεταθετημένα δεδομένα σαν έξοδο. Αυτή η μετάθεση χαρτογραφεί κάθε bit εισόδου σε μια θέση εξόδου, κανένα bit δεν χρησιμοποιείται 2 φορές και κανένα δεν αναγνωρίζεται.

2.6.1.5 Μέθοδοι

Μια μέθοδος κρυπτογράφησης θεωρείται ότι είναι ο συνδυασμός ενός βασικού κρυπτογραφήματος, μερικές μικρές τροφοδοτήσεις και ένα σύνολο απλών λειτουργιών. Η ασφάλεια του συστήματος αναγνωρίζεται από το κρυπτογράφημα και όχι από την μέθοδο. Θεωρώντας τον αλγόριθμο DES 4 μέθοδοι λειτουργίας έχουν καθοριστεί. Αυτές οι μέθοδοι μπορεί να χρησιμοποιηθούν και σε συμμετρικά block κρυπτογραφήματα. Τα βασικά χαρακτηριστικά αυτών των μεθόδων εξετάζονται παρακάτω**.**

(a). Electronic Codebook Mode

Το Electronic codebook mode είναι ένα μια πρότυπη και απλή μέθοδος. Διαβάζει ένα block σχεδίου κειμένου των 64 bit, το κρυπτογραφεί και δίνει την κρυπτογραφημένη μορφή του. Αφού το κλειδί που χρησιμοποιούμε παραμένει το ίδιο για ένα συγκεκριμένο block του σχεδίου κειμένου, το κρυπτοκείμενο θα παραμείνει το ίδιο. Με αυτόν τον τρόπο, ένα codebook των 2^{64} εισόδων μπορεί να παραχθεί κρατώντας κάθε πιθανό block των 64 bit του σχεδίου κειμένου και να ανταποκρίνεται στο κρυπτογραφημένο block. Στην περίπτωση που το μήνυμα είναι μεγαλύτερο των 64 bit, προσθήκες του τελευταίου block μπορεί να ακολουθήσουν με σκοπό να αποκτήσουν τα bit block που απαιτούνται. Μια τυπική μορφή του ECB χρησιμοποιείται για μετάδοση μιας μοναδικής αξίας,(π.χ κλειδί κρυπτογράφησης). Γενικά το ECB είναι μια μέθοδος χαμηλής ασφάλειας. Αυτό βασίζεται στο γεγονός ότι το ίδιο block του κρυπτοκειμένου συνεχώς παράγει το ίδιο κρυπτοκείμενο. Στην περίπτωση μεγάλου μήκους μηνύματος όπου τα 64 bit block του σχεδίου κειμένου εμφανίζονται περισσότερο από μια φορά, ο επιτιθέμενος μπορεί να κάνει νύξη στα περιεχόμενα του σχεδίου κειμένου. Επιπλέον ο επιτιθέμενος μπορεί να αντικαταστήσει blocks κρυπτοκειμένου με άλλα blocks ή να ξαναρυθμίσει blocks. Ο τύπος αυτός επίθεσης είναι γνωστός και ως ‘block επανάληψης’.

(b). Cipher Block Chaining (CBC)

Λαμβάνοντας υπόψη τα μειονεκτήματα του ECB μαζί με το πόσο τρωτό είναι σε μια επίθεση επανάληψης η Cipher Block Chaining (CBC) μέθοδος ξεπερνά την αδυναμία του ECB. Η μέθοδος αυτή συνεργάζεται με μια τεχνική στην οποία το ίδιο block του σχεδίου κειμένου, αν επαναλαμβάνεται, παράγει διαφορετικά blocks κρυπτοκειμένου. Η είσοδος τώρα στον αλγόριθμο κρυπτογράφησης θα ναι η πύλη XOR του ισχύοντος 64 bit σχεδίου κειμένου με τα προπορευόμενα 64 bit του κρυπτοκειμένου. Το πρώτο block του κρυπτοκειμένου δεν θα γίνει XOR με τίποτα (ή θα γίνει XOR με όλα τα μηδενικά). Το τελικό αποτέλεσμα αυτής της διαδικασίας είναι ότι επαναλαμβάνοντας τα 64 bits δεν εκτίθενται. Για αποκρυπτογράφηση, κάθε block κρυπτογραφήματος περνά μέσα από τον αλγόριθμο. Το αποτέλεσμα αυτό μαζί με το block του κρυπτοκειμένου με την πύλη XOR παράγει το block του σχεδίου κειμένου. Με σκοπό να δυναμώσει το CBC ένας αρχικός φορέας IV μπορεί να χρησιμοποιηθεί. Ο IV με XOR του πρώτου block του σχεδίου κειμένου αποκτάμε το πρώτο block κρυπτογραφήματος. Το IV θα πρέπει να ναι γνωστό και στον αποστολέα και στον δέκτη και για λόγους ασφαλείας θα πρέπει να προστατεύεται σαν το κλειδί. Εκτός από αυτήν τη χρήση για να κατορθωθεί εμπιστευτικότητα θα πρέπει να χρησιμοποιηθεί και για έγκριση.

(c). Cipher Feedback Mode (CFB)

Στο CFM ένα μπλοκ κρυπτογράφημα συνεργάζεται από αυτό συγχρονιζόμενη ροή κρυπτογραφήματος. Ένας καθορισμένος αριθμός από bits “j” bits τα ονομάζουμε, επεξεργάζονται σε κάποια χρονική στιγμή. Σε γενικές γραμμές το εισαγόμενο κείμενο χρησιμοποιείται σαν είσοδο στον αλγόριθμο κρυπτογράφησης για να παραχθεί μια ψευδοτυχαία έξοδος. Τότε με XOR η έξοδος αυτή και το σχέδιο κειμένου παράγουν το επόμενο bit του κρυπτοκειμένου. CFB χρησιμοποιείται για γενικούς σκοπούς για προσανατολισμένη ροή μετάδοσης και μπορεί επίσης να χρησιμοποιηθεί για παροχή εξουσιοδότησης.

(d). Output Feedback Mode (OFB)

Το OFB είναι παρόμοιο με το CFB. Το μόνο χαρακτηριστικό που διαφέρει το OFB από το CFB είναι ότι η είσοδος του αλγόριθμου κρυπτογράφησης είναι τώρα η εισαγόμενη DES έξοδος. Το OFB χρησιμοποιείται για προσανατολισμένη ροή μετάδοσης πάνω σε θορυβώδη κανάλια.

2.6.1.6 DES Βελτιώσεις

Καθώς έχουμε αναφερθεί ήδη στον αλγόριθμο DES ο οποίος παρέχει ένα υψηλό επίπεδο ασφάλειας. Το σθένος του DES ποικίλει ανάλογα με το μήκος του κλειδιού του αλγόριθμου, τον αριθμό των γύρων και από των σχεδιασμό του S-boxes. Παρόλη την δύναμη του DES, η ανάπτυξη των συστημάτων των υπολογιστών μπορεί να επιφέρει επιθέσεις που είναι πιθανό να σπάσουν το σύστημα. Διάφορες μελέτες έχουν γίνει εστιάζοντας στο πως θα δυναμώσουν το DES. Αυτό μπορούμε να το επιτύχουμε αυξάνοντας το μέγεθος του κλειδιού κάνοντας το να συνεργαστεί με τον ίδιο αλγόριθμο χρησιμοποιώντας διάφορα S-boxes, στην τελική αυξάνοντας τον αριθμό των γύρων.

2.6.1.6.1 Τριπλό DES

Ένας τρόπος για να γίνει η πρώτη πρόταση είναι να χρησιμοποιηθεί πολλαπλή κρυπτογράφηση, όπου κρυπτογραφεί μπλοκ σε διάφορες χρονικές στιγμές χρησιμοποιώντας διαφορετικό κλειδί. Η πιο γνωστή φόρμα πολλαπλής κρυπτογράφησης έχει 2 διαδικασίες κρυπτογράφησης και 2 κλειδιά. Έτσι, δίνεται το σχέδιο κειμένου P και 2 κλειδιά k_1 και k_2. Οι εξισώσεις που ακολουθούν δείχνουν πως παράγεται το κρυπτοκείμενο και πως ξανακαλύπτεται αντίστοιχα το σχέδιο κειμένου:

$$C=E_{K2}(E_{K1}(P)) \quad \text{and} \quad P=D_{K1}(D_{K2}(C))$$

Κατά πόσο η μετατροπή αυτή δυναμώσει το σύστημα εξαρτάται από την πιθανότητα κάποιος να βρει 3_o κλειδί K_3 όπως:

$$E_{K2}(E_{K1}(P))=E_{K3}(P)$$

Ένας αλγόριθμος του οποίου κρατιέται αυτή η σχέση ονομάζεται γκρουπ. Πρόσφατες έρευνες είπαν ότι το DES δεν είναι γκρουπ. Έτσι η πολλαπλή κρυπτογράφηση ουσιαστικά βελτιώνει το DES. Η διπλή κρυπτογράφηση μπορεί να αποδειχθεί τρωτή σε μια μέση επίθεση όπου ο επιτιθέμενος κάνει επίθεση και στο κλειδί κρυπτογράφησης με την μια. Γι' αυτό τον λόγο η διπλή κρυπτογράφηση θεωρείται ότι είναι ελαφρώς καλύτερη από το DES.

Η τριπλή κρυπτογράφηση δεν είναι τρωτή σε μια μέση επίθεση. Μια πρόταση για μια τέτοια κρυπτογράφηση είναι το τριπλό DES στο οποίο μια τέτοια ακολουθία κρυπτογράφησης, μια αποκρυπτογράφηση και μια ακόμη κρυπτογράφηση παρουσιάζεται στο επόμενο σχήμα με σκοπό να αποκτήσουμε το κρυπτοκείμενο:

$$C=E_{K1}(D_{K2}(E_{K1}(P)))$$

Η διαδικασία της αποκρυπτογράφησης είναι αντίστροφη:

$$P=D_{K1}(E_{K2}(D_{K1}(C)))$$

2.6.1.6.2 Μεταβλητά S-boxes

Κάποιος μπορεί να ισχυριστεί ότι τροποποιώντας τον αλγόριθμο έτσι που τα S-boxes να εξαρτώνται από το κλειδί θα βοηθούσε στο να αποφευχθούν πιθανές επιθέσεις. Μέχρι στιγμής, η χρήση των υπάρχων S-boxes έχει αποδειχτεί ότι είναι δυνατά απέναντι σε επιθέσεις και έτσι οποιαδήποτε αλλαγή αυτών τα καθιστά ικανά. Ένα πολύ χρήσιμο συμπέρασμα ενός εξαρτώμενου κλειδιού των S-boxes είναι ότι επειδή δεν είναι σταθερά, είναι πιθανό να αναλύσει τα S-boxes προοδευτικά με τον χρόνο ψάχνοντας για αδυναμίες.

2.6.1.6.3 Αύξηση Αριθμών Των Γύρων

Έχει αποδειχθεί ότι αυξάνοντας τον αριθμό των γύρων, οι περισσότεροι αλγόριθμοι γίνονται πιο ανθεκτικοί κάτω από οποιαδήποτε επίθεση. Γενικά ο αριθμός των γύρων διαλέγεται έτσι ώστε οποιαδήποτε μέθοδος κρυπτοανάλυσης να απαιτεί περισσότερη προσπάθεια από μια σκληρή και δυναμική επίθεση. Η σπανιότητα μιας επιτυχημένης επίθεσης στο DES οδηγεί στην δομή, είναι απλό το DES διαφέρει κατά λίγο από τους 16 γύρους. Η πιο πετυχημένη επίθεση σε μια μειωμένη ποικιλία του DES ήταν μια μέθοδο που καλούταν διαφορική κρυπτοανάλυση (θα εξεταστεί πιο κάτω), το οποίο μπορούσε να σπάσει ποικιλίες του DES με 15 γύρους πιο γρήγορα από μια διεξοδική επίθεση.

2.6.2 Πιο Συμβατικοί Αλγόριθμοι

2.6.2.1 Lucifer

Ο αλγόριθμος Lucifer χρησιμοποιήθηκε από την IBM 3614 Consumer Transaction Facility, είναι παρόμοιο με το DES και συμβιβάζεται χρησιμοποιώντας σάντουιτς από P-boxes και S-boxes των 4 bit εισόδου και 4 bit εξόδου. Αυτός ο αλγόριθμος χρησιμοποιεί 128 bit μπλοκ. Τα δεδομένα εισόδου περνούν μέσα από εναλλακτικά στρώματα μέσα από τα boxes. Σε κάθε S-box υπάρχουν 2 πιθανές καταστάσεις S_0 και S_1. Η είσοδος των S-boxes είναι το bit μετάδοσης εξόδου των S-boxes του προηγούμενου γύρου και η είσοδος του πρώτου γύρου είναι το σχέδιο κειμένου. Ο αλγόριθμος Lucifer έχει 16 γύρους αλλά καμία αλλαγή δεν γίνεται μεταξύ των γύρων και δεν υπάρχει άνοιγμα στο μπλοκ του σχεδίου κειμένου.

Χρησιμοποιώντας διαφορετική κρυπτοανάλυση, ο Biham και ο Shamir απέδειξαν ότι ένας αλγόριθμος Lucifer με 32 bit μπλοκ και 8 γύρους μπορεί να σπάσει με 40 διαλεγμένα σχέδια κειμένων και 2^{29} βήματα. Η ίδια επίθεση έσπασε 128 bit Lucifer με 8 γύρους, 60 διαλεγμένα σχέδια κειμένου και 2^{53} βήματα. Αυτές οι επιθέσεις έγιναν χρησιμοποιώντας αλγόριθμο DES και S-boxes. Αν χρησιμοποιούνταν διαφορετικά S-boxes, οι επιθέσεις κατά του Lucifer έχει αποδειχθεί ότι είναι πιο εύκολες. Το κλειδί σύνδεσης κρυπτοανάλυσης μπορεί να σπάσει 128 bit Lucifer, με οποιοδήποτε αριθμό

γύρων, με 2^{33} διαλεγμένα σχέδια κειμένων, ή με 2^{65} γνωστά σχέδια κειμένων.

2.6.2.2 FEAL

Ο αλγόριθμος FEAL σχεδιάστηκε από τον Akihiro Shimuzu και τον Shoji Miyagushi από την Ιαπωνική NTT. Ο αλγόριθμος αυτός ήταν παρόμοιος με τον DES χρησιμοποιώντας 64 bit μπλοκ, ένα 64 bit κλειδί και 4 γύρους που το έκανα πιο γρήγορο.

Χρησιμοποιώντας μια διαλεγμένη επίθεση σχεδίου κειμένου, οι κρυπτοαναλυστές κατάφεραν να σπάσουν επιτυχώς τον αλγόριθμο FEAL-4. Μια καινούργια έκδοση του αλγόριθμου FEAL συστήθηκε χρησιμοποιώντας 8 γύρους, ο FEAL-8. Μια επιτυχημένη επίθεση ενάντια αυτής της έκδοσης παρουσιάστηκε το 1989 από τον Biham και τον Shamir. Μια καινούργια τροποποίηση του αλγόριθμου ήταν ο αλγόριθμος FEAL-N όπου χρησιμοποιούσε περισσότερους από 8 γύρους. Ο Biham και ο Shamir χρησιμοποίησαν διαφορετικές κρυπτοαναλύσεις ενάντια του FEAL-N και ήταν ικανοί να το σπάσουν πιο γρήγορα από μια σκληρή επίθεση για οποιοδήποτε αριθμό γύρων μικρότερο από 32. Τελικά οι Biham και Shamir κατόρθωσαν να δείξουν ότι σπάζοντας τον αλγόριθμο FEAL-NX, μια νέα έκδοση του FEAL-N, με 128 bit κλειδί, ήταν απλό να επιτευχθεί σπάζοντας τον FEAL-N με κλειδί των 64 bit.

2.6.2.3 IDEA

Η πρώτη έκδοση του αλγόριθμου IDEA (International Data Algorithm) λεγόταν PES (Proposed Encryption Standard) και είχε φτιαχτεί από τους Xuejia Lai και James Massey το 1990. Μια διορθωτική έκδοση, σχεδιάστηκε να ναι πιο δυνατή σε δυνατότερες και διαφορετικές επιθέσεις, ήταν ο IPES (Improved Proposed Encryption Standard) και περιγράφτηκε το 1991.Ο IPES άλλαξε όνομα σε IDEA το 1992.

Στο IDEA, το μπέρδεμα κατορθώνεται μιξάροντας 3 διαφορετικές λειτουργίες : bit με bit, με αποκλειστικό OR (XOR), με άθροιση ακέραιων αριθμών με μέτρο 2^{16} (είσοδοι και έξοδοι είναι 16 bit ακέραιοι), πολλαπλασιασμένα από ακέραιους με μέτρο $2^{16} + 1$ (είσοδοι και έξοδοι των 16 bit ακέραιοι ξέχωρα από τα μπλοκ των μηδέν και παριστάνονται σαν 2^{16}). Στο IDEA η διάδοση κατορθώνεται χάρη στον πολλαπλασιασμό / πρόσθεση (MA) δομών των βασικών μπλοκ αλγορίθμων.

Ο IDEA αποδείχθηκε ότι είναι 2 φορές πιο γρήγορος από τον DES. Χάρη στο μήκος του κλειδιού που χρησιμοποιεί, φαίνεται άτρωτο σε πολύ σκληρές επιθέσεις. Οι σχεδιαστές του αλγορίθμου προσπάθησαν να

εξοπλίσουν τον IDEA με όλες τις έννοιες έτσι ώστε να μπορεί να αντισταθεί σε διαφορετικές κρυπτοαναλύσεις. Διαφωνίες αλλά όχι ακριβής αποδείξεις δηλώνουν ότι ο IDEA είναι άτρωτος σε επιθέσεις από διαφορετικές κρυπτοαναλύσεις μετά από 4 από τους 8 γύρους. Θεωρώντας ότι ο αλγόριθμος είναι σχετικά καινούργιος είναι πιθανό ότι μελλοντικές επιθέσεις μπορεί να καταφέρουν να το σπάσουν.

2.6.2.4 Blowfish

Το Blowfish είναι ένα συμμετρικό μπλοκ κρυπτογράφησης αναπτυγμένο από τον Bruce Schneier. Ο αλγόριθμος χρησιμοποιεί 64 bit μπλοκ για κρυπτογράφηση και το μήκος του κλειδιού ποικίλει σε 448 bit. Αυτό παρέχει στο σύστημα ένα υψηλό επίπεδο ασφαλείας. Τα πιο σημαντικά χαρακτηριστικά του αλγόριθμου είναι: η ταχύτητά του, η πυκνότητά του και η απλότητά του. Ο Blowfish κρυπτογραφεί δεδομένα σε 32 bit μικροεπεξεργαστών σε μια ακτίνα των 18 χρονοκύκλων ανά bit. Μπορεί να τρέξει σε λιγότερο από 5 K μνήμης και η δομή του είναι πολύ απλή από την στιγμή που χρησιμοποιεί απλές λειτουργίες. Μέχρι στιγμής η ασφάλεια του Blowfish δεν έχει απειληθεί από οποιαδήποτε επίθεση. Το Kent Marsh Ltd. χρησιμοποιεί τον Blowfish. Το κρυπτογράφημα είναι κομμάτι του Nautilus και του PGPfone.

Άλλοι γνωστοί συμβατικοί αλγόριθμοι είναι οι NewDES, REDOC II, CAST-128, RC5 και RC2.

2.7 Κοινό Κλειδί Κρυπτογράφησης

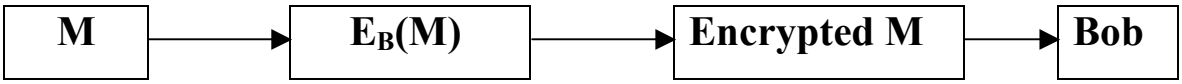
2.7.1 Overview

Το κοινό κλειδί κρυπτογράφησης είναι ένας όρος που χρησιμοποιείται για να καλύψει την περιοχή της ασύμμετρης κρυπτογραφίας. Το κύριο χαρακτηριστικό όπου διαφέρει η ασύμμετρη κρυπτογραφία από την συμμετρική, είναι ότι χρησιμοποιούν διαφορετικό κλειδί για κρυπτογράφηση και αποκρυπτογράφηση. Επιπλέον έχουν το πλεονέκτημα ότι το κλειδί κρυπτογράφησης μπορεί να γίνει κοινό ενώ το κλειδί αποκρυπτογράφησης πρέπει πάντα να είναι κρυφό. Κάποιος μπορεί να αναφερθεί στο κλειδί κρυπτογράφησης σαν κοινό κλειδί και το κλειδί αποκρυπτογράφησης σαν μυστικό κλειδί.

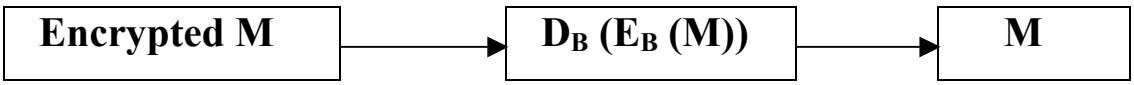
Με σκοπό να κατανοήσουμε πως λειτουργεί το κοινό κλειδί του αλγορίθμου, ας υποθέσουμε ότι 2 χρήστες η Alice και ο Bob συμφωνούν

στο σύστημα δημοσίου κλειδιού και το Ε δείχνει την διαδικασία της κρυπτογράφησης και το D την διαδικασία αποκρυπτογράφησης. Αν η Alice θέλει να στείλει μήνυμα στον Bob, πρώτα θα πρέπει να μάθει το κοινό κλειδί του Bob, έτσι πρέπει πρώτα να της στείλει το κοινό κλειδί του. Μετά κρυπτογραφεί το μήνυμα χρησιμοποιώντας το κλειδί του Bob και στέλνει το μήνυμα. Ο Bob παραλαμβάνει το μήνυμα και το αποκρυπτογραφεί εφαρμόζοντας το μυστικό του κλειδί. Ο Bob θα πρέπει να ακολουθήσει την ίδια διαδικασία αν θέλει να στείλει μήνυμα στην Alice. Υποθέτοντας ότι τα E_A και E_B είναι τα κοινά κλειδιά της Alice και του Bob αντίστοιχα και ότι D_A και D_B τα μυστικά κλειδιά της Alice και του Bob αντίστοιχα, η διαδικασία που ακολουθεί δείχνει πως ο Bob επιτυχώς δέχεται και αποκρυπτογραφεί το μήνυμα M που έστειλε η Alice:

Η Alice στέλνει μήνυμα στον Bob:



Ο Bob δέχεται το μήνυμα



Κανονικό Μήνυμα

Οι διαδικασίες της κρυπτογράφησης και αποκρυπτογράφησης έχουν τις παρακάτω ιδιότητες:

1. Οι χρήστες θα πρέπει να υπολογίζουν με αποδοτικό τρόπο ένα ζευγάρι μυστικού και κοινού κλειδιού.
2. Η γνώση του κοινού κλειδιού δε θα πρέπει να καθιστά ικανό τον υπολογισμό του μυστικού κλειδιού.
3. Η κρυπτογράφηση που ακολουθείται από αποκρυπτογράφηση θα πρέπει να δίνει το γνήσιο μήνυμα.
4. Η αποκρυπτογράφηση που ακολουθείται από κρυπτογράφηση θα πρέπει να δίνει το γνήσιο μήνυμα.

Οι 3 πρώτες προτεραιότητες καθορίζουν την έννοια « παγιδο-πόρτα ενός δρόμου λειτουργίας»(‘trap-door one-way function’), όπου η λειτουργία είναι πιο εύκολο να υπολογιστεί σε μια κατεύθυνση, αλλά πολύ δύσκολο να υπολογιστεί από την άλλη εκτός αν κάποια ειδική πληροφορία είναι γνωστή. Έτσι με σκοπό να προετοιμάσουμε το κοινό κλειδί κρυπτοσυστήματος, μια έξυπνη παγιδο-πόρτα θα βρεθεί μπροστά μας.

Σε ένα δίκτυο από χρήστες, κάθε χρήστης έχει ένα μοναδικό ζευγάρι από κλειδιά. Με στόχο να είναι ικανή η επικοινωνία μεταξύ των χρηστών, μια βάση δεδομένων δημιουργήθηκε κρατώντας τα κοινά κλειδιά όλων των χρηστών και γίνεται χρήσιμη για κάθε χρήστη.

Επίσης το νόημα ενός «δίκαιου» κρυπτοσυστήματος κοινού κλειδιού έχει συσταθεί. Σ' ένα δίκαιο κρυπτοσύστημα κοινού κλειδιού η καλή ισορροπία μεταξύ των αναγκών της κυβέρνησης και των πολιτών είναι απαραίτητο. Τα δίκαια κρυπτοσυστήματα κοινών κλειδιών εγγυώνται ότι το σύστημα δεν μπορεί να κάνει κατάχρηση από παράνομους οργανισμούς και ότι οι πολίτες έχουν τα ίδια δικαιώματα για την ιδιωτική ζωή τους και προστατεύονται από τον νόμο.

2.7.2 Ψηφιακές Υπογραφές

Οι ψηφιακές υπογραφές χρησιμοποιούνται για να χορηγήσουν την γνησιότητα του μηνύματος. Με αυτόν τον τρόπο ο αποστολέας του μηνύματος μπορεί να ελεγχθεί και να πιστοποιηθεί. Ο αποστολέας κρυπτογραφεί το μήνυμα που θέλει να στείλει μαζί με το κοινό κλειδί και στέλνει το κρυπτογραφημένο μήνυμα. Αυτό το μήνυμα δουλεύει σαν ψηφιακή υπογραφή. Αν ο δέκτης καταφέρει να πάρει το μήνυμα σωστά χρησιμοποιώντας το κοινό κλειδί του αποστολέα, τότε είναι σίγουρο ότι το μήνυμα ήρθε από τον συγκεκριμένο αποστολέα και όχι από κάποιον άλλο που ισχυρίζεται ότι είναι ο αποστολέας.

Είναι πολύ σημαντικό να παρατηρήσουμε ότι αυτό το σχήμα παρέχει γνησιότητα αλλά δεν εγγυάται την εμπιστευτικότητα. Και αυτό γιατί κάθε παρατηρητής μπορεί να αποκρυπτογραφήσει το μήνυμα χρησιμοποιώντας το κοινό κλειδί του αποστολέα. Είναι πιθανό να παρέχουμε γνησιότητα και εμπιστευτικότητα υιοθετώντας το παρακάτω σχήμα. Σ' αυτό το σχήμα το M είναι το μήνυμα που πρόκειται να σταλθεί, (KU_a, KR_a) είναι το ζευγάρι κλειδιών του αποστολέα και (KU_b, KR_b) είναι του δέκτη το ζευγάρι κλειδιών.

- Ο αποστολέας κρυπτογραφεί το μήνυμα χρησιμοποιώντας το μυστικό κλειδί του, αυτό παρέχει την ψηφιακή υπογραφή: $E_{Kra}(M)$

- Ο αποστολέας κρυπτογραφεί ξανά το μήνυμα χρησιμοποιώντας το κοινό κλειδί του δέκτη και στέλνει το κρυπτοκείμενο:
C: E_{Kub} (E_{Kra} (M)) = C

- Το κρυπτοκείμενο τότε αποκρυπτογραφείται από τον δέκτη χρησιμοποιώντας το μυστικό κλειδί του: D_{Kua} (D_{KRb} (C)) = M

Το μειονέκτημα αυτής της προσέγγισης είναι ότι το κοινό κλειδί του αλγόριθμου θα πρέπει να εφαρμόζεται 4 φορές παρά 2 σε κάθε επικοινωνία.

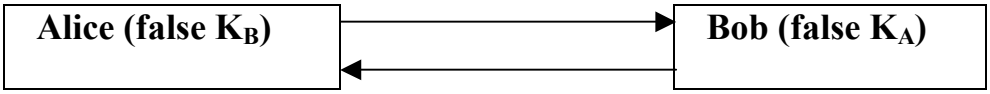
2.7.3 Λειτουργίες του Hash

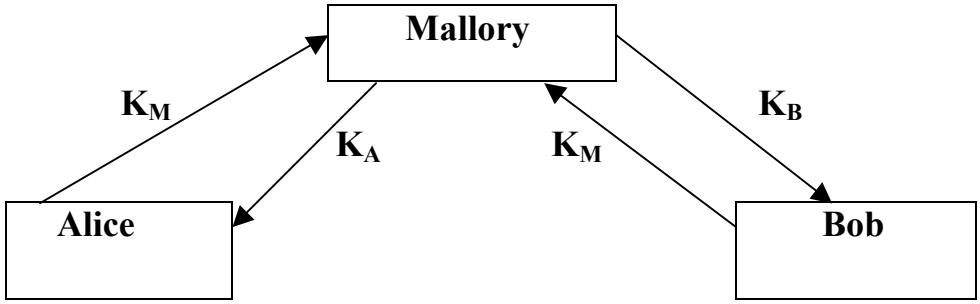
Ένας άλλος τρόπος να παρέχουμε γνησιότητα στο μήνυμα είναι η λειτουργία Hash ενός δρόμου. Μια λειτουργία Hash έχει πολλές ονομασίες: λειτουργία συμπίεσης, λειτουργία συστολής, περίληψη μηνύματος ή δακτυλικό αποτύπωμα. Η λειτουργία Hash είναι μια λειτουργία η οποία κάνει διάφορα μήκη εισόδου string M (μήνυμα) και το μετατρέπει σ' ένα σταθερό string μήκους εξόδου και καλείται αξία Hash H(M). Ένα δοσμένο μήνυμα πάντα μπερδεύεται με την ίδια αξία, αλλά είναι τόσο το καλύτερο να βρει 2 μηνύματα που θα δίνουν την ίδια Hash αξία σαν έξοδο. Μια οποιαδήποτε αλλαγή στο bit του μηνύματος θα δώσει διαφορετικό αποτέλεσμα σαν Hash αξία. Οι λειτουργίες Hash δίνουν ένα αποτύπωμα του μηνύματος και μπορεί να χρησιμοποιηθεί αντί της κρυπτογράφησης με μυστικά κλειδιά με σκοπό να παρέχουν ακεραιότητα στο μήνυμα.

2.7.4 Ψηφιακές Βεβαιώσεις

Οι ψηφιακές διαβεβαιώσεις είναι έννοιες σύνδεσης ευκρίνειας ενός προσώπου σε ένα συγκεκριμένο δημόσιο κλειδί. Η βασική ιδέα ενός εξωτερικού σώματος (Trusted Third Party ή Certification Authority (CA)), παίρνει τις λεπτομέρειες του ενός και το δημόσιο κλειδί του, τα πακετάρει και στην συνέχεια υπογράφει το πακέτο.

Το πρωτόκολλο με το οποίο οι χρήστες ανταλλάσσουν τα δημόσια κλειδιά τους και στην συνέχεια τα χρησιμοποιούν όταν το πρόσωπο που στέλνει το δημόσιο κλειδί του είναι ο πραγματικός ιδιοκτήτης του κλειδιού. Οι κίνδυνοι του να μην 'δέσουν' το κλειδί στον χρήστη ερμηνεύεται από την 'συνάντηση στην μέση της επίθεσης (meet-in-the-middle attack):





Το παραπάνω διάγραμμα μας δείχνει πως παρουσιάζεται η επίθεση. Η Alice σκέφτεται ότι μόλις στέλνει το μήνυμα το κρυπτογραφεί με του Bob το δημόσιο κλειδί K_B. Ο Bob σκέφτεται ότι χρησιμοποιεί το κλειδί της Alice K_A. Στην πραγματικότητα ο Mallory, ο επιτιθέμενος, ανακόπτει το πρώτο μήνυμα που στάλθηκε περιλαμβανομένου και των δημοσίων κλειδιών τους και τα αντικαθιστά με δικό του K_M. Έτσι τώρα παρακολουθεί το κανάλι μεταξύ της Alice και του Bob ανακόπτοντας κάθε μήνυμα, αποκρυπτογραφώντας τα με το δικό του ιδιωτικό κλειδί, τα ξανά-κρυπτογραφεί με το σκόπιμο σαν δέκτη κλειδί και το στέλνει. Η Alice και ο Bob εκτός αν δεν συγκρίνουν τα κλειδιά που χρησιμοποιούν δε θα καταλάβουν για την επίθεση. Η ίδια τακτική επίθεσης μπορεί να χρησιμοποιηθεί για να πλαστογραφήσει υπογραφές στα μηνύματα. Έτσι το δημόσιο κλειδί θα πρέπει να ναι πιο δυνατό στον χρήστη του.

Μια ψηφιακή διαβεβαίωση είναι ένας φάκελος με 4 στοιχεία:

- ∇ Ένα κοινό κλειδί
- ∇ Συνδετικές πληροφορίες του κοινού κλειδιού με τον ιδιοκτήτη του
- ∇ Πληροφορίες για το θέμα της διαβεβαίωσης
- ∇ Η ψηφιακή υπογραφή του θέματος

Μια τυπική πληροφορία διαβεβαίωσης περιλαμβάνει το όνομα του κατόχου, το e-mail του, το όνομα της εταιρείας του, το τηλέφωνό του, ένα μοναδικό στοιχείο της ταυτότητάς του για διαβεβαίωση, μέρα έκδοσης και ημερομηνία λήξης.

Η διαβεβαίωση μπορεί είτε να παραλάβει το κλειδί και να το βεβαιώσει, ή να γενικεύσει το ζευγάρι κλειδιών και να διανείμει και τα 2 και το μυστικό και το κοινό κλειδί και να τα βεβαιώσει μαζί. Για λόγους ασφαλείας είναι καλύτερο γενικά το ότι αν ο χρήστης γενικεύει το ζευγάρι

κλειδιών και το κοινό μεταδίδεται στο CA, με αυτόν τον τρόπο το μυστικό κλειδί θα κρατείται μόνο σε μια τοποθεσία.

Το μυστικό κλειδί κάθε χρήστη είναι αποθηκευμένο σε δίσκο, ή σε μια smart card προστατευμένη με κάποιο κωδικό. Αν η επιλογή του κωδικού είναι καλή τότε θα ναι αδύνατο για κάποιον άλλον να βρει και να χρησιμοποιήσει το μυστικό κλειδί. Σε περίπτωση που κάποιος αποκτήσει πρόσβαση στο μυστικό κλειδί, τότε μια λίστα ονόματι Certificate Revocation List (CRL) θα πρέπει να χρησιμοποιείται. Αυτή η λίστα περιέχει όλες τις διαβεβαιώσεις που δεν πρέπει να εμπιστευόμαστε.

2.7.5 Αλγόριθμοι Δημοσίων Κλειδιών

2.7.5.1 Κρυπτοσύστημα RSA

Ο αλγόριθμος RSA είναι ίσως ο πιο ευρέως χρησιμοποιούμενος από όλα τα συστήματα δημοσίων κλειδιών. Ανακοινώθηκε το 1977 από τους Ronald Rivest, Adi Shamir και Leonard Adleman του MIT.

Το Κρυπτοσύστημα RSA δουλεύει ως εξής:

1. Διαλέγουμε 2 νούμερα p και q
2. Υπολογίζουμε το ποσό n=pq
3. Διαλέγουμε ένα μικρό νούμερο e σχετικά κύριο με το (p-1)(q-1)
4. Υπολογίζουμε το d ως de=1 mod ((p-1)(q-1))

Το ζευγάρι (n,e) είναι το κοινό κλειδί του αλγορίθμου και το ζευγάρι (n,d) το μυστικό κλειδί. Για ένα μήνυμα M και ένα κρυπτοκείμενο C, η κρυπτογράφηση και αποκρυπτογράφηση θα γίνουν όπως δείχνει το διάγραμμα:

$$C=M^e \bmod n \qquad \text{και}$$

$$M= C^d \bmod n= (M^e)^d \bmod n= M^{ed} \bmod n$$

Και ο αποστολέας και ο δέκτης πρέπει να γνωρίζουν την τιμή του n, ο αποστολέας ξέρει την τιμή του e και ο δέκτης την τιμή του d.

Ο αλγόριθμος RSA είναι ένα κομμάτι πολλών παγκοσμίων προτύπων. Ο αλγόριθμος RSA βρέθηκε σε πρότυπα του Internet και πρότεινε πρωτόκολλα περιλαμβάνοντας το S/MIME και S/WAN που θα εξεταστούν σε άλλο κεφάλαιο. Επίσης ο αλγόριθμος RSA έχει χτιστεί σε πρότυπα

λειτουργικά συστήματα από την Microsoft, Apple, Sun και Novell. Σε hardware ο RSA μπορεί να βρεθεί σε ασφαλής τηλεφωνικές γραμμές, σε Ethernet network cards, και σε έξυπνες κάρτες.

Η λειτουργία του RSA θεωρείται ότι είναι ένα προσαρμοσμένο εμπόρευμα. Οι τυπικοί εμπορικοί αλγόριθμοι χρησιμοποιούν σαν εργαλείο το RSA, λειτουργίες του κοινού κλειδιού παίρνουν σαν $O(k^2)$ βήματα, οι λειτουργίες του μυστικού κλειδιού παίρνουν σαν $O(k^3)$ βήματα και το γενικό κλειδί παίρνει $O(k^4)$ λειτουργίες , όπου k είναι το νούμερο των bits του συντελεστή. Η ταχύτητα και η αποδοτικότητα πολλών εφαρμογών του RSA αυξάνεται γρήγορα.

Το DES και άλλα μπλοκ κρυπτογραφήματα σε σύγκριση με το RSA είναι πολύ πιο γρήγορα. Το Des είναι τουλάχιστον 100 φορές πιο γρήγορο στο software και μεταξύ 1000 με 10,000 φορές πιο γρήγορο στο hardware και εξαρτάται από τις εφαρμογές.

2.7.5.2 Αλγόριθμος Diffie-Hellman

Ο πρώτος αλγόριθμος κοινού κλειδιού δημοσιεύτηκε από τους Diffie-Hellman και γενικά αναφέρεται σαν το κλειδί ανταλλαγής των Diffie-Hellman. Ο αλγόριθμος αυτός περιορίζεται μόνο στην ασφαλή ανταλλαγή κλειδιών που θα χρησιμοποιηθούν στην συνέχεια για περαιτέρω κρυπτογραφήσεις.

Υποθέτοντας ότι οι χρήστες Α και Β θέλουν να ανταλλάξουν κλειδί, η διαδικασία που ακολουθείται είναι η εξής:

- ∇ Ένας πρώτος αριθμός q και ένας ακέραιος a ο οποίος είναι αρχική ρίζα του q γίνονται δημόσια. (Μια αρχική ρίζα του q είναι εκείνες οι δυνάμεις που παράγουν όλοι οι ακέραιοι του 1 σε q-1)
- ∇ Ο χρήστης Α επιλέγει ένα τυχαίο ακέραιο $X_A<q$ και υπολογίζει $Y_A= a^{XA} \bmod q$
- ∇ Όμοια ο χρήστης Β υπολογίζει $Y_B= a^{XB} \bmod q$
- ∇ Κάθε πλευρά κρατά την τιμή Χ μυστική και κάνει την τιμή Υ γνωστή στην άλλη πλευρά
- ∇ Ο χρήστης Α υπολογίζει το κλειδί σαν $K= (Y_B)^{XA} \bmod q$ και Β σαν $K= (Y_A)^{XB} \bmod q$

Με αυτόν τον τρόπο οι 2 χρήστες κατόρθωσαν να αλλάξουν ένα μυστικό κλειδί. Η ασφάλεια του αλγορίθμου στηρίζεται στην δυσκολία υπολογισμού των X_A και X_B ειδικότερα όταν μεγάλοι πρώτοι αριθμοί χρησιμοποιούνται.

2.7.5.3 Ελλειπτική Καμπύλη Κρυπτογράφησης

Η ελλειπτική καμπύλη κρυπτογράφησης, Elliptic Curve Cryptography (ECC), είναι μια σχετικά καινούργια περιοχή στην κρυπτογραφία δημοσίου κλειδιού. Συγκριτικά με το σύστημα RSA, η ECC φαίνεται να δίνει την ευκαιρία δημιουργίας μιας πάγιας διαδικασίας όμοια με την ασφάλεια για μικρότερο μέγεθος bit μπορεί να επιτευχθεί.

Έχοντας υπόψιν τη φάση κρυπτογράφησης, το σύστημα προσπαθεί να κωδικοποιήσει το μήνυμα m να σταλεί σαν x-y σε σημείο P_m. Αυτό το σημείο θα το κρυπτογραφήσει και τελικά θα το αποκρυπτογραφήσει. Η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης απαιτεί και την ύπαρξη ενός σημείου G και ένα ελλειπτικό γκρουπ $E_p(a, b)$ σαν παραμέτρους. Ο χρήστης A επιλέγει ένα ιδιωτικό κλειδί n_a και γενικεύει το δημόσιο κλειδί $P_A=n_a * G$. Για να κρυπτογραφήσουμε και να στείλουμε ένα μήνυμα από το P_m στο B, ο A διαλέγει ένα τυχαίο θετικό ακέραιο K και παράγει το κρυπτοκείμενο C_m όπου περιέχει ζευγάρι από σημεία $C_m= \{k G, P_m + k P_B\}$. Για να αποκρυπτογραφήσουμε το κρυπτοκείμενο, το B πολλαπλασιάζει το πρώτο σημείο με το ζευγάρι των μυστικών κλειδιών του χρήστη B και αφαιρεί το αποτέλεσμα από το δεύτερο σημείο.

Η ασφάλεια του αλγόριθμου ECC εξαρτάται από το πόσο δύσκολο είναι να καθορίσεις το κλειδί k δοσμένου των k P και P. Αυτό αναφέρεται σαν πρόβλημα της ελλειπτικής καμπύλης λογαρίθμου.

2.8 Κρυπτοανάλυση

Η Κρυπτοανάλυση είναι μια επιστήμη ανάκτησης του σχεδίου κειμένου ενός μηνύματος ή ενός κλειδιού που έχει χρησιμοποιηθεί για να κρυπτογραφήσει το μήνυμα. Με την βοήθεια της κρυπτοανάλυσης, οι αλγόριθμοι κρυπτογράφησης και τα πρωτόκολλα κρυπτογραφημάτων μπορεί να γίνουν τρωτά και τελικά να σπάσουν. Η προσπάθεια που μπορεί να γίνει για να σπάσει ένα κρυπτογραφικό σύστημα λέγεται επίθεση. Πολλοί σχεδιαστές των αλγορίθμων με στόχο να πετύχουν καλύτερη ασφάλεια για τους αλγόριθμους τους, έχουν προσπαθήσει να χρησιμοποιήσουν την κρυπτοανάλυση για να βρουν και να διορθώσουν πιθανές αδυναμίες. Υπάρχουν μερικοί γενικοί τύποι επιθέσεων και παίρνοντας υπόψη ότι η κρυπτοανάλυση έχει πλήρη γνώση για τους αλγόριθμους κρυπτογράφησης, σκοπός τους είναι να αποσπάσουν το κλειδί:

♦ Μια επίθεση μόνο στο κρυπτοκείμενο (ciphertext-only-attack), είναι μια επίθεση όπου ο κρυπτοαναλυτής έχει κρυπτοκείμενο πολλών μηνυμάτων και χρησιμοποιεί τον ίδιο αλγόριθμο, προσπαθεί να αποσπάσει το σχέδιο κειμένου από όσα περισσότερα μηνύματα μπορεί. Μια τέτοια επίθεση είναι δύσκολο να γίνει γιατί απαιτεί πολλά δείγματα κρυπτοκειμένου.

♦ Επίθεση σε γνωστό σχέδιο κειμένου (known-plaintext attack), είναι η επίθεση όπου ο κρυπτοαναλυτής έχει πρόσβαση και στα δείγματα του κρυπτοκειμένου και στο αντίστοιχο σχέδιο κειμένου.

♦ Μια επίθεση σε διαλεγμένο σχέδιο κειμένου (chosen-plaintext attack), είναι μια επίθεση όπου ο κρυπτοαναλυτής είναι ικανός να διαλέξει το σχέδιο κειμένου και στην συνέχεια να αποκτήσει το κρυπτογραφημένο κείμενο. Αυτός ο τρόπος επίθεσης είναι πιο δυνατός από την επίθεση σε γνωστό σχέδιο κειμένου με την έννοια ότι ο επιτιθέμενος μπορεί να διαλέξει όποια μπλοκ σχεδίου κειμένου θέλει.

♦ Μια επίθεση σε προσαρμοσμένο διαλεγμένο σχέδιο κειμένου (adaptive-chosen-plaintext attack), είναι μια ειδική περίπτωση επίθεσης σε διαλεγμένο σχέδιο κειμένου. Ο επιτιθέμενος μπορεί να διαλέξει όποιο μπλοκ σχεδίου κειμένου επιθυμεί και η επιλογή του μπορεί να βασίζεται σε προηγούμενες κρυπτογραφήσεις.

♦ Μια επίθεση σε διαλεγμένο κρυπτοκείμενο (chosen-ciphertext attack), είναι η επίθεση όπου ο κρυπτοαναλυτής μπορεί να διαλέξει μπλοκ κρυπτοκειμένου και να βρει την φόρμα του σχεδίου κειμένου. Αυτός ο τύπος επίθεσης είναι πιο πολύ εφαρμόσιμος σε κρυπτοσυστήματα κοινού κλειδιού.

♦ Μια επίθεση σε προσαρμοσμένο διαλεγμένο κρυπτοκείμενο (adaptive-chosen-ciphertext attack), είναι μια ειδική περίπτωση της διαλεγμένης επίθεσης κρυπτοκειμένου. Ο επιτιθέμενος κατέχει ένα κομμάτι hardware αποκρυπτογράφησης , αλλά δεν μπορεί να βρει το κλειδί αποκρυπτογράφησης χρησιμοποιώντας αυτό το hardware.

Επιπλέον υπάρχουν και άλλοι τρόποι επίθεσης βασισμένοι στα προηγούμενα είδη και εξαρτώνται από την τάξη του αλγόριθμου κρυπτογράφησης που χρησιμοποιείται για την κρυπτογράφηση του σχεδίου κειμένου. Κάθε κρυπτοαναλυτής διαφορετικές έννοιες επίθεσης, ένα συμβατικό αλγόριθμο που τον συγκρίνει για να σπάσει τον αλγόριθμο του δημόσιου κλειδιού. Και αυτό γιατί και τα 2 συστήματα φαίνεται να έχουν

διαφορετικές δομές και έτσι διαφορετικές αδυναμίες θα ναι η βάση για επίθεση.

2.8.1 Κρυπτοανάλυση Συμβατικών Αλγορίθμων

Υπάρχουν 4 τύποι επίθεσης όπου ένας μπορεί να ανέβει ενάντια σε ένα συμμετρικό μπλοκ κρυπτογραφήματος. Αυτές οι επιθέσεις είναι: η διαφορική κρυπτοανάλυση, κρυπτοανάλυση συνδετικών κλειδιών, γραμμική κρυπτοανάλυση και η αλγεβρική κρυπτοανάλυση.

Η διαφορική κρυπτοανάλυση (differential cryptanalysis) συντάχθηκε από τον Murphy κατά του FEAL-4 και στην συνέχεια υιοθετήθηκε και τελειοποιήθηκε από τους Biham και Shamir που χρησιμοποίησαν αυτή την επίθεση κατά του DES. Γενικά είναι επίθεση διαλεγμένου σχεδίου κειμένου και αναλύει την διαφορά που εμφανίζεται όταν κρυπτογραφούνται 2 συγγενικά σχέδια κειμένων χρησιμοποιώντας το ίδιο κλειδί. Ξέχωρα από την επίθεση κατά του DES, η διαφορική κρυπτοανάλυση ήταν και κατά των λειτουργιών Hash.

Η κρυπτοανάλυση συνδετικών κλειδιών (related-key cryptanalysis) είναι μια επίθεση όπου ο κρυπτοαναλυτής εξετάζει τις διαφορές μεταξύ των κλειδιών. Ο επιτιθέμενος στην πραγματικότητα διαλέγει μια σχέση μεταξύ των κλειδιών χωρίς να ξέρει τα ίδια τα κλειδιά. Τα δεδομένα τότε κρυπτογραφούνται χρησιμοποιώντας και τα 2 κλειδιά. Αυτό το είδος επίθεσης ήταν η πρώτη επίθεση κατά του αλγοριθμικού κλειδιού DES.

Η γραμμική κρυπτοανάλυση (linear cryptanalysis) συντάχθηκε από τους Matsui και Yamagishi κατά του FEAL. Αργότερα χρησιμοποιήθηκε για επίθεση κατά του DES. Είναι μια επίθεση σε γνωστό σχέδιο κειμένου και χρησιμοποιεί γραμμικές προσεγγίσεις για να περιγράψει την δράση του μπλοκ κρυπτογραφήματος. Εξετάζοντας κατάλληλα ζεύγη σχεδίων κειμένων και αντιστοιχώντας κρυπτοκείμενο, σημαντική πληροφορία για το κλειδί μπορεί να φανερωθεί. Αυτό θα αυξήσει την πιθανότητα για επιτυχημένη επίθεση.

Τέλος έχουμε την αλγεβρική επίθεση (algebraic attack) χρησιμοποιούνται κατά των μπλοκ κρυπτογραφημάτων όπου η δομή τους βασίζεται σε μαθηματικές έννοιες. Τέτοιες επιθέσεις έχει αποδειχθεί ότι είναι επιτυχής όταν το κρυπτογράφημα είναι ένα γκρουπ ή όχι. Σε περίπτωση που το κρυπτογράφημα είναι όντως γκρουπ τότε θεωρητικά είναι αδύναμο.

2.8.2 Κρυπτοανάλυση RSA

Ο πιο γνωστός τρόπος για να σπάσει το κρυπτοσύστημα RSA είναι να βρεθεί το ιδιωτικό κλειδί ενός συγκεκριμένου δημοσίου κλειδιού. Με αυτόν τον τρόπο ο επιτιθέμενος θα μπορεί να διαβάζει όλα τα κρυπτογραφημένα μηνύματα και να παραποιεί τις υπογραφές. Για να το πετύχει αυτό η επίθεση πρέπει να κάνει τον συντελεστή δημόσιο n, σε 2 από τους συντελεστές του p και q. Αν καταφέρει να το πετύχει αυτό θα μπορεί τότε να υπολογίσει το ιδιωτικό κλειδί d χρησιμοποιώντας απλώς τα p, q και τον δημόσιο εκθέτη e. Η δυσκολία επίθεσης στο κρυπτοσύστημα RSA σε αυτό το σχήμα βασίζεται στην δυσκολία του συντελεστή n. Για πολύ μεγάλους πρώτους αριθμούς αυτό φαίνεται αδύνατο.

Ένας άλλος τρόπος να σπάσει το RSA είναι να βρεθεί τεχνική να υπολογιστεί το e^{th} ρίζες του n. Αφού $C= M^e \bmod n$, το e^{th} ρίζα του C mod n είναι το μήνυμα M. Αυτή η επίθεση θα επιτρέπει σε κάποιον να ανακαλύπτει κρυπτογραφημένα μηνύματα χωρίς να γνωρίζει το μυστικό κλειδί. Μέχρι στιγμής δεν υπάρχουν μέθοδοι να σπάσει το RSA με αυτό το τρόπο.

Μια πολύ καινούργια περιοχή επιθέσεων ανακαλύφθηκε από τον Paul Kocher. Η βάση αυτών των επιθέσεων είναι ότι διαφορετικές λειτουργίες κρυπτογράφησης όπως οι εκθετικές λειτουργίες του RSA, παίρνουν ασυνεχή διαφορετικά ποσά για επεξεργασία σε διαφορετικούς χρόνους. Ο επιτιθέμενος εξετάζει χρονικές διαφορές στις λειτουργίες του RSA και αυτό ίσως τον οδηγήσει να ανακαλύψει το μυστικό κλειδί. Αυτός ο τύπος επίθεσης είναι γνωστός και σαν χρονική επίθεση (timing attack).

Επίσης υπάρχουν και άλλου είδους επιθέσεις στο RSA. Μια από αυτές είναι η επίθεση κοινού συντελεστή (common modulus attack) όπου διάφοροι χρήστες μοιράζονται το ίδιο n αλλά έχουν διαφορετικές τιμές για το e και d. Αυτό μπορεί να αναγκάσει τον επιτιθέμενο να εξάγει το μήνυμα χωρίς να κάνει συντελεστή τον n. Τέλος αν το d είναι ίσο με το ¼ του μήκους του n και το e είναι μικρότερο του n, το d μπορεί να το βρει. Με σκοπό να αποφύγουμε αυτές τις 2 επιθέσεις τα περισσότερα κρυπτογραφικά πρωτόκολλα κοινών κλειδιών δεν μοιράζονται συντελεστές κοινού κλειδιού μεταξύ των χρηστών και δεν διαλέγουν μικρές τιμές για την αποκρυπτογράφηση.

2.9 Επίλογος

Η ανάπτυξη των συστημάτων υπολογιστών έχουν κάνει τα δεδομένα τρωτά σε μη εξουσιοδοτημένες προσβάσεις. Η κρυπτογραφία θεωρείται η βάση για περαιτέρω διαδικασίες και αλγόριθμους που αναπτύσσονται για να εμποδίσουν τις επιθέσεις ασφαλείας. Σ' ένα σύστημα κρυπτογραφίας τα δεδομένα κρυπτογραφούνται στο σημείο μετάδοσης και ανάλογα αποκρυπτογραφούνται στην παραλαβή. Η ποιότητα της ασφάλειας εξαρτάται από την δύναμη του συστήματος και από τον κρυπτογραφικό αλγόριθμο που χρησιμοποιείται. Μέχρι τώρα υπάρχου 2 βασικές κατηγορίες κρυπτογραφικών αλγόριθμων: συμβατικοί αλγόριθμοι και οι αλγόριθμοι δημοσίων κλειδιών. Το πρότυπο σχήμα κρυπτογράφησης σε παλιότερο τύπο είναι ο αλγόριθμος DES. Ο περαιτέρω τύπος αλγορίθμων έχει γίνει το ίδρυμα κατασκευής ειδών ασφαλείας που είναι πολύ χρήσιμα σήμερα στην αγορά ηλεκτρονικής ασφάλειας. Το κρυπτοσύστημα RSA είναι ένα παράδειγμα ενός δυνατού αλγόριθμου κοινού κλειδιού.

Και το κοινό κλειδί και οι συμβατικοί αλγόριθμοι απειλούνται από επιθέσεις κρυπτοανάλυσης. Γενικά η κρυπτοανάλυση είναι η επιστήμη που ανακαλύπτει κρυπτογραφημένα μηνύματα ή το κλειδί που χρησιμοποιείται για την διαδικασία κρυπτογράφησης δεδομένων που ακολουθείται. Για κάθε κατηγορία αλγορίθμων κρυπτογράφησης υπάρχουν συγκεκριμένες επιθέσεις όπου παίρνουν το πλεονέκτημα μιας συγκεκριμένης αδυναμίας που φαίνεται να έχει το κρυπτοσύστημα. Σε κάθε περίπτωση ο σχεδιαστής του αλγόριθμου κρυπτογράφησης θα πρέπει πρώτα να παίρνει υπόψιν του όλα τα βασικά χαρακτηριστικά κάθε επίθεσης κρυπτοανάλυσης και μετά να κατασκευάζει το σύστημα. Το σύστημα κρυπτογράφησης πρέπει να ναι απρόσβλητο σε κάθε δυνατή επίθεση που μπορεί να απειλήσει την ακεραιότητα και την αυθεντικότητα της μεταδιδόμενης πληροφορίας.

ΚΕΦ 3: Πρακτική Ασφάλεια Δικτύου

3.1 Εισαγωγή

Οι πιο κοινές έννοιες για να διαφυλάσσεται η ηλεκτρονική ασφάλεια είναι η υποδομή του δημοσίου κλειδιού. Βασισμένο στην κρυπτογραφία του δημοσίου κλειδιού, το PKI θεωρείται ότι είναι η πρότυπη δομή για να αναπτυχθούν τα πιο ασφαλή προϊόντα που είναι γενικά χρήσιμα. Τα τμήματα των διαγραμμάτων πιο κάτω συνιστούν μια προσπάθεια να δώσουν μια ολοκληρωμένη άποψη των βασικών χαρακτηριστικών του PKI και πως αυτά συνεργάζονται μεταξύ τους και κάνουν ένα κανάλι επικοινωνίας ασφαλές μεταξύ των χρηστών στο δίκτυο. Επιπλέον αυτό το κεφάλαιο εστιάζει στις βασικές λύσεις ασφαλείας του PKI τόσο καλά όσο και τα χρήσιμα προϊόντα στην ηλεκτρονική αγορά ασφαλείας. Σε επόμενο κομμάτι του κεφαλαίου θα γίνει αναφορά στις πιο γνωστές συνεισφορές εταιρειών στην ηλεκτρονική ασφάλεια.

3.2 Δομή Κοινού Κλειδιού

Είμαστε στην μέση της ηλεκτρονικής επανάστασης των business. Η νέα παγκόσμια κουλτούρα της συναλλαγής ηλεκτρονικών πληροφοριών και του δικτύου προϋποθέτει μεγάλη απειλή από οποιαδήποτε άλλη απάτη, κρυφοκοίταγμα του e-mail και κλεψίματος δεδομένων και για τις εταιρείες και για μεμονωμένες περιπτώσεις. Η ασφάλεια της πληροφορίας είναι ένα μεγάλο θέμα για την σημερινή κοινωνία. Η κρυπτογραφία κοινού κλειδιού δεν είναι αρκετή αν θέλουμε να ξαναδημιουργήσουμε συνθήκες με την παραδοσιακή επικοινωνία με χαρτί στον ηλεκτρονικό κόσμο. Με σκοπό να το πετύχουμε αυτό η δομή κοινού κλειδιού (Public Key Infrastructure) PKI έρχεται να εδραιώσει το κλειδί με το οποίο ξεκλειδώνονται τα οφέλη ενός αληθινού ασφαλή ηλεκτρονικού κόσμου.

Στο Internet το X.509 PKI ή αλλιώς PKIX Roadmap, το PKIX Working Group καθορίζει ένα PKI σαν ‘Το στήσιμο ενός hardware, software άνθρωποι και διαδικασίες χρειάζονται να δημιουργήσουν, να καταφέρουν, να αποθηκεύσουν, να διαμοιράσουν και να ανακαλέσουν βεβαιώσεις βασισμένα στην κρυπτογραφία του κοινού κλειδιού.’

Το PKI παρέχει 4 βασικές λειτουργίες ασφάλειας εμπορικών συναλλαγών. Εμπιστευτικότητα: κρατά την πληροφορία μυστική, Ακεραιότητα: αποδεικνύει ότι η πληροφορία δεν έχει αλλοιωθεί, Αυθεντικότητα: αποδεικνύει την ταυτότητα των χαρακτηριστικών και η Μη

απόρριψη: διασφαλίζει ότι η πληροφορία δεν αποκηρύσσεται. Τα βασικά εργαλεία του PKI είναι τα παρακάτω:

⇒ Ασφαλής Πολιτική

⇒ Βεβαίωση γνησιότητας (Certificate Authority, CA)

⇒ Γνησιότητα Εγγραφής (Registration Authority, RA)

⇒ Διαβεβαίωση διανομής του συστήματος

⇒ Εφαρμογές εξουσιοδότησης του PKI

Η ασφαλής πολιτική χρησιμοποιείται για τον καθορισμό ενός ανωτέρου επιπέδου διεύθυνσης του οργανισμού για ασφάλεια πληροφορίας τόσο στις αρχές και στην πορεία για την χρήση της κρυπτογραφίας. Τυπικά θα περιλαμβάνει δηλώσεις στο πως οι οργανισμοί θα διαχειρίζονται κλειδιά και πολύτιμες πληροφορίες και θα θέτει το επίπεδο ελέγχου που απαιτείται για να ταιριάξουν τα επίπεδα ρίσκου.

Το σύστημα βεβαίωσης γνησιότητας είναι η βάση εμπιστοσύνης του PKI καθώς χειρίζεται διαβεβαιώσεις του κοινού κλειδιού για ολόκληρο τον κύκλο ζωής. Ο CA είναι υπεύθυνος για την έκδοση διαβεβαιώσεων με το να συνδέει την ταυτότητα του χρήστη ή το κοινό κλειδί του συστήματος με την ψηφιακή υπογραφή. Επίσης ο CA σχεδιάζει ημερομηνίες λήξης των διαβεβαιώσεων και τις διασφαλίζει τις βεβαιώσεις ανακαλώντας τες όταν αυτό είναι απαραίτητο εκδίδοντας το CRL(λίστες ανάκλησης).

Η γνησιότητα εγγραφής παρέχει το σημείο επαφής ανάμεσα στον χρήστη και το CA. Συλλαμβάνει και επικυρώνει την ιδιότητα των χρηστών και ενδίδει στην αίτηση για διαβεβαίωση στο CA. Οι δια βεβαιώσεις μπορούν να διανεμηθούν σε έναν αριθμό τρόπων που εξαρτάται από την δομή του περιβάλλοντος του PKI. Η διανομή μπορεί να εξεταστεί από τους χρήστες μόνο, ή από μια υπηρεσία καθοδήγησης. Ένας server καθοδήγησης μπορεί ήδη να υπάρχει μέσα σε ένα οργανισμό ή μπορεί να είναι μέρος λύσης του PKI.

Οι εφαρμογές εξουσιοδότησης του PKI που μπορούν να αναπτυχθούν είναι: επικοινωνίες μεταξύ web servers και browsers, e-mail, ανταλλαγή ηλεκτρονικών δεδομένων (Electronic Data Interchange,EDI), για συναλλαγές πιστωτικών καρτών μέσο Internet και για Virtual Private Network (VPN). Είναι απαραίτητο όταν αναλαμβάνοντας μια έρευνα για την εφαρμογή του PKI όπου το σύστημα του PKI είναι ευαίσθητο με την έννοια ότι τα συστατικά του είναι εύκολα να αλλοιωθούν. Το PKI πρέπει να

ναι εύκολο στην χρήση ακόμη και από μη ειδικευμένο προσωπικό στους οργανισμούς. Καθώς η εμπιστοσύνη των οργανισμών για το PKI αυξάνει, είναι απαραίτητο το σύστημα να κάνει μια κλίμακα και να ταιριάξει αυτή την αύξηση. Η ασφάλεια του CA και του RA είναι πρωταρχικής σημασίας, αφού συμβιβάζονται μεταξύ τους, ολόκληρο το PKI σύστημα απειλείται.

Στις μέρες μας ένας μεγάλος αριθμός από οργανισμούς χρησιμοποιεί σαν εργαλείο συστήματα PKI. Ακολουθούν μερικά παραδείγματα του PKI:

- **Φορολογικό Γραφείο Αυστραλίας :** Αυτό σχεδιάζει να κάνει e-tax δηλαδή ένα βασισμένο στο Internet φόρο εισοδήματος ετοιμασίες επιστροφής και εγκαθίδρυσης software, απαραίτητο για το κοινό για εγκαθίδρυση των φόρων επιστροφής του 1999.

- **Τράπεζα Ιρλανδίας:** Χρησιμοποιεί ένα PKI σύστημα για 'Business on line' να παρέχει μια ασφαλή φόρμα στους πελάτες της τραπέζης για να διαχειρίζονται τις τραπεζικές τους απαιτήσεις μέσο του Internet.

- **Communedata (KMD):** Το KMD είναι το μεγαλύτερο λειτουργικό σύστημα της Δανίας σαν σπίτι του software. Το KMD διαχειρίζεται ψηφιακές αιτήσεις και για business και για τους πολίτες της Δανίας και καταφέρνει με την υποδομή να επιτρέπει ηλεκτρονική επικοινωνία σε ένα ασφαλή και εμπιστευτικό περιβάλλον.

- **PPT Ταχυδρομείο:** Η Ολλανδέζικη ταχυδρομική αρχή, PPT ταχυδρομείο, χρησιμοποιεί το PKI για να προσφέρει στο e-mail και στις βεβαιώσεις του web σε εταιρείες και πολίτες έτσι που να μπορούν να δεσμευτούν με την ηλεκτρονική δραστηριότητα της επικοινωνίας.

- **Teleno:** Είναι ο αρχηγός στην αγορά της Νορβηγίας στην περιοχή των τηλεπικοινωνιών και είναι επίσης ένα από τα μεγαλύτερα Internet Service Providers στον κόσμο. Η Telenor χρησιμοποιεί ένα συνδυασμό συστημάτων PKI και κιτ εργαλείων για να παρέχουν μια πλήρη λύση του PKI στον πληθυσμό της Νορβηγίας.
- **Γενική Ένωση Ταχυδρομείων (Universal Postal Union, UPU):** Βασισμένο στην Ελβετία, η UPU χρησιμοποιεί ένα PKI για να ασφαλίσει τα μηνύματα αναφορικά με πια σειρά θα μεταφέρονται χρήματα μεταξύ διεθνών ταχυδρομικών εξουσιών.

Συνοψίζοντας μια μεγάλη ανάπτυξη του PKI γίνεται σταδιακά κατά μήκος της ανάγκης για ασφάλεια γύρω από τον ηλεκτρονικό κόσμο που μας περιβάλλει. Για να πετύχει στις ηλεκτρονικές business, οι οργανισμοί πρέπει να χρησιμοποιούν PKI το οποίο θα τους προστατεύει με ασφάλεια και μυστικότητα.

3.3 Λύσεις Ασφαλείας Και Δίκτυο

Το PKI σύστημα είναι υιοθετημένο να παρέχει το κέντρο του σκελετού για μια μεγάλη ποικιλία από εργαλεία, αιτήσεις, τακτικές και προϊόντα που σκοπός τους είναι να τα συνδυάσουν και να επιτύχουν τις 4 βασικές αρχές λειτουργιών για ασφάλεια: εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα και μη απόρριψης. Σε αυτό το κομμάτι ένας αριθμός από προϊόντα επισκεπτόμαστε και μελετάμε.

3.3.1 Έξυπνες Κάρτες (Smartcards)

Μια έξυπνη κάρτα είναι μια συγκεκριμένη σε διαστάσεις πλαστική κάρτα η οποία περιέχει μικρο-ηλεκτρονικό πακέτο συμπεριλαμβανομένου μιας μνήμης και ενός επεξεργαστή που κοντρολάρει, διαβάζει και έχει πρόσβαση για να γράφει στην μνήμη. Αυτή η κάρτα διαφέρει από την μαγνητική με λωρίδες κάρτα (magnetic stripe card). Όχι τόσο στην χωρετικότητα της μνήμης όσο στην εσωτερική υπολογιστική δύναμη, εξ ου και το όνομα έξυπνη κάρτα.

Οι έξυπνες κάρτες είναι σε χρήση τα τελευταία 20 χρόνια. Έχει απλωθεί σε όλες τις ηπείρους και έχουν μια ποικιλία σε αιτήσεις: ηλεκτρονικό ρευστό χρήμα, κινητά τηλέφωνα, ταυτότητες συνδρομητών ή ακόμη για προσωπικές πληροφορίες υγείας.

Η ευρεία χρήση των έξυπνων καρτών αυξάνεται ραγδαία καθώς το κόστος των chip πέφτει και η χωρετικότητα μνήμης και η δύναμη επεξεργασίας αυξάνουν. Ένας από τους συντελεστές κλειδιού οδηγεί τώρα την αύξηση προς τα εμπρός στην τρίτη γενιά λειτουργικών συστημάτων έξυπνων καρτών: διευκόλυνση πολλαπλών αιτήσεων για να συνυπάρχουν με μια κάρτα. Η μεγάλη πλειοψηφία των έξυπνων καρτών σε αυτό το σημείο έχουν χρήση μιας κάρτας. Το επόμενο βήμα είναι να τα κάνουν πιο λειτουργικά υιοθετώντας συστήματα λειτουργικών πολλαπλών αιτήσεων. Αυτή την στιγμή ένας αριθμός από διαφορετικά λειτουργικά συστήματα ανταγωνίζονται για αποδοχή. Το ιδανικό λειτουργικό σύστημα πρέπει να είναι ασφαλές, εύκαμπτο και να μπορεί να μεταφέρει σε διαφορετικές πλατφόρμες πωλητών.

3.3.2 Barrier Boxes

Σήμερα αυτές οι συσκευές χρησιμοποιούνται για να προστατέψουν απευθείας συνδέσεις στο λιμάνι διοίκησης σε μια ποικιλία επικοινωνιών και συσκευών ασφαλείας. Οι πιο πρόσφατες εκδόσεις είναι οι βάσεις για

μοντέρνα αυθεντικά συστήματα. Σήμερα οι συσκευές αυτές έχουν προοδεύσει τα οποία έχουν εσωτερικά V36 modems. Τέτοιες συσκευές μπορεί να παρέχουν κρυπτογράφηση σε μια απευθείας σύνδεση αν απαιτείται ή ακόμη κύκλο ισχύς στην συσκευή που προστατεύουν.

3.3.3 S/MIME

Το S/MIME σημαίνει Secure/Multipurpose Internet Mail Extensions και σχεδιάστηκε για να προσθέσει ασφάλεια στο e-mail με σχήμα MIME. Το MIME είναι μια επέκταση του RFC 822 (mail transfer protocol) που σκοπό έχει να ονομάσει κάποια από τα προβλήματα του πρωτοκόλλου SMTP (Simple Mail Transfer Protocol). Το S/MIME παρέχει τις παρακάτω λειτουργίες:

⇒ **Enveloped Data:** Κρυπτογραφημένα περιεχόμενα οποιουδήποτε τύπου και κρυπτογραφημένο περιεχόμενο κλειδιών κρυπτογράφησης για έναν ή περισσότερους δέκτες.

⇒ **Signed Data:** Μια ψηφιακή υπογραφή παρουσιάζεται παίρνοντας την περίληψη του μηνύματος του περιεχομένου που υπογράφεται και μετά κρυπτογραφείται με του υπογεγραμμένου το μυστικό κλειδί. Το περιεχόμενο με την επιπλέον υπογραφή κωδικοποιείται χρησιμοποιώντας base64.

⇒ **Clear-Signed Data:** Μια ψηφιακή υπογραφή του περιεχομένου παρουσιάζεται αλλά μόνο η ψηφιακή υπογραφή κωδικοποιείται με χρήση base64.

⇒ **Signed and enveloped data:** Υπογεγραμμένα και κωδικοποιημένα μόνο αντικείμενα μπορούν να φωλιάζουν. Signed data ή clear-signed data μπορούν να κρυπτογραφηθούν.

Το S/MIME χρησιμοποιείται για να ασφαλίσει το MIME με υπογραφή κρυπτογράφηση ή και τα δυο. Ένα MIME μπορεί να ναι ολόκληρο το μήνυμα ή ένα ή ένα κομμάτι κειμένου από αυτό. Το S/MIME αναπτύχθηκε ειδικά για Internet Standard.

3.3.4 PGP

Η πολύ καλή μυστικότητα (Pretty Good Privacy, PGP) είναι ένα πακέτο software αρχικά αναπτυγμένο από τον Phil Zimmermann το οποίο παρέχει διαδικασίες κρυπτογράφησης για ασφαλή e-mail και για αποθήκευση φακέλων. Ο Zimmermann παρουσίασε ένα συνδυασμό από κρυπτοσυστήματα και πρωτόκολλα και δημιούργησε πρόγραμμα το οποίο μπορεί να τρέξει διάφορες πλατφόρμες.

Το PGP παρέχει μήνυμα κρυπτογράφησης, ψηφιακές υπογραφές και εναρμονισμό του e-mail. Η ευρεία χρήση του PGP οφείλεται στα παρακάτω:

- → Όπως αναφέρθηκε προηγουμένως μπορεί να τρέξει μια ποικιλία πλατφόρμων συμπεριλαμβανομένου DOS/Windows, UNIX, Macintosh και πολλά άλλα.
- → Δημιουργεί ένα συνδυασμό αλγορίθμων κοινών κλειδιών όπως τα RSA, DSS και Diffie-Hellman μαζί με ένα συνδυασμό από συμβατικούς αλγορίθμους όπως CAST-128, IDEA, 3DES και τέλος ο SHA-1 για κώδικα Hash.
- → Έχει μια μεγάλο εύρος εφαρμογής καθώς μπορεί να χρησιμοποιηθεί από άλλους οργανισμούς και μονάδες.
- → Δεν αναπτύχθηκε ή ελέγχεται από κυβερνητικούς ή πρότυπους οργανισμούς.

Γενικά το PGP είναι ένα δυναμικό πακέτο και η χρήση του είναι για να παρέχει προστασία στα e-mail στο κοντινό μέλλον.

3.3.5 Firewalls

Τα Firewalls είναι συστήματα σχεδιασμένα για να προστατεύουν τοπικά συστήματα, το LAN (Local Area Network), ή δίκτυα συστημάτων από τα δίκτυα που βασίζονται σε απειλές ασφαλείας. Την ίδια στιγμή παρέχει πρόσβαση στον έξω κόσμο μέσα από ευρείες περιοχές του δικτύου (WAN) και το Internet. Από τότε που η χρήση του Internet έχει γίνει ζωτικής σημασίας και για οργανισμούς και ατομικά, καθιστά ικανό τον έξω κόσμο να επιδρά στα περιουσιακά στοιχεία του δικτύου. Αυτό δημιουργεί ένα αριθμό από απειλές για τους οργανισμούς. Καθώς υπάρχουν έννοιες παροχής κάθε σταθμού εργασίας και server σε δίκτυο με δυνατή ασφάλεια όπως η αυθαίρετη προστασία, αυτό φαίνεται να μην είναι μια πρακτική προσέγγιση. Ένας εναλλακτικός και ευρέως αποδεκτός τρόπος για να το καταφέρουμε αυτό είναι η χρήση του firewall. Το firewall τοποθετείται μεταξύ του συλλογικού δικτύου και του Internet για να καταφέρει ένα σύνδεσμο ελέγχου και να στήσει ένα εξωτερικό τοίχο ή περίμετρο ασφαλείας. Ο σκοπός αυτής της περιμέτρου είναι να παρέχει μια προστασία από τύπους επιθέσεων βασισμένοι στο Internet και να κατονομάσει ένα μόνο σημείο φραγής όπου η ασφάλεια και ο έλεγχος μπορούν να επιβληθούν. Το firewall μπορεί να ναι ένα μόνο σύστημα υπολογιστή ή ένα σετ από 2 υπολογιστές που μπορούν και συνεργάζονται μεταξύ τους.

Οι βασικοί στόχοι του σχεδιασμού του firewall είναι οι παρακάτω:

- Όλοι η κίνηση από μέσα και από έξω και κάποια ελαττώματα πρέπει να περάσουν μέσα από το firewall
- Μόνο συγκεκριμένη κίνηση, που είναι καθορισμένη από την τοπική τακτική ασφαλείας, θα επιτρέπεται να περνά.
- Το firewall από μόνο του είναι άτρωτο σε διεισδύσεις.

Επίσης υπάρχουν 4 τρόποι όπου το firewall ελέγχει την πρόσβαση εφαρμόζοντας την πολιτική του site ασφαλείας. Αυτοί είναι:

- **Υπηρεσία ελέγχου (Service Control):** Καθορίζει τους τύπους των υπηρεσιών του Internet που μπορεί να υπάρχει πρόσβαση εσωτερικά και εξωτερικά.
- **Υπηρεσία Διεύθυνσης (Direction Control):** Καθορίζει την διεύθυνση όπου ειδικές υπηρεσίες επιτρέπονται να περάσουν μέσο του firewall.
- **Έλεγχος Χρήστη (User Control):** Ελέγχει την πρόσβαση σε μια υπηρεσία που εξαρτάται από το ποιος χρήστης επιθυμεί να έχει πρόσβαση.
- **Έλεγχος Συμπεριφοράς (Behavior Control):** Ελέγχει πως χρησιμοποιούνται συγκεκριμένες υπηρεσίες.

Αυτό που δεν μπορεί να κάνει το firewall είναι ότι δεν μπορεί να παρέχει προστασία σε επιθέσεις που διαπερνούν το firewall. Έτσι το firewall δεν μπορεί να παρέχει καμία προστασία όσο αναφορά τις εσωτερικές απειλές. Τέλος το firewall δεν μπορεί να παρέχει προστασία από μεταφορά προγραμμάτων ή φακέλων τα οποία έχουν προσβληθεί από ιούς.

Γενικά υπάρχουν 3 βασικοί τύποι του firewall: packet filters, application-level-gateways και circuit-level gateways. Κάποιος μπορεί να ισχυριστεί ότι η ανάπτυξη του firewall μπορεί να ανεβάσει το επίπεδο ασφαλείας του δικτύου κατά μεγάλο βαθμό.

3.3.6 Ουσιαστικό Ιδιωτικό Δίκτυο

Το Ουσιαστικό ιδιωτικό δίκτυο (Virtual Private Network,VPN) είναι ένα δίκτυο που χρησιμοποιείται για να έχουμε ένα ασφαλές κανάλι μεταξύ πολλαπλών site κατά μήκος ενός μη ασφαλούς δικτύου όπως είναι το Internet. Το VPN είναι για ιδιωτικό δίκτυο το οποίο απλώνεται στο Internet με σκοπό να ασφαλίσει τις επικοινωνίες σε περιφερειακές και μεμονωμένες υπηρεσίες που επιτρέπουν LAN-over-Internet με αυξημένο κόστος και επιτρέπουν extra συνδέσεις με πελάτες και προμηθευτές. Προγενέστερα στην ανάπτυξη του VPN η μόνη έννοια για προσέγγιση αυτού του είδους επικοινωνίας ήταν με ακριβές μισθωμένες γραμμές ή με διαμορφωμένα εφεδρικά κυκλώματα.

Υπάρχει ένας μεγάλος αριθμός από εφαρμογές του VPN όπου κάθε μια έχει τις δικές της απαιτήσεις . Βασικά υπάρχουν 3 είδη VPN:

♦ **Intranet VPN:** Αυτά είναι VPN μεταξύ εσωτερικών ενσωματωμένων και παραρτημάτων τμημάτων. Οι ιδιαίτερες απαιτήσεις που απαιτούνται είναι: δυνατή κρυπτογράφηση δεδομένων, αξιοπιστία, μια διεύθυνση δεδομένων για 'πώληση' και 'πελάτες' και μια βάση δεδομένων για να προσαρμόσει μη πρότυπα νούμερα νέων χρηστών και τμημάτων.

♦ **Remote Access VPN:** Αυτά είναι VPN μεταξύ ενσωματωμένων δικτύων και κινούμενων ή κινητών υπαλλήλων. Σε αυτή την φάση δυνατή εξουσιοδότηση είναι εφαρμόσιμη σε συνδυασμό με μια κεντρική διεύθυνση και υψηλό βαθμό αναρρίχησης τα οποία θα χειρίζονται τον αυξανόμενο αριθμό των χρηστών που έχουν πρόσβαση στο VPN.

♦ **Extranet VPN:** Αυτό εγκαθίσταται μεταξύ εταιρειών και των συνεργατών της, πελατών και προμηθευτών. Αυτό το συγκεκριμένο VPN απαιτεί μια πρότυπη λύση βάσης (standard-based solution), για να βεβαιώσει την ικανότητα με την έννοια ότι οι συνεργάτες των business μπορεί να συνεργάζονται. Το αποδεκτό από την VPN πρότυπο για Internet-based επικοινωνία είναι η IPSec που αναφέρεται σαν πρωτόκολλο ασφαλείας του Internet (Internet Protocol Security).

Στις μέρες μας υπάρχουν αρκετοί μη σαφής μέθοδοι εφαρμογής του VPN. Πολλά από τα διαθέσιμα προϊόντα είναι ημιτελή και εστιάζονται μόνο σε διαφορετικούς τύπους αιτήσεων του VPN. Οι εφευρέτες του VPN παρέχουν προϊόντα τα οποία μπορούν να παρέχουν επικύρωση γνησιότητας και κρυπτογράφησης, παρόλο που αυτά τα δυο στην πραγματικότητα δεν είναι επαρκή για να οδηγήσουν το VPN για να πραγματοποιήσει τον αρχικό στόχο του. Έτσι χρησιμοποιώντας μη ολοκληρωμένα VPN τα οποία περιορίζουν την λειτουργικότητα του VPN και η πιθανότητα αύξησης των απειλών ασφαλείας αυξάνεται.

3.3.7 GSM

Το GSM σημαίνει (Global System for Mobile Communications), και είναι ένα κυψελοειδής δίκτυο σε περισσότερες από 200 χώρες στον κόσμο. Επειδή χρησιμοποιεί ραδιοσυχνότητες, όπου το GSM είναι μια ασύρματη πλατφόρμα. Αυτό σημαίνει ότι οι χρήστες του GSM μπορούν να είναι πλήρως κινητοί χωρίς να ανησυχούν για προσαρμογές και καλώδια που θα χρειάζονταν σε διαφορετική περίπτωση.

Το κυριότερο χαρακτηριστικό του GSM είναι ότι μπορεί να χρησιμοποιηθεί για υπολογισμό δεδομένων. Οι υπηρεσίες μικρών

μηνυμάτων (Short Message Service, SMS) αφήνει τους subscribers του GSM να στέλνουν και να λαμβάνουν δεδομένα από το κυψελοειδής τηλέφωνό τους χρησιμοποιώντας το πολύ 160 χαρακτήρες. Χάρη στο γεγονός ότι το GSM είναι ψηφιακό, κάποιος μπορεί να συνδέσει το τηλέφωνό του με το laptop του και να στείλει ή να λάβει e-mail, faxes, να κάνει περιήγηση στο Internet ή ακόμη και να χει πρόσβαση στην εταιρεία του LAN/intranet. Το κατάλληλο 'roaming' του GSN επιτρέπει στους κυψελοειδής subscribers να χρησιμοποιούν υπηρεσίες σε οποιαδήποτε περιοχή του GSM στον κόσμο κάτω από οποιεσδήποτε συνθήκες όπου ο provider τους έχει roaming διαφωνίες.

Τα GSM enable-phones έχουν ενσωματωμένα έξυπνες κάρτες (smartcards) που καλούνται Subscriber Identity Module (SIM). Οι κάρτες SIM είναι μοναδικές για κάθε subscriber και χρησιμοποιείται για αναγνώριση του ποσού του στο δίκτυο και να παρέχει επικύρωση.

Το δίκτυο του GSM λειτουργεί με 3 διαφορετικές συχνότητες : GSM 900 (στα 900 MHZ η ακτίνα συχνότητας), GSM 1800 (1800 MHZ) και τέλος GSM 1900 (1900 MHZ). Μέχρι στιγμής η πιο η συχνότητα που χρησιμοποιείται είναι των 900 MHZ.

3.4 Εταιρείες Ασφαλείας στην Πράξη

Όπως έχει ήδη αναφερθεί η μαζική χρήση του Internet και η εκρηκτική άνοδος των ηλεκτρονικών business έχουν κάνει επιτακτική την ανάγκη για ασφάλεια σε οποιαδήποτε network-based επικοινωνία. Γι' αυτό το λόγο μια ποικιλία από εταιρείες έχουν στήσει ένα βασικό σκοπό να σπρώξουν στην αγορά προϊόντα τους που υπόσχονται υψηλό επίπεδο ασφαλείας. Το PKI δείχνει την βάση αυτής της ακολουθίας των προϊόντων που είναι χρήσιμα. Έχοντας μια γρήγορη ματιά στον ηλεκτρονικό κόσμο κάποιος μπορεί να αναγνωρίσει τις πιο γνωστές εταιρείες:

- **Baltimore Technologies:** Η εταιρεία αυτή είναι η παγκόσμια αρχηγός στο PKI και στην e-security τεχνολογία. Παρέχει μια σειρά από προϊόντα που επιτρέπουν και ασφαλίζουν τον κόσμο των e-business. Τα πιο αξιοσημείωτα προϊόντα είναι: σύστημα UniCERT PKI το οποίο είναι Certificate Management Infrastructure, το PKI-Plus που εφαρμόζει αιτήσεις για να λειτουργήσει με το PKI σύστημα παρέχοντας δυνατό Digital Certificate systems, η Baltimore Telepathy η οποία είναι μια συμπληρωμένη λύση για κινητή επικοινωνία, το MailSecure το οποίο είναι προϊόν που ασφαλίζει το e-mail και τέλος έχουμε το SureWare το οποίο είναι ένα αξιόπιστο και ασφαλές κρυπτογραφικό hardware. Σε αντίθεση υπάρχουν πολλά προϊόντα για Web και WAP ασφάλεια.

- **iD2 Technologies:** Η εταιρεία αυτή είναι ο κύριος προμηθευτής smartcard βασισμένοι σε PKI λύσεις. Τέτοια τεχνολογία σήμερα είναι εκ των πραγμάτων πρότυπο για ασφάλεια ψηφιακών συναλλαγών και αναγνώρισης ταυτοτήτων στο Internet. Ο iD2 παρέχει στην αγορά ‘ iD2 Certificate Manager’το οποίο είναι ένα προϊόν που συστήνεται για να συνδυάσει όλα τα απαραίτητα εργαλεία για δημιουργία διεύθυνσης και ανάκλησης ψηφιακών υπογραφών. Ο iD2 Certificate Manager είναι το κλειδί του διαχειριστή των ψηφιακών ταυτοτήτων.

- **Telcordia Technologies:** Η εταιρεία αυτή είναι ο προμηθευτής των software τηλεπικοινωνιακών δικτύων και επαγγελματικών υπηρεσιών. Η Telecordia κάνει τις τηλεπικοινωνίες μπράτσο των Science Applications International Corporation (SAIC), ένα από τα μεγαλύτερα συστήματα και προγραμμάτων διεύθυνσης στον κόσμο.
- **Trintech:** Η Trintech θεωρείται το μέλλον των ασύρματων δικτύων. Ανακοινώνοντας ‘PayWare mAdress’ αποθέματα για ασφαλή πληρωμή δια μέσο του φυσικού κόσμου, με virtual ή κυψελοειδής κανάλια επικοινωνίας. ‘PayWare EveryWhere’ είναι μια τέλος με τέλος ακτίνα ηλεκτρονικής λύσης.

- **IBM:** Το 1999 συστήθηκε η IBM Institute for Advanced Commerce (IAC) για να κατονομάσει την αγορά και τις business που αφορούν ένα στόχο ανάπτυξης μεγάλου όρου αναπαραγωγής επικοινωνιακών λύσεων για ανάγκες συνεργασίας. Η ερευνητική IBM επίσης ερευνά και κάνει προόδους σε πλειστηριασμούς μέσο του Internet, επικοινωνία virtual reality, τεχνολογία μικροσυναλλαγών μέσο του Internet, e-coupons και προαγωγές και ανταλλαγή ηλεκτρονικών δεδομένων.

- **Entrust Technologies:** Η Entrust παρέχει μια σειρά από προϊόντα λύσεων ασφαλείας για το PKI, για ασφάλεια του e-mail, ασφάλεια του Web, VPN, και για ασφάλεια των ασυρμάτων συναλλαγών. Οι ‘Entrust/PKI™’, Entrust/PKI Developer Edition, Entrust/PKI για WAP Certificates είναι όλα λύσεις PKI για να εδραιώσει την ασφάλεια και εμπιστοσύνη στα κανάλια για e-business, Entrust/Express, Entrust/Unity και Entrust/WebConnector τα οποία δημιουργούν ένα σετ από λύσεις ασφαλείας του e-mail. Το Entrust προσφέρει VPN λύσεις όπως Entrust/Access™ και Entrust/VPNConnector τα οποία προωθούν την ανάπτυξη των ψηφιακών διαβεβαιώσεων στις βιομηχανικές συσκευές των VPN.

- **Certicom:** Είναι ο εργοστασιακός προμηθευτής τεχνολογιών ασφαλείας για κινητά συστήματα. Η Certicom βασικά εστιάζεται σε κινητές συνδετικές ασφαλής συσκευές σε επιχειρήσεις και σε συστήματα ηλεκτρονικής επικοινωνίας. Η γραμμή προϊόντων της Certicom περιλαμβάνει κιτ

εργαλείων κρυπτογράφησης και αιτήσεων τα οποία καθιστούν ικανή την εμπιστοσύνη σε διεύθυνση, ανάπτυξη του PKI, πρωτόκολλα ασφαλούς επικοινωνίας,, κοινά κλειδιά και συμμετρική κρυπτογραφία. Στην περιοχή της ασύρματης ασφάλειας η Certicom προσφέρει την SSL (Secure Sockets Layer) Plus for Embedded Systems η οποία βασίζεται σε πρότυπα του Internet, TLS (Transport Layer Security) προσδιορισμός, και 'WTLS Plus' βασίζεται στον προσδιορισμό του WAP για ασύρματα TLS.

3.5 Επίλογος

Καθώς ένας νέος ηλεκτρονικός κόσμος εγκαθίσταται η ανάγκη για υπηρεσίες του Internet είναι μεγάλη. Και το ηλεκτρονικό mail και η χρήση του World Wide Web κάνουν 2 από τις πιο σημαντικές κατανεμημένες αιτήσεις του Internet. Επιπλέον αυτές οι υπηρεσίες έχουν γίνει εφαρμόσιμες και για κινητά τηλέφωνα και άλλες ασύρματες συσκευές. Έτσι η ασφάλεια είναι ένα θέμα που χωρίς καμία αμφιβολία προκαλεί μεγάλο ενδιαφέρον. Η δομή του κοινού κλειδιού έρχεται να μας δώσει την δυνατότητα για να εμποδίσουμε επιθέσεις και να δυναμώσουμε την εμπιστοσύνη στις ηλεκτρονικές business. Το PKI είναι μια επέκταση κοινού κλειδιού κρυπτογράφησης και παρέχει ένα σύστημα με εμπιστευτικότητα, ακεραιότητα αυθεντικότητα και μη άρνησης.

Με σκοπό να εγκαθιδρύσουμε ένα έμπιστο ηλεκτρονικό κόσμο εταιρείες ασφαλείας, υπηρεσίες και κοινωνίες έχουν στηθεί. Ο βασικός σκοπός τους είναι να παρουσιάσουν μια πιο βαθιά έρευνα στο πως απειλές ασφαλείας μπορούν να χαθούν και τελικά να λείψουν από τον ηλεκτρονικό κόσμο με όλες τις πιθανές έννοιες που διασφαλίζουν την ασφάλεια. Τα πιο ευρέως χρησιμοποιούμενα προϊόντα ασφαλείας είναι οι smartcards, S/MIME, PGP, firewalls, VPN και τέλος GSM. Κάθε ένα από αυτά έχει ένα ιδιαίτερο σκοπό αλλά ένας πετυχημένος συνδυασμός από αυτά μπορεί να καταπνίξει ηλεκτρονικές απάτες, κλοπή δεδομένων και οποιαδήποτε άλλη απειλή ασφάλειας της πληροφορίας.

ΚΕΦ 4: Κρυπτοσύστημα RSA – Πρώτοι Αριθμοί

4.1 Εισαγωγή

Σκοπός αυτού του κεφαλαίου είναι να δοθεί μια καθαρή έννοια του κρυπτοσυστήματος κοινού κλειδιού του RSA. Μια συζήτηση στο πως συνδέεται η θεωρεία και τα χαρακτηριστικά των πρώτων αριθμών με τις εφαρμογές του συστήματος που παρουσιάζονται. Επιπλέον, ειδική προσοχή δίνεται στην διορθωτική ικανότητα και στην δύναμη του κρυπτοσυστήματος RSA, ακολουθούμενο από πιθανούς τρόπους ενίσχυσης του συγκεκριμένου πακέτου κρυπτογράφησης.

4.2 Πρώτοι Αριθμοί

Σε αυτό το κομμάτι θα δοθούν έννοιες θεωρητικές έννοιες βασικών αριθμών και θεωρήματα θα παρουσιαστούν. Οι περιοχές αυτές των μαθηματικών εφαρμόζονται στην κρυπτογραφία και ιδιαίτερα σε εφαρμογές του κρυπτοσυστήματος κοινού κλειδιού του RSA.

⇒ **Προσαρμοσμένη Αριθμητική**

Αν έχουμε 2 θετικούς ακεραίους a, n, αν τα διαιρέσουμε το a με το n παίρνουμε το πηλίκο q και ένα υπόλοιπο r από τα οποία ισχύει η σχέση: $a = q\,n + r$. Το υπόλοιπο r συχνά αναφέρεται και σαν residue. Ορίζουμε ‘a mod n’ να είναι το υπόλοιπο όταν το a διαιρείται από το n έτσι θα χουμε $r = a \bmod n$.

Αν a, b 2 ακέραιοι τα οποία προσδιορίζουν έναν ακέραιο n. Οι ακέραιοι a και b λέγονται ‘σύμφωνα’ (congruent), συντελεστής του ακεραίου n και αυτό σαν συντομογραφία γράφεται σαν: $a = b \bmod n$, αν το a-b διαιρείται από το n.

⇒ **Πρώτοι Αριθμοί**

Ένας ακέραιος $n > 1$ είναι πρώτος αριθμός μόνο και μόνο όταν ο διαιρέτης τους είναι τα +1 και –1 και τα +n και –n.

Οι ακέραιοι a, b λέγονται ‘σχετικοί πρώτοι’, αν ο κοινός διαιρέτης τους είναι το 1. Αυτό θα σημειώνεται σαν gcd (a, b) = 1.

Ένας ‘ ψευτοπρώτος ‘ αριθμός n σε μια βάση a είναι ένας τυχαίος σύνθετος αριθμός με $n-1 = d\ 2^s$ (για τυχαίο d) για κάθε ένα $a^d = 1 \bmod n$, ή $a^k = -1 \bmod n$, για $k = d\ 2^r$ και r =0, 1, 2, …., s-1.

⇒ **<u>Παραγοντοποίηση</u>**

Παραγοντοποίηση ενός αριθμού σημαίνει να βρούμε τους πρώτους παράγοντές του.

⇒ **<u>Ανάστροφη Αναπαραγωγή</u>**

Υποθέτουμε ότι ο n είναι πρώτος αριθμός και ο w είναι σχετικός πρώτος του n. Ανάστροφη αναπαραγωγή του w, είναι ένας αριθμός z τέτοιος ώστε $w\ z = 1 \bmod n$.

⇒ **<u>Θεωρεία του Fermat</u>**

Η θεωρεία του Fermat δηλώνει το εξής: Αν n είναι πρώτος αριθμός και a θετικός ακέραιος όχι διαιρετέος από το n τότε $a^{p-1} \equiv 1 \bmod n$.

⇒ **<u>Η θεωρεία του Euler</u>**

Η αθροιστική συνάρτηση του Euler φ (n) είναι ένας αριθμός από θετικούς ακεραίους μικρότεροι του n οι οποίοι είναι σχετικοί πρώτοι του n. Για έναν πρώτο αριθμό n, η φ (n) = n – 1. Υποθέτοντας ότι έχουμε 2 πρώτους αριθμούς p και q για n = p q τότε φ (n) = (p-1) (q-1).

Το θεώρημα του Euler λέει ότι για κάθε a και n ότι είναι σχετικοί πρώτοι : $a^{\varphi(n)} \equiv 1 \bmod n$

⇒ **<u>Θεώρημα Κινέζικου Υπολοίπου</u>**

Αυτό το θεώρημα λέει ότι αν p και q είναι 2 πρώτοι αριθμοί και $a \equiv b \bmod p$ και $a \equiv b \bmod q$, τότε $a \equiv b \bmod (p\ q)$.

⇒ **<u>Θεώρημα του Euclid</u>**

Το θεώρημα του Euclid βασίζεται στο ακόλουθο θεώρημα: εχθρικό κάθε μη αρνητικός ακέραιος a και κάθε θετικός ακέραιος b,
gcd (a, b) = gcd (b, a mod b).

4.3 Ισχύς RSA

Η εφαρμογή του κρυπτοσυστήματος εξαρτάται από το γεγονός ότι:

♦ Είναι σχετικά εύκολο να καθοριστεί πότε ένας αριθμός είναι πρώτος χρησιμοποιώντας αλγορίθμους που παρουσιάζουν τα πρωταρχικά τεστ. Με αυτόν τον τρόπο μεγάλες βάσεις δεδομένων πρώτων αριθμών μπορούν να δημιουργηθούν.

♦ Είναι εύκολο να υπολογιστεί η παράγωγος 2 αριθμών.

♦ Είναι εύκολο να καθοριστεί ένας σχετικά πρώτος αριθμός ‘e’ σε σχέση με κάποιο άλλο νούμερο.

Η ασφάλεια αυτού του κρυπτοσυστήματος εξαρτάται από το γεγονός ότι κάποιος χρειάζεται να γνωρίζει τους πρώτους αριθμούς p και q με στόχο να βρει το μυστικό κλειδί ‘d’ και δεν υπάρχουν αποτελεσματικοί αλγόριθμοι για να χρησιμοποιήσουν τα p και q από το ‘n’ το οποίο έχει γίνει κοινό. Στην πραγματικότητα μια καλή επιλογή από πρώτους συντελεστές για το n θα κάνει το κρυπτοσύστημα RSA άτρωτο κάτω από περισσότερες επιθέσεις.

Όπως έχει ήδη αναφερθεί το κρυπτοσύστημα RSA χρησιμοποιεί ένα συντελεστή του τύπου n = p q, όπου τα p και q είναι χωρισμένα σε ασυνήθιστα πρώτους αριθμούς. Οι πρώτοι αριθμοί p και q πρέπει να έχουν κατάλληλο μέγεθος έτσι ώστε η παραγοντοποίηση των παραγόντων είναι πέρα από κάθε υπολογίσιμη προσέγγιση. Επιπλέον πρέπει να ναι τυχαίοι πρώτοι με την έννοια ότι πρέπει να διαλέγονται σαν μια συνάρτηση τυχαίας εισόδου μέσα από μια διαδικασία καθορισμού κατάλληλων θεμελιωδών υποψηφίων όπου μια εξαντλητική επίθεση είναι αόρατη. Πρακτικά η αποτελεσματικότητα των πρώτων πρέπει να χει και προκαθορισμένο μήκος bit, για τον προσδιορισμό του συστήματος. Η ανακάλυψη του RSA οδήγησε σε μελέτη επιπρόσθετων περιορισμών στην επιλογή των p και q που είναι απαραίτητο να σιγουρέψουν πως το σύστημα RSA είναι ασφαλές από επιθέσεις, και η αντίληψη ενός δυνατού πρώτου αριθμού ορίζεται. Οι δυνατοί πρώτοι έχουν συγκεκριμένες προτεραιότητες που κάνουν τον παράγωγο n δύσκολο συντελεστή από ειδικές μεθόδους. Πάντως πλεονεκτήματα στον συντελεστή φαίνεται να έχει περιορισμένο πλεονέκτημα των δυνατών πρώτων αριθμών. Ένα τέτοιο πλεονέκτημα είναι ο συντελεστής ελλειπτικής καμπύλης. Αυτό δεν σημαίνει ότι είναι λιγότερο ασφαλής από έναν αδύναμο πρώτο αριθμό, αλλά διαλέγοντας μόνο δυνατούς πρώτους αριθμούς δεν αυξάνει την ασφάλεια. Σημασία έχει να διαλέγουμε μεγάλους αρκετά πρώτους αριθμούς. Συγκρίνοντας με τους τυχαίους πρώτους, οι δυνατοί πρώτοι απαιτούν ένα μικρό επιπρόσθετο

χρόνο για υπολογισμό, έτσι υπάρχει μικρό επιπλέον κόστος που τα χρησιμοποιούμε.

Ένα άλλο θέμα που κάποιος μπορεί να θεωρήσει όπου υπάρχει η πιθανότητα να ξεμείνουμε από διάφορους πρώτους. Όπως απέδειξε ο Euclid πριν από 2000 χρόνια υπάρχουν απεριόριστοι πρώτοι αριθμοί. Καθώς το κρυπτοσύστημα RSA χρησιμοποιείται σε εφαρμογές με ένα προκαθορισμένο μήκος κλειδιού, ο αριθμός των πρώτων που ίσως χρησιμοποιηθεί είναι πεπερασμένος. Σε αντίθεση με αυτό ο αριθμός των διαθέσιμων πρώτων είναι πολύ μεγάλος. Σύμφωνα με την θεωρεία των πρώτων αριθμών, ο αριθμός των πρώτων που είναι ή μικρότερος ή ίσος με το n είναι ασύμπτωτος με το n ln (n). Αυτό σημαίνει ότι το μήκος των πρώτων είναι 512 bits ή λιγότερο από 10^{150}. Με άλλα λόγια δεν πρόκειται ποτέ να ξεμείνουμε από πρώτους αριθμούς.

4.4 Παράδειγμα RSA

Με σκοπό να υλοποιήσουμε ένα τρόπο εφαρμογής του RSA δίνεται το επόμενο παράδειγμα.

Έστω η Alice να διαλέγει p = 5 και q = 7 για να φτιάξει το κοινό και το μυστικό της κλειδί. Τότε n = 35. Αν η Alice έχει e = 5 τότε ο σχετικός πρώτος θα ναι 4 * 6 = 24.

Τότε d = 5 αφού 5 * 5 = 1 mod 24. έτσι η ιδιοκτησία του μηνύματος της Alice είναι: $P_A(M) = M^5 \bmod 35$ και $S_A(M) = M^5 \bmod 35$.

Ας υποθέσουμε ότι ο Bob θέλει να στείλει μήνυμα ‘3 mod 35’ στην Alice. Το περιεχόμενό του θα ναι $P_A(3) = 3^5 \bmod 35 = 243 \bmod 35 = 33 \bmod 35$. Έτσι ο Bob στέλνει κρυπτογραφημένο μήνυμα ’33 mod 35’ στην Alice.

Η Alice υπολογίζει το γνήσιο μήνυμα από τις έννοιες του :
S_A: $S_A(33 \bmod 35) = 33^5 \bmod 35$, αυτό είναι ισοδύναμο με το μήνυμα που στάλθηκε ‘3 mod 35’.

Με σκοπό να υλοποιήσουμε αυτό το παράδειγμα αποφεύγοντας τις σύνθετες διαμορφώσεις και συνδυασμούς διαλέγουμε μικρούς πρώτους αριθμούς. Πρακτικά, για να αυξήσουμε την δύναμη του συστήματος κάποιος μπορεί να διαλέξει μεγάλους πρώτους αριθμούς.

4.5 Ορθότητα του RSA

Με στόχο να αποδειχθεί η ορθότητα του RSA κάποιος μπορεί να πει ότι η επόμενη εξίσωση θα ναι: $P(S(M)) = S(P(M)) = M^{ed} \bmod n$ [57].

Αφού τα e και d είναι αντίστροφα πολλαπλάσια του $\varphi(n) = (p-1)(q-1)$ τότε θα έχουμε: $ed = 1 + k(p-1)(q-1)$ για κάποιον ακέραιο k.

Αν $M \equiv 0 \bmod n$, τότε $M^{ed} \equiv \bmod n$

Έστω $M \neq 0$ τότε θα έχουμε

$$\rightarrow \quad M^{ed} \equiv M^{1 + k(p-1)(q-1)}$$

$$\equiv M (M^{(p-1)})^{k(q-1)}$$

$$\equiv M\, 1^{k(q-1)} \pmod p \quad \text{(Από θεώρημα Fermat)}$$

$$\equiv M \pmod p$$

$$\rightarrow \quad M^{ed} \equiv M^{1 + k(p-1)(q-1)}$$

$$\equiv M (M^{(q-1)})^{k(p-1)}$$

$$\equiv M\, 1^{k(p-1)} \pmod n \quad \text{(Από θεώρημα Fermat)}$$

$$\equiv M \pmod q$$

Από το Κινέζικο Θεώρημα Υπολοίπου θα έχουμε ότι $M^{ed} = M \bmod (p, q)$ και έτσι τελικά $M^{ed} = M \bmod n$ για όλα τα M.

4.6 Βελτιώσεις Παραγοντοποίησης

Η παραγοντοποίηση έχει γίνει πιο εύκολη τα τελευταία 15 για 3 λόγους: το hardware των υπολογιστών έχει γίνει πολύ ισχυρό, οι υπολογιστές είναι άφθονοι και φθηνοί και τέλος έχουν γίνει καλύτεροι αλγόριθμοι Παραγοντοποίησης.

Παρόλο που οι βελτιώσεις των hardware έχουν ονομάσει τρόπους επιθέσεων στο RSA έχουν επίσης κάνει το RSA πιο ασφαλές. Αυτό γιατί μια βελτίωση του hardware μπορεί να επιτρέψει στον επιτιθέμενο να παραγοντοποιήσει 2 ψηφία περισσότερο, την ίδια στιγμή θα επιτρέψει στον χρήστη του αλγόριθμου RSA να χρησιμοποιήσει κλειδί για ντουζίνες από ψηφία περισσότερο από πριν. Έτσι η βελτίωση αυτή θα προσθέσει περισσότερη ασφάλεια στο RSA περισσότερη από την επίθεση. Την ίδια χρονική στιγμή υπάρχει ο κίνδυνος στο μέλλον η παραγοντοποίηση να

γίνεται με πιο γρήγορα μηχανήματα. Αυτές οι μηχανές μπορεί να χρησιμοποιηθούν ενάντια των κλειδιών που είχαν δημιουργηθεί στο παρελθόν. Κάτω από αυτές τις συνθήκες η ανάπτυξη του hardware βοηθά μόνο τους επιτιθέμενους και όχι το κρυπτοσύστημα RSA. Ένας τρόπος αντιμετώπισης αυτού του προβλήματος είναι να χρησιμοποιήσουμε μεγαλύτερα κλειδιά σε σχέση με αυτά που χρησιμοποιούνται σήμερα. Επίσης κάθε κλειδί θα μπορεί να αντικαθίσταται από ένα άλλο μεγαλύτερο κάθε μερικά χρόνια, με σκοπό να κερδίσουμε πλεονέκτημα για περισσότερη ασφάλεια που μπορεί να προσφέρουν οι βελτιώσεις του hardware.

Στις μέρες μας όχι μόνο η δύναμη των υπολογιστών αλλά και ο αριθμός τους έχει αυξηθεί προοδευτικά. Αφού μερικοί αλγόριθμοι Παραγοντοποίησης μπορούν να χρησιμοποιηθούν σε εφαρμογές χρησιμοποιώντας πολλούς υπολογιστές που δουλεύουν μαζί, ένα πρόβλημα μπορεί να λυθεί πιο γρήγορα. Αυτή η ανάπτυξη των υπολογιστών δεν φαίνεται να παρέχει περαιτέρω ασφάλεια στο κρυπτοσύστημα RSA.

Άλλη μια απειλή ενάντια στο RSA, είναι το γεγονός ότι έχουν δημιουργηθεί καλύτεροι αλγόριθμοι Παραγοντοποίησης. Σε σύγκριση με το παρελθόν η παραγοντοποίηση έχει γίνει ένα εύκολο κομμάτι, άσχετα από την ταχύτητα του hardware. Παρόλα αυτά η παραγοντοποίηση είναι ένα δύσκολο πρόβλημα. Η πιθανότητα ανάπτυξης αλγορίθμου Παραγοντοποίησης μπορεί να αποδυναμώσει σοβαρά το RSA, αλλά αυτή η περίπτωση σύμφωνα με τους ειδικούς φαίνεται μακρινή και όχι πραγματοποιήσιμη.

4.7 Μέγεθος Κλειδιού RSA

Άλλο ένα θέμα το οποίο έχει εμφανιστεί έχει να κάνει με το μέγεθος του κλειδιού που πρέπει να χρησιμοποιηθεί όταν εφαρμόζεται ο RSA. Το μέγεθος του κλειδιού στον αλγόριθμο RSA τυπικά αναφέρεται στο μέγεθος του παράγοντα n. Οι 2 πρώτοι αριθμοί p και q, που συνθέτουν τον n, θα πρέπει να ναι περίπου ίσου μήκους. Αυτό κάνει το n πιο δύσκολο για παραγοντοποίηση από το αν ένας από τους 2 πρώτους είναι πολύ μικρότερος από τον άλλον. Σε περίπτωση που οι 2 πρώτοι που έχουν επιλεχθεί είναι πολύ κοντά ή η διαφορά τους είναι πολύ μικρή για ένα προκαθορισμένο ποσό, τότε υπάρχει ρίσκο στην ασφάλεια. Πάντως η πιθανότητα για κάτι τέτοιο είναι πάρα πολύ μικρή.

Η επιλογή του μεγέθους του RSA κλειδιού εξαρτάται από τις απαιτήσεις ασφαλείας. Όσο μεγαλύτερος είναι ο παράγοντας τόσο καλύτερη ασφάλεια έχουμε αλλά και πιο αργές λειτουργίες του RSA. Η απόφαση για το μέγεθος του κλειδιού θα πρέπει να παρθεί σύμφωνα με την αξία των προστατευμένων δεδομένων, την χρονική στιγμή που πρέπει να

προστατευθούν και τέλος πόσο ισχυρές μπορεί να είναι οι απειλές. Θα πρέπει να σημειωθεί ότι το μήκος του κλειδιού για το RSA σύστημα είναι πολύ μεγαλύτερο από αυτά των μπλοκ κρυπτογραφίας όπως το DES, αλλά η ασφάλεια ενός RSA κλειδιού δεν μπορεί να συγκριθεί με την ασφάλεια κλειδιού άλλου συστήματος ξεκάθαρα σε σχέση με το μήκος. Εργαστήρια του RSA προτείνουν συνήθως μήκη κλειδιών 1024 bit για συγκροτημένη χρήση και 2048 bit για πολύ σημαντικά αρχεία όπως το root κλειδί που χρησιμοποιείται από συγκεκριμένη αρχή.

Γενικά αυξάνοντας το μέγεθος του κλειδιού μπορεί να είναι η απαρχή για περαιτέρω μείωση της ασφάλειας που προκαλείται από τις βελτιώσεις που έχουμε ήδη προαναφερθεί. Όσο το hardware συνεχίζει να βελτιώνεται σε γρήγορη ακτίνα σε σχέση με την ακτίνα περιπλοκής των αλγορίθμων παραγοντοποίησης που μειώνεται, τότε η ασφάλεια του RSA αυξάνει υποθέτοντας ότι οι χρήστες αυξάνουν τακτικά το μέγεθος του κλειδιού τους σε λογικά ποσά.

4.8 Επίλογος

Σήμερα πρέπει να δοθεί μεγάλη προσοχή και στους αλγόριθμους κοινού κλειδιού και ιδιαίτερα στο κρυπτοσύστημα κοινού κλειδιού RSA. Το RSA είναι ένα κρυπτοσύστημα το οποίο δουλεύει με βάση την θεωρεία των πρώτων αριθμών. Η ασφάλεια αυτού του συστήματος βασίζεται κυρίως στην δυσκολία του να βρεθούν πρώτοι παράγοντες ενός γνωστού αριθμού. Με αυτόν τον τρόπο το μυστικό κλειδί του αλγορίθμου δεν μπορεί εύκολα να αποκτηθεί και έτσι το κρυπτοσύστημα δεν είναι τρωτό σε ειδικές επιθέσεις. Παρόλα αυτά βελτιώσεις παραγοντοποίησης έχουν επιτευχθεί και το γεγονός ανάπτυξης ενός ειδικού αλγόριθμου παραγοντοποίησης είναι ένα πολύ δύσκολο κεφάλαιο. Η επιλογή του μεγέθους του RSA κλειδιού είναι επίσης μια άλλη έννοια ώθησης της αντίστασης του κρυπτοσυστήματος ενάντια σε επιθέσεις κρυπτοανάλυσησης. Γενικά έχει αποδειχθεί ότι το RSA είναι ένα ισχυρό πακέτο κρυπτογράφησης και οποιαδήποτε προσπάθεια επίθεσης στο σύστημα έχει αποτύχει ή δεν είναι επαρκής.

ΚΕΦ 5: Πρωταρχικά Τεστ Αλγορίθμων

5.1 Εισαγωγή

Έχοντας υπόψη την θεωρεία των πρώτων αριθμών το πως συνδέεται με το κοινό κλειδί κρυπτοσυστήματος RSA κάποιος μπορεί να ισχυριστεί ότι η επιλογή ενός ζευγαριού πρώτων διαμορφώνει την βάση ενός επιτυχημένου RSA συστήματος. Με σκοπό να παρουσιαστεί αυτή η επιλογή, κάποιος πρέπει πρώτα να παράγει το ζευγάρι των πρώτων που θα χρησιμοποιηθεί. Η μέθοδος της γενιάς των πρώτων αριθμών και τα αρχικά τεστ των τεχνικών που υιοθετούνται σε αυτό το κομμάτι είναι τα θέματα που θα συζητηθούν παρακάτω. Συγκεκριμένα ένα αρχικό ειδικό τεστ που ονομάζεται τεστ πιθανοτήτων Rabin-Miller, το οποίο θα εξεταστεί σε βάθος και θα συγκριθεί με τα άλλα τεστ που έχουν ήδη αναφερθεί σε προηγούμενα κεφάλαια. Τέλος μια εφαρμογή ενός RSA αλγορίθμου κρυπτογράφησης θα παρουσιαστεί σε συνδυασμό με το τεστ των Rabin-Miller το οποίο χρησιμοποιείται για να τεστάρει ζευγάρι πρώτων αριθμών που χρησιμοποιούνται στο RSA σύστημα.

5.2 Γενιά Πρώτων Αριθμών

Όπως έχει ήδη αναφερθεί η χρήση των πρώτων αριθμών συστήνει την βάση για την εφαρμογή του RSA κρυπτοσυστήματος. Επομένως στην ερώτηση στο πως κανείς μπορεί να δημιουργήσει πρώτους αριθμούς που θα χρησιμοποιηθούν τελικά στην ανάπτυξη του RSA δημιουργείται. Η πιο φυσική μέθοδος για να πραγματοποιηθεί αυτό είναι να διαλεχτεί ένας τυχαίος και περιττός αριθμός ‘n’ κατάλληλου μεγέθους και στην συνέχεια να ελεγχθεί αν αυτός είναι πρώτος αριθμός ή όχι. Στην περίπτωση που αποδειχθεί ότι δεν είναι τότε πρέπει να γίνει ξανά επιλογή και να γίνει η ίδια διαδικασία.

Ένα τεστ για αρχικότητα μπορεί να είναι τεστ που να αποδεικνύει ότι το υποψήφιο νούμερο είναι πρώτος, σε περίπτωση που το νούμερο αναφέρεται σαν αποδείξιμος πρώτος, είτε να ναι τεστ το οποίο εδραιώνει ένα πιο αδύναμο αποτέλεσμα, όπως ότι ο n είναι ‘πιθανόν’ πρώτος. Ο επόμενος τύπος τεστ καλείται ‘Αρχικά Τεστ Πιθανοτήτων’ (Probabilistic Primality Tests), και καθορίζει με μαθηματική ακρίβεια ποια υποψήφια n είναι σύνθετα. Τα τεστ πιθανοτήτων δεν αποδεικνύουν ότι το n είναι πρώτος, έτσι σε αυτή την περίπτωση το νούμερο που τεστάρεται δηλώνεται ότι είναι ‘πιθανόν πρώτος’. Από την άλλη μεριά τα αληθή αρχικά τεστ όπως

λέγονται επιτρέπουν σε κάποιον να δηλώνει με μαθηματική ακρίβεια ότι ένας αριθμός είναι πρώτος. Σε σύγκριση με τα τεστ πιθανοτήτων τα αληθή αρχικά τεστ απαιτείται να έχουν πολύ καλύτερες μαθηματικές πηγές.

5.3 Πρωταρχικά Τεστ

5.3.1 Αληθή Πρωταρχικά Τεστ

5.3.1.1 Lucas-Lehmer Τεστ

Το τεστ αυτό χρησιμοποιείται για να καθορίσει την αρχικότητα των καλούμενων Mersenne αριθμών. Ένας Mersenne αριθμός είναι ένας ακέραιος του τύπου 2^{s-1}, όπου s≥ 2. Αν 2^{s-1} είναι πρώτος τότε είναι Mersenne αριθμός.

Σύμφωνα με τους Lucas-Lehmer το τεστ γίνεται για να καθορίσει το πότε ένας Mersenne αριθμός είναι πρώτος . Η διαδικασία είναι η ακόλουθη:

→ Έστω s≥ 3. Ο Mersenne αριθμός $n = 2^{s-1}$ είναι πρώτος όταν και μόνο όταν ικανοποιούνται οι 2 επόμενες καταστάσεις:

1. s είναι πρώτος και
2. Η συχνότητα των ακεραίων καθορίζεται από $u_0 = 4$ και
   $u_{k=1} = (u_k^2 - 2) \bmod n$, για k≥ 0 και ικανοποιείται το $u_{s-2} = 0$.

Ο αλγόριθμος που χρησιμοποιείται για την εφαρμογή αυτού του τεστ αποδεικνύεται ότι είναι ένας προκαθορισμένος πολύποδας χρόνου αλγόριθμος.

5.3.1.2 Τεστ με την χρήση Παραγόντων

Ένα πρωταρχικό τεστ σε έναν ακέραιο n μπορεί να παρουσιαστεί με την χρήση παραγοντοποίησης ή με μερική παραγοντοποίηση του (n-1). Η παραγοντοποίηση του n-1 μπορεί να ναι πιο εύκολη στον υπολογισμό αν n είναι αριθμός Fermat όπου αυτό ισχύει αν ο n είναι ένας αριθμός της μορφής $n = 2^k + 1$ όπου $k = 2^l$.

Σύμφωνα με αυτό το τεστ:

→ Έστω n ≥ 3 είναι ένας ακέραιος. Τότε ο n είναι πρώτος αν και μόνο αν υπάρχει ακέραιος a που να ικανοποιεί τα εξής:

1. $a^{n-1} \equiv 1 \bmod n$ και

2. $a^{(n-1)/q} \neq 1 \bmod n$ για κάθε πρώτο διαιρέτη q του (n –1).

5.3.1.3 Jacobi Sum Set

Το τεστ Jacobi Sum είναι ένα άλλο αληθινό πρωταρχικό τεστ. Η βασική ιδέα είναι να ελέγξουμε ένα κομμάτι από αναλογίες οι οποίες αναλογούν στην θεωρεία του Fermat σε σίγουρα κυκλοτομικά δαχτυλίδια. Αυτός είναι σχεδόν ένας πολυώνυμος χρόνος αλγορίθμου.

Ένα μειονέκτημα του αλγορίθμου είναι ότι δεν παράγει βεβαίωση η οποία θα ήταν ικανή να μπορεί να επαληθεύσει την ερώτηση σε μικρότερο χρόνο από το να τρέξει ο αλγόριθμος από μόνος του.

5.3.1.4 Τεστ Ελλειπτικής Καμπύλης

Η έκδοση αυτή του αλγορίθμου που χρησιμοποιείται πρακτικά συνήθως αναφέρεται σαν Atkin's Test ή Elliptic Test Primality Providing Algorithm (ECPP). Σε σύγκριση με το τεστ του Jacobi Sum έχει το πλεονέκτημα να παρέχει σύντομη βεβαίωση αρχικότητας η οποία μπορεί να χρησιμοποιηθεί να βεβαιώσει την αρχικότητα του αριθμού.

Το τεστ Atkin έχει χρησιμοποιηθεί πιο πολύ να αποδείξει την αρχικότητα των αριθμών που είναι περισσότεροι από 1000 δεκάδες.

5.3.2 Πρωταρχικά Τεστ Πιθανοτήτων

5.3.2.1 Fermat's Τεστ

Το θεώρημα του Fermat βεβαιώνει ότι αν n πρώτος αριθμός και a ένας οποιοσδήποτε ακέραιος με $1 \leq a \leq n-1$, τότε θα έχουμε $a^{n-1} \equiv 1 \bmod n$. Έτσι για ένα δοσμένο ακέραιο όπου η πρωταρχικότητα του είναι σε ερώτηση, βρίσκοντας ένα νούμερο 'a' σε αυτό το κενό όπως αυτή η ισοδυναμία δεν είναι αληθής επαρκεί για να δειχτεί ότι ο n είναι σύνθετος.

→ Έστω n ένας περιττός σύνθετος ακέραιος. Ένας ακέραιος a, $1 \leq a \leq n-1$ ονομάζεται μάρτυρας του Fermat (Fermat's witness) για το πόσο σύνθετος είναι ο n όταν $a^{n-1} \neq 1 \bmod n$.

Αυτό που πρέπει να σημειωθεί είναι ότι το τεστ του Fermat δεν είναι ακριβώς πρωταρχικό τεστ αφού συνήθως αποτυγχάνει να διακρίνει μεταξύ πρώτων αριθμών και ειδικών σύνθετων ακεραίων που καλούνται αριθμοί Carmichael.

5.3.2.2 Τεστ Solovay – Strassen

Το πρωταρχικό τεστ πιθανοτήτων των Solovay-Strassen ήταν από τα πρώτα τεστ που εκλαϊκεύτηκαν από την εμφάνιση της κρυπτογραφίας κοινού κλειδιού και συγκεκριμένα στο κρυπτοσύστημα RSA. Το τεστ αυτό βασίζεται στο παρακάτω γεγονός:

→ **Κριτήριο Euler:** Έστω n ένας περιττός πρώτος. Τότε $a^{(n-1)/2} \equiv (a/n) \bmod n$ για όλους τους ακεραίους 'a' που ικανοποιούν την σχέση gcd (a, n)= 1.

Πρακτικά το κρυπτοσύστημα RSA δεν χρησιμοποιεί το τεστ των Solovay-Strassen στις παρούσες εφαρμογές. Και αυτό γιατί ένα εναλλακτικό τεστ των Rabin-Miller είναι χρήσιμο.

5.3.2.3 Τεστ Rabin-Miller

Πρακτικά το τεστ των Rabin-Miller είναι αυτό που χρησιμοποιείται πιο πολύ. Αναφέρεται επίσης και σαν 'Τεστ Δυνατών Ψευδοπρώτων' (Strong Pseudoprime Test). Το τεστ που παρουσιάζουμε βασίζεται στα παρακάτω γεγονότα:

→ **Γεγονός 1:** Έστω n ένας περιττός πρώτος και $n-1 = 2^s r$, όπου r περιττός. Έστω r a να ναι ένας ακέραιος gcd (a, n)= 1. Τότε είτε ο $a^r \equiv 1 \bmod n$, ή $a^k \equiv -1 \bmod n$, με $k=2^j r$ για κάποιο j, $0 \leq j \leq s-1$.

→ **Γεγονός 2:** Αν ο n είναι περιττός πρώτος τότε η εξίσωση $x^2 \equiv 1 \bmod n$ έχει 2 λύσεις. Οι λύσεις αυτές είναι $x \equiv 1$ και $x \equiv -1$.

Το τεστ γενικά περιγράφεται σύμφωνα με τον παρακάτω ορισμό:
→ Έστω n ένας περιττός σύνθετος αριθμός και $n-1 = 2^s r$ όπου r περιττός. Έστω a ένας ακέραιος στο διάστημα [1, n-1].

1. Αν $a^r \neq 1 \bmod n$ και $a^k \neq -1 \bmod n$, $k =2^j r$, για όλα τα j, $j \leq s-1$, τότε ο a καλείται 'δυνατός μάρτυρας' (strong witness) για τον n.
2. Αν είτε $a^r \equiv 1 \bmod n$ ή $a^k \equiv -1 \bmod n$ για κάποιο j, $j \leq s-1$ τότε ο n λέγεται 'δυνατός ψευδοπρώτος' (strong pseudoprime) στην βάση a. Ο ακέραιος a λέγεται 'δυνατός ψεύτης' (strong liar) για την αρχικότητα του n.

Στο παράρτημα Α υπάρχει ένα διάγραμμα της εφαρμογής του τεστ των Rabin-Miller. Ο αλγόριθμος χρησιμοποιείται για εφαρμογές των τεστ για να

καθορίσουν πότε ο αριθμός που ελέγχεται είναι πιθανόν πρώτος ή όχι, είναι το επόμενο κομμάτι που λαμβάνεται υπόψη. Η διαδικασία για την εφαρμογή του τεστ λέγεται 'probablyprime' και τα βασικά χαρακτηριστικά του είναι αυτά που ακολουθούν:

→ **probablyprime[n, t]**

Είσοδος: ένας παράξενος ακέραιος n≥ 3 και μια παράμετρος ασφαλείας t≥ 1 η οποία καθορίζει έναν αριθμό διαφορετικού του 'a' για το οποίο το τεστ θα τρέχει.

Έξοδος: για την ερώτηση του probablyprime[n, t] το τεστ θα έχει έξοδο 'True' αν το n είναι πιθανός πρώτος αλλιώς αν δεν είναι θα είναι 'False'.

Γράφουμε $n- 1=2^s r$, όπου r περιττός
Για 'i' από 1 στο t γίνονται τα εξής:

1. Διαλέγουμε ένα τυχαίο αριθμό 'a' τέτοιο ώστε $2\leq a\leq n-2$
2. Θέτουμε $z=a^r \bmod n$
3. Αν z=1 ή αν z=n-1 τότε ο n περνά το τεστ και ίσως είναι πρώτος αριθμός.
4. Αν j>0 και z=n-1 τότε ο n δεν είναι πρώτος.
5. Θέτουμε j=j+1. Αν j<s και $z\neq n-1$ θέτουμε $z=z^2 \bmod n$ και γυρίζουμε στο βήμα 4. Αν z=n-1 τότε ο n περνά το τεστ και ίσως είναι πρώτος αριθμός.
6. Αν j=s και $z\neq n-1$ τότε ο n δεν είναι πρώτος.

Η πιθανότητα ενός σύνθετου αριθμού περνώντας το τεστ των Rabin-Miller μειώνεται πιο γρήγορα αν συγκριθεί με άλλα πρωταρχικά πιθανοτικά τεστ. Τρία τέταρτα των πιθανών αξιών του 'a' εγγυούνται για να ναι μάρτυρες. Αυτό σημαίνει ότι ένας σύνθετος αριθμός θα γλιστρήσει μέσο του τεστ 't' όχι περισσότερο από $1/4^t$ του χρόνου όπου t ο αριθμός των επαναλήψεων. Για τους περισσότερους τυχαίους αριθμούς όπως το 99.9 τοις εκατό των πιθανών 'a' αξιών είναι μάρτυρες (witnesses).

Υπάρχουν καλύτερες εκτιμήσεις: Για υποψήφιους πρώτους των n-bit όπου n είναι περισσότεροι του 100, η πιθανότητα λάθους είναι μικρότερη από 1 σε $4n2^w$ με $w=(k/2)^{(1/2)}$. Και για 256-bit n η πιθανότητα λάθους σε 6 τεστ είναι μικρότερη από 1 σε 2^{51} .

5.3.2.4 Συμπεράσματα Από Τα Τεστ

Έχοντας υπόψη και τα δυο τεστ των Rabin-Miller και των Solovay-Strassen, κάποιος μπορεί να ισχυριστεί ότι και τα 2 είναι σωστά στο γεγονός

ότι είτε η είσοδος είναι στην πραγματικότητα πρώτος, ή ότι μοιράζονται το ότι η είσοδος είναι σύνθετη. Πάντως συγκρίνοντας αυτά τα δυο τεστ, το τεστ των Rabin-Miller φαίνεται να έχει αντικαταστήσει το τεστ των Solovay-Strassen σε μια από τις περισσότερες βεβαιώσεις περιλαμβάνοντας και τον αλγόριθμο RSA. Οι λόγοι που το τεστ των Rabin-miller θεωρείται καλύτερο είναι οι εξής:

⇒ Το τεστ των Solovay-Strassen έχει αποδειχθεί ότι υπολογιστικά είναι πιο ακριβό.

⇒ Η εφαρμογή του είναι πολύ πιο δύσκολη.

⇒ Σύμφωνα με εκτιμήσεις οι πιθανότητες λάθους του τεστ των Rabin-Miller είναι λιγότερες από αυτές του τεστ των Solovay-Strassen.

5.4 Εφαρμογή Παραδείγματος RSA

Υποθέτουμε ότι κάποιος θέλει να κρυπτογραφήσει το παρακάτω μήνυμα υιοθετώντας το κρυπτοσύστημα RSA κοινού κλειδιού:

M = THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Για να κρυπτογραφήσουμε το M, το μήνυμα θα πρέπει πρώτα να μετατραπεί σε ακέραιο. Το σχήμα για να κωδικοποιήσουμε την αλφάβητο είναι του τύπου: SPACE: 00, A =01, B =02,…..Z =26. Έτσι το μήνυμα M θα γίνει:

M = 2008050 0172109 0311000 2181523 1400061 5240010 2113161 9001522 0518002 0080500 1201262 5000415 07

Ας υποθέσουμε τώρα ότι το διαλεγμένο ζευγάρι από πρώτους αριθμούς τεστάρονται από τον αλγόριθμο Rabin-Miller στο παράρτημα A, είναι p = 1877 και q =1901. Τότε n = 3568177 και e =1103 σχετικά πρώτος στο (p-1)(q-1) = 3564400. Το κλειδί του συστήματος το οποίο θα γίνει κοινό είναι το ακόλουθο ζευγάρι: (n, e) = (3568177, 1103). Το μήνυμα M θα κρυπτογραφηθεί σε μπλοκ έτσι ώστε κάθε μπλοκ να αντιπροσωπεύει ακεραίους όχι μεγαλύτερους του n. Έτσι η κρυπτογράφηση θα παρουσιάζεται με 12 μπλοκ των 7 μονάδων για κάθε ένα και για κάθε ένα μπλοκ των 2 μονάδων.

Το πρώτο μπλοκ M_1 = 2008050 θα κρυπτογραφηθεί από

$C_1 = 2008050^{1103} \bmod 3568177$ το οποίο είναι ίσο με $C_1 = 1728489$. Κάνοντας ακριβώς την ίδια διαδικασία για το κάθε ένα από τα εναπομείναντα μπλοκ ολόκληρο το μήνυμα θα γίνει:

1728489 2512835 2076705 3248027 1596366 1018233 165098 1888640 810690 1883678 744028

Αυτό το μήνυμα μπορεί να αποκρυπτογραφηθεί υψώνοντας κάθε μπλοκ ως έξης d^{th} power (modulo n) όπου d είναι το κλειδί αποκρυπτογράφησης του αλγορίθμου.

5.5 Επίλογος

Όπως το κεφ 4 αποδεικνύει ότι και το κοινό κλειδί και το μυστικό κλειδί στο RSA κρυπτοσύστημα αποκτούνται με την χρήση των πρώτων αριθμών. Συνεπώς εμφανίζεται το ερώτημα στο πως μπορούμε να γενικεύσουμε τους πρώτους αριθμούς. Ένα πρωταρχικό τεστ είναι ένα τεστ με το οποίο τσεκάρεται πότε ένας δοσμένος αριθμός είναι πρώτος ή όχι. Γενικά υπάρχουν 2 κύριοι τύποι πρωταρχικών τεστ: αληθή πρωταρχικά τεστ και τα πρωταρχικά τεστ πιθανοτήτων. Η βασική διαφορά αυτών των 2 είναι ότι το είδος του τύπου του τεστ αποδεικνύει ότι ο υποψήφιος αριθμός είναι πρώτος επειδή ο υποψήφιος εγκαθιστά ένα αδύναμο αποτέλεσμα ότι το νούμερο είναι ‘πιθανόν’ πρώτος.

Το κρυπτοσύστημα RSA υιοθετεί ένα πρωταρχικό αλγόριθμο πιθανοτήτων που λέγεται τεστ Rabin-Miller. Αυτό το τεστ καθορίζει με βεβαιότητα ποιοι αριθμοί είναι σύνθετοι αλλά δεν αποδεικνύει ποιοι αριθμοί είναι πρώτοι. Ειδικότερα, η πιθανότητα ενός σύνθετου αριθμού που περνά το τεστ είναι το πολύ στο τέταρτο από τις βάσεις πιθανοτήτων ‘a’ για τις οποίες τρέχει το τεστ. Σε σύγκριση με τα άλλα πρωταρχικά τεστ , ο αλγόριθμος Rabin-Miller έχει αποδειχθεί ότι είναι ο πιο αποτελεσματικός στο να κρίνει τη πιθανότητα του υποψήφιου αριθμού.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα τελευταία χρόνια έχει υπάρξει μια μεγάλη αύξηση στην καθημερινή χρήση των δικτύων με έσω-υπολογιστές. Τα δίκτυα υπολογιστών είναι μια προσπάθεια σύνδεσης διαφορετικών συστημάτων υπολογιστών και τερματικών. Αυτά αναφέρονται σαν πηγές δικτύου και η εσωτερική σύνδεση απαιτεί και συσκευές software και συσκευές hardware. Όταν γίνεται η οργάνωση ξεχωριστών πηγών υπολογιστών για να δράσουν σαν ένα σύστημα, τα μονοπάτια δεδομένων μεταξύ των πηγών πρέπει να υπάρχουν για να διευκολύνεται η επικοινωνία τους. Έτσι κανάλια επικοινωνιών εγκαθίσταται για να καλύψουν έννοιες δεδομένων που ρέουν από οποιαδήποτε πηγή δικτύου σε άλλη πηγή δικτύου. Ο τρόπος διεργασίας και διανομής των δεδομένων στο δίκτυο, που συνεισφέρει στο να γίνει μετάδοση πληροφορίας μεταξύ υπολογιστών είναι ένα θέμα προς εξερεύνηση. Συνεπώς το θέμα παροχής υψηλού βαθμού ασφαλείας της πληροφορίας έχει γίνει περίπλοκο και πολύ ευαίσθητο. Επιπλέον περαιτέρω μυστική σκέψη εμβαθύνει την ανάγκη σχεδιασμού επικοινωνιακών δεσμών και δικτύων τα οποία ενσωματώνουν δομές προστασίας δεδομένων.

Η νέα παγκόσμια κουλτούρα της ανταλλαγής ηλεκτρονικής πληροφορίας και δικτύου έχει θέσει την βάση συνδετικού Internet. Το Internet περιέχει έναν αριθμό από Local Area Networks που λέγονται και αλλιώς LAN, σύνδεση εσωτερικά PCs, servers και ίσως ένα ή δυο κύριες κατασκευές που παρέχουν και σε οργανισμούς και σε μεμονωμένους χρήστες ουσιαστικές πληροφορίες και υπηρεσίες. Η πανταχού παρούσα φύση χαμηλού κόστους του Internet έχει προκαλέσει έκρηξη στο Electronic Data Processing όσο και στις ηλεκτρονικές business και στις δραστηριότητες ηλεκτρονικής επικοινωνίας. Το Internet παρέχει συνεργασίες με νέες και ενδιαφέρουσες ευκαιρίες για την ανάπτυξη ενός πρόσθετου καναλιού για προσφορά υπηρεσιών. Τοποθετώντας τις business ‘on line’ ανοίγει ένας νέος κόσμος πιθανοτήτων όπως αύξηση επιπέδου υπηρεσιών, ηλεκτρονικές συναλλαγές και πληρωμές , web shopping και αυξημένης ικανότητας. Το Wireless Application Protocol (WAP) σχεδιάστηκε για να εργάζεται εντός των περιορισμών που έχουν οι κινητές ασύρματες συσκευές που πρέπει να λειτουργούν, παρουσιάζοντας μια ευκαιρία στους ασύρματους συνδρομητές να κερδίσουν από κινητή πρόσβαση σε αιτήσεις του Internet. Έτσι οι υπηρεσίες του Internet μπορεί να αναπτυχθούν και από ασύρματες συσκευές.

Η παγκόσμια δημοτικότητα του Internet σε συνδυασμό με το γεγονός ότι το Internet παραμένει ανώνυμο, κάνει πιο δύσκολο το να ξέρει κανείς ποιος είναι στην άλλη πλευρά του δικτύου, πια μεγάλη πιθανότητα υπάρχει να είναι απάτη, ηλεκτρονικό mail, κρυφοκοίταγμα, κλοπή δεδομένων όπως

η ακούσια διόρθωση φακέλων από αναρμόδιους χρήστες. Με αυτό τον τρόπο η ασφάλεια της πληροφορίας έχει γίνει θέμα τεράστιου ενδιαφέροντος για τον σημερινό ηλεκτρονικό κόσμο. Κάποιος πρέπει να έχει τα ίδια επίπεδα αυτοπεποίθησης και εμπιστοσύνης στον ηλεκτρονικό κόσμο όπως και στον παραδοσιακό κόσμο. Με σκοπό να ασφαλιστούν οι business και οι επικοινωνίες του Internet, συσκευές κρυπτογράφησης δικτύου και άλλες τεχνικές χρησιμοποιούνται. Διάφορες εταιρείες ασφαλείας και υπηρεσίες έχουν επίσης εισαχθεί με βασικό στόχο να εξοπλίσουν την αγορά με ηλεκτρονική επικοινωνία και λύσεις ηλεκτρονικής ασφάλειας. Τα προϊόντα ασφαλείας που ναι διαθέσιμα στην ηλεκτρονική κοινωνία υπόσχονται να προσφέρουν στους πελάτες τους αληθινή παγκόσμια ηλεκτρονική ασφάλεια.

Η εδραίωση των κρίκων των δεδομένων επικοινωνίας μεταξύ συστημάτων υπολογιστών έχει κάνει την μεταφερόμενη πληροφορία ιδιαίτερα τρωτή στην εισχώρηση ανεπιθύμητων χρηστών. Η κρυπτογραφία είναι η επιστήμη που ειδικεύεται στην προσφορά πιθανών λύσεων για προβλήματα ασφαλείας. Πολλές κρυπτογραφικές έννοιες έχουν χρησιμοποιηθεί για αιώνες από τον στρατό μέχρι πρόσφατα όπου κρυπτογραφικά σχήματα έχουν μεγάλη σημασία για τον εμπορικό κόσμο. Γενικά η κρυπτογραφία μπορεί να παρέχει προστασία, επικύρωση όπου ένα μήνυμα δεν έχει αλλαχτεί κατά την μεταφορά και απόλυτα επικυρώνει τον αποστολέα. Σ’ ένα αλγόριθμο κρυπτογραφίας, η πληροφορία αλλάζει με τέτοιους τρόπους όπου αν παραβιαστεί η ασφάλεια η πληροφορία παραμένει συγκαλυμμένη. Η κρυπτογραφία φαίνεται να προστατεύει την μεταδιδόμενη πληροφορία από τροποποιήσεις και εσφαλμένη διαδρομή εισάγοντας μηχανισμούς κρυπτογράφησης δεδομένων.

Όταν εφαρμόζεται ένας αλγόριθμος κρυπτογράφησης, η πληροφορία κρυπτογραφείται σε μια ενδιάμεση μορφή στο σημείο μετάδοσης και στην συνέχεια ανακτάται στο τέλος του σημείου επικοινωνίας. Η δύναμη του κρυπτοσυστήματος καθορίζεται από την αντίσταση που φαίνεται να έχει το σύστημα όταν δέχεται επίθεση. Τα κρυπτοσυστήματα είναι χωρισμένα σε 2 θεμελιώδης κατηγορίες: στους συμβατικούς αλγόριθμους και στους αλγόριθμους κοινού κλειδιού. Τα συμβατικά σχήματα διαφέρουν από το κοινό κλειδί από την μια ότι στην χρήση τους χρησιμοποιούν ένα μόνο κλειδί κρυπτογράφησης. Οι πιο γνωστοί συμβατικοί αλγόριθμοι που χρησιμοποιούνται είναι οι Data Encryption Standard DES, IDEA, FEAL, και Blowfish. Από την άλλη μεριά οι αλγόριθμοι κοινού κλειδιού χρησιμοποιούν 2 κλειδιά κρυπτογράφησης όπου το ένα είναι κοινό και το άλλο μυστικό. Ένα παράδειγμα κρυπτοσυστήματος κοινού κλειδιού είναι ο αλγόριθμος RSA, το οποίο είναι ένα από τα πιο δυνατά συστήματα του είδους του. Και οι 2 τύποι αλγορίθμων κρυπτογράφησης μπορεί να ναι θύματα της κρυπτοανάλυσης. Μια κρυπτοαναλυτική επίθεση μπορεί να

πάρει σαν πλεονέκτημα κάθε πιθανή αδυναμία που μπορεί να έχει το κρυπτοσύστημα και σκοπός του είναι να ανακτήσει το κλειδί κρυπτογράφησης ή και το αρχικό μήνυμα που πρόκειται να μεταδοθεί. Αναπόφευκτα μερικές επιθέσεις ασφαλείας είναι πολύ δύσκολο να ανιχνευθούν ή ακόμη και να εμποδιστούν. Μέχρι στιγμής διάφοροι πρόοδοι έχουν γίνει και σε συσκευές software και σε συσκευές hardware και μπορούν πιο εύκολα να σταματήσουν επιθέσεις. Αλλά πρακτικά όμως τα περισσότερα από τα τεχνολογικά επιτεύγματα έχουν δώσει το ερέθισμα να ξεπερνούν κατά ένα βαθμό το όπλο των επιτιθεμένων. Έχοντας υπόψη την ευαίσθητη φύση της πληροφορίας, το υιοθετημένο κρυπτοσύστημα δεν πρέπει να υποχωρεί σε επιθέσεις που απειλούν την αυθεντικότητα και ακεραιότητα των δεδομένων. Για να κρατηθεί η πληροφορία αλώβητη στα πιο απαιτητικά περιβάλλον ασφαλείας, το κοινό κλειδί κρυπτογραφίας έχει προηγηθεί από μια συγκεκριμένη εταιρεία ασφαλείας την Public Key Infrastructure (PKI).

Το PKI είναι ένα σύστημα που χρησιμοποιεί κρυπτογραφία κοινού κλειδιού και ψηφιακές βεβαιώσεις για να κατορθώσει ασφαλής υπηρεσίες του Internet. Γενικά προσφέρει μια κοινή φόρμα ασφαλείας για επιχειρήσεις και κοινό δίκτυο. Το PKI συμπληρώνει την βάση για εφαρμογή διάφορων λύσεων ασφαλείας όπως οι έξυπνες κάρτες (smartcards), S/MIME, PGP, VPN's, GSM και τα firewalls. Με την βοήθεια του PKI ένας μπορεί να ασφαλίσει το ηλεκτρονικό mail, τα web sites, όπως συναλλαγές business-to-business και συναλλαγές από χρήστη σε χρήστη. Σαν αποτέλεσμα το PKI έχει γίνει το πρότυπο ασφαλείας του Internet. Πολλές υπάρχουσες εταιρείες ασφαλείας και ερευνητικά κέντρα δίνουν μεγάλη έμφαση στην ικανότητα και λειτουργικότητα του PKI και εφοδιάζουν την αγορά με προϊόντα τους. Εταιρείες όπως η IBM, Certicom, Baltimore και η iD2 δουλεύουν σε προϊόντα που υπόσχονται αυξημένη ασφάλεια και εμπιστοσύνη. Χωρίς καμία αμφιβολία, πιο μεγάλο ενδιαφέρον παρατηρείται σε πιο σοβαρά θέματα περικύκλωσης της πληροφορίας. Αυτό τέλος αντανακλά σε πιο δυνατή αύξηση ευκαιριών για εξάλειψη της αλλοίωσης και καταστροφής της πληροφορίας.

Στις μέρες μας κρυπτοσυστήματα κοινού κλειδιού και ιδιαίτερα ο αλγόριθμος κοινού κλειδιού RSA χρησιμοποιούνται για επιτευχθεί υψηλότερο επίπεδο ασφάλειας της πληροφορίας. Η δύναμη του κρυπτοσυστήματος RSA βασίζεται στο γεγονός ότι δεν υπάρχουν αποδοτικές έννοιες για να βρεθούν πρώτοι παράγοντες οπουδήποτε αριθμού. Από τότε που και τα δυο κλειδιά, κοινό και μυστικό, εκφράζονται με βάση την παράγωγο των 2 πρώτων αριθμών, η ασφάλεια του μυστικού κλειδιού εξαρτάται από την εύρεση της πρώτης παραγώγου. Καθώς οι μέθοδοι παραγοντοποίησης συνεχίζουν να βελτιώνονται και η δύναμη των υπολογιστών να αυξάνεται, μια περαιτέρω γνώμη υποστήριξης του

αλγόριθμου RSA είναι να αυξήσουμε το μέγεθος του κλειδιού στην κρυπτογράφηση RSA. Η ταχύτητα και η αποδοτικότητα πολλών εμπορικών και χρήσιμων software και hardware εφαρμογών του αλγορίθμου RSA αυξάνεται ραγδαία. Σε σύγκριση με το DES το κρυπτοσύστημα RSA έχει αποδειχθεί πολύ πιο αργό. Πάντως το RSA γενικά χρησιμοποιείται σε μια ευρεία ποικιλία προϊόντων και τύπων σε βιομηχανίες σε όλο τον κόσμο.

Έχοντας υπόψη τα βασικά βήματα που ακολουθήθηκαν για την εφαρμογή του RSA, το θέμα της γενιάς των πρώτων αριθμών υψώνεται. Η ανάγκη του RSA για μεγάλους πρώτους αριθμούς καθοδηγείται από την εισαγωγή των πρωταρχικών τεστ για καθορισμό πότε 2 αριθμοί είναι πρώτοι ή όχι. Συγκεκριμένα υπάρχουν 2 τύποι πρωταρχικών τεστ: τα αληθή πρωταρχικά τεστ και τα πρωταρχικά τεστ πιθανοτήτων. Στο κρυπτοσύστημα RSA η διαδικασία των πρωταρχικών τεστ εστιάζεται στα πρωταρχικά τεστ πιθανοτήτων των αλγόριθμων. Ειδικότερα, ο RSA υιοθετεί το πρωταρχικό τεστ των Rabin-Miller το οποίο καθορίζει με σιγουριά ποιοι αριθμοί είναι σύνθετοι αλλά δεν αποδεικνύει αν ότι ο αριθμός είναι πρώτος. Παρόλα αυτά, η πιθανότητα λάθους είναι αρκετά μικρή κάνοντας αυτό το τεστ πιο δυνατό και προτιμότερο σε σύγκριση με άλλα πρωταρχικά τεστ πιθανοτήτων.

Σαν τελικό συμπέρασμα ο ηλεκτρονικός κόσμος έχει αναπτυχθεί ραγδαία τα τελευταία χρόνια και όλο και περισσότεροι οργανισμοί έχουν την διάθεση για μετάδοση των business με έναν ηλεκτρονικό τρόπο. Το Internet έχει ήδη δείξει τον επαναστατικό τρόπο παρουσίασης των business, ταυτόχρονα αυξάνοντας το κόστος λειτουργικότητας και αυξάνοντας επίσης το επίπεδο εξυπηρέτησης πελατών. Πάντως η επιθυμία για ασφαλή Internet είναι πολύ μεγάλη. Μέχρι τώρα μεγάλα πλεονεκτήματα έχουν προσεγγίσει την περιοχή ασφάλειας της πληροφορίας, αλλά ακόμη περαιτέρω καινοτομίες αναμένεται να ονομαστούν για ασφαλής μελλοντικές γραμμές επικοινωνίας.

ΠΑΡΑΠΟΜΠΕΣ

1. DeMillo, R.A, Davida, G.I, Dobkin, D.P, Harrison, M.A, Lipton, R.J. (1983). 'Applied cryptology, cryptographic protocols, και computer security models', Proceedings of Symposia in Applied Mathematics,v29, American Mathematical Society, USA.

2. http://www.nsb.gov.tw/english/nsb0f/nsbf11.htm

3. http://www.tieturi.fi/DSN2000/sessionedescription.asp?id=108

4. http://www.rsasecurity.com/rsalabs/faq/4-2-1.html

5. http://www.rsasecurity.com/rsalabs/faq/4-2-2.html

6. http://www.rsasecurity.com/rsalabs/faq/4-2-3.html

7. http://www.mondex.com/

8. http://www.rsasecurity.com/rsalabs/faq/4-2-4.html

9. http://www.rsasecurity.com/rsalabs/faq/4-2-5.html

10. Stallings, William. (1999). 'Cryptography and Network Security, Principles and Practice', Prentice Hall Inc, USA.

11. http://www.nsb.gov.tw/english/nsb0f/nsbf14.htm

12. http://www.nmrc.org/faqs/hackfaq/hackfaq-2.html

13. http://www.Europe.cnn.com/TECH/specials/hackers/cyberterror/

14. http://www.europ.cnn.com/2000/TECH/space/07/03/nasa.hacker.02/

15. http://www.tieturi.fi/DSN2000/sessiondescription.asp?id=110

16. http://www.semper.org/sirene/outsideworld/orgs.html

17. http://www.internettcrimesgroup.com/services.htm

18. Dinardo, C.T. (1978). 'Computers and Security', The Information Technology Series,vIII, AFIPS Press, USA

19. Schneier, B. (1996). 'Applied Cryptography', John Wiley & Sons Inc, USA

20. Meyer, C.H. and Matyas, S.M (1982). 'Cryptography: A new dimension in computer data security'. Wiley-Interscience, NY

21. Dorothy, E. and Denning, R. (1982). 'Cryptography and data security', Addison-Wesley Publishing Company Inc, USA

22. Bosworth, B. (1982). 'Codes, ciphers and computes: A introduction to information security', Hayden Book Company Inc, USA

23. Welsh, D. (1988). 'Codes and cryptography', Clarendon Press, Oxford

24. Deavours, C.A., Kahn, D., Mellen, G., Winkel, B. (1987). 'Cryptology-Yesterday, today, and tomorrow', Artech House Inc, USA pp. 379-396

25. Davio, M., Desmedt, Y., Quisquarter, J.J. (1985). 'Propagation characteristics on the DES', Advances in Cryptology, EUROCRYPT'84, Springer-Verlag, Germany

26. Campbell, K.W. (1993). 'DES is not a group', Advances in Cryptology-CRYPTO'92, Springer Verlag, Germany

27. Biham, E., Shamir, A. (1993). 'Differential cryptanalysis of the full 16 round DES', Advances in Cryptology-CRYPTO'92. Springer Verlag, Germany

28. Hoffman, L.J. (1977). 'Modern methods for computer security and privacy', Prentice Hall Inc, USA

29. Kranakis, E., (1986). 'Primality and Cryptography', John Wiley and Sons Ltd, Great Britain

30. Micali, S., (1993). 'Fair public key cryptosystems', Advances in Cryptology-CRYPTO'92, Springer Verlag, Germany

31. Baltimore Paper. (2000). 'A beginner's guide to public key cryptography and certificates', UniCERT Overview Guide v3.0.6, Baltimore Technologies, plc.

32. http://venus.utm.edu/research/primes/glossary/RSA.html

33. http://www.rsasecurity.co.uk/rsalabs/faq/3-1-9.html

34. http://www.rsasecurity.co.uk/rsalabs/faq/3-1-2.html

35. http://www.rsasecurity.com/rsalabs/faq/2-4-2.html

36. http://www.rsasecurity.com/rsalabs/faq/2-4-5.html

37. http://www.rsasecurity.co.uk/rsalabs/faq/3-1-3.html

38. http://www.stack.nl/~galactus/remailers/attack-2.html

39. Baltimore Paper. (2000). 'What is a public key infrastructure?', UniCERT Overview Guide v3.0.6, Baltimore Technologies, plc

40. http://www.baltimore.com
Baltimore Paper. (2000). 'An introduction to PKI: Executive Briefing' Baltimore Technologies, plc

41. Turbat, A. (1985). 'Smart Cards: Introductory remarks', Advances in cryptology, EUROCRYPT'84, Springer-Verlag, Germany

42. http://www.harrier.com/networks/solutions/smartcard.html

43. http://www.harrier.com/networks/solutions/barrier.html

44. http://www.checkpoint.com/products/vpn1/vpndef.html

45. http://www.gsmdata.com/whatsgsm.htm

46. http://www.baltimore.com/products/index.html

47. http://www.id2tech.com/

48. http://www.telcordia.com/pssindex.html

49. http://www.trintech.com/products/index/html
50. http://www.research.ibm.com/cross_disciplines/ecommerce.html

51. http://www.entrust.com/products/index.html

52. http://www.certicom.ca/products/index.html

53. Menezes, A. J., Oorschot, P. C., Landrock, P (1997). 'Handbook of applied cryptology', chapter4, σελ 133-138

54. http://www.rsasecurity.co.uk/rsalabs/faq/3-1-4.html

55. http://www.rsasecurity.co.uk/rsalabs/faq/3-1-6.html

56. http://www.csm.astate.edu/~rossa/datasec/cnp.html

57. Cormen, T. H., Leiserson, C. E., Rivest, R. L. (1990). 'An introduction to algorithms', MIT Press, USA

58. http://www.rsasecurity.co.uk/rsalabs/faq/2-3-5.html

59. http://www.rsasecurity.co.uk/rsalabs/faq/3-1-5.html

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Ασφάλεια Πληροφοριών, Τεχνικά Νομικά και Κοινωνικά Θέματα. ΕΛΛΗΝΙΚΗ ΕΤΑΙΡΕΙΑ ΕΠΙΣΤΗΜΟΝΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ.

2. Le, T. V., Nguyen, K. Q., Varadharajan, V. (1999). 'How to prove that a committed number is', Advances in Cryptology- ASIACRYPT'99, Springer-Verlag, Germany

3. Miller, G. (1976). 'Rienmann's hypothesis and tests for primality', J.Comp. Syst. Sci.13, σελ 300-317

4. Monier, L. (1980). 'Evaluation and comparison of two efficient probabilistic primality testing algorithms', Theor. Comp. Sci.12, σελ 97-108

5. Rabin, M. O. (1980). 'Probabilistic algorithm for testing primality', J Number Th. 12, σελ 128-138

6. Wolfram, S. (1996). 'The Mathematica Book', Wolfram Research Inc, USA

ΠΑΡΑΡΤΗΜΑ Α

ΕΦΑΡΜΟΓΗ ΠΡΟΓΡΑΜΜΑΤΟΣ RABIN-MILLER

Ο παρακάτω κώδικας εφαρμόζει το πρωταρχικό τεστ των Rabin-Miller και τρέχει πάνω στην Mathematica Version 2.2 Software Package για windows.

```
(*  This function takes a number n as input                                    *)
(*  and outputs a list of the exponent  s and the odd factor  r, such          *)
(*  that  n = 2^s  r                                                          *)


sr [n_] := Module [  (s = 0,  r = n),
While [ Mod [r, 2] == 0, s ++;  r = Quotient [r, 2]  ];
{s, r}
]

(*  The function 'tnp' tests for ;test not prime', and the returns          *)
(*  'True' if n is not prime                                                *)
(*  and 'false' if n is prime. The tests performed are:                     *)
(*  Initialize  dl  to  1  and  d2  to  'a'                                 *)
(*  While the exponent is nonzero and positive                              *)
(*  {                                                                       *)
(*  1. If the lower bit of the exponent r is 1 (if r is odd),               *)
(*  multiply   d2  into  d1                                                 *)
(*  Square  d2  and  shift  off the lower bit of the exponent               *)
(*  2. If the squaring produced – 1modn, return false                       *)
(*  3. If  1 is produced then we have square roots of 1 other               *)
(*  than  =1, -1, and return True                                          *)
(*  ]                                                                       *)
(*  Square   d2  (b – 1) times. If any  square is –1modn, return False,    *)
(*  if it is 1, return True                                                 *)
(*  In the last test, if we have either 1 or –1modn, then return            *)
(*  False, else True                                                        *)

tnp [n_, a_, s_, r_]  : = Module [ {ex = r, d1 = 1, d2 = a, twos = s},
While  [ex > 0,
     If [Mod[ex, 2] == 1, d1 = Mod[d1 * d2, n], ];
    d2 = Mod[d2 * d2, n];
    ex = Quotient[ex, 2];
    If  [  d2 ==  n – 1,  Return[False], ];
```

```
    If [ d2 == 1, Return[True], ];
];
If [ d1 == n – 1, Return[False], ];
If [ d1 == 1, Return[False], ];
While [twos > 1,
        d1 = Mod [d1*d1, n];
        twos --;
        If [ d1 == n – 1, Return [False], ];
        If [ d1 == 1, return [True], ];
];

If [ (d1 == 1) || d1 == n – 1, Return [False], return [True]];
]



(* The function 'probablyprime' takes as input the number n to be *)
(* tested, and the number of iterations for different 'a' *)
(* If the function returns True then n may be prime, *)
(* if False then the tested number is composite *)



probablyprime [n_, t_] : =Module [
            {srres = sr {n – 1], a},

For [ i=0, i < t, i++,
    a = Random [Integer, {2, n-2} ];
    Print ["Trying", a];
    If [tnp [n, a, First [srres], Last [srres] ], Return [False}, ]
];

Return [True]
]
```

ΤΕΣΤ ΠΡΟΓΡΑΜΜΑΤΟΣ

Probablyprime[11111111111111111,20]
Trying 57957008531214907
Trying 774056409820823160
Trying 262708053201618473
Trying 399417081636265442
Trying 1059604173485215773
Trying 213354400423098751
Trying 265562424597563945
Trying 60347265851735263
Trying 529603508932235888
Trying 519939539526423050
Trying 783262771854441985
Trying 320624152961793383
Trying 743648647822212647
Trying 304260230543347581
Trying 934592893067890040
Trying 171089833998691915
Trying 905270565937962851
Trying 794250238239744611
Trying 7239710711136294
Trying 296247883224520967
True

probablyprime[1001,5]
Trying 136
False

probablyprime[9,4]
Trying 4
False

probablyprime[7,5]
Trying 5
Trying 4
Trying 3
Trying 3
Trying 4
True
probablyprime[35667529,10]
Trying 4198871
Trying 1357737

Trying 25740762
Trying 14996774
Trying 27542159
Trying 29198941
Trying 18067140
Trying 14486606
Trying 11047869
Trying 3190906
True

probablyprime[1999,10]
Trying 1944
Trying 1782
Trying 794
Trying 1534
Trying 528
Trying 690
Trying 1374
Trying 612
Trying 1637
Trying 583
True

probablyprime[674563988,15]
Trying 372019365
False

probablyprime[3457631,15]
Trying 1701908
Trying 1381681
Trying 2063386
Trying 836607
Trying 3201845
Trying 2888939
Trying 1033654
Trying 470562
Trying 1360607
Trying 468115
Trying 3235995
Trying 3095260
Trying 1830317
Trying 103422
Trying 343478
True

probablyprime[4563413,15]
Trying 1932480
Trying 3324130
Trying 4464101
Trying 2864605
Trying 1904704
Trying 2951037
Trying 2720629
Trying 691817
Trying 2902172
Trying 12087
Trying 323681
Trying 3814349
Trying 3414256
Trying 4307798
Trying 3901286
True

probablyprime[1877,10]
Trying 662
Trying 1856
Trying 779
Trying 1541
Trying 314
Trying 1024
Trying 888
Trying 205
Trying 641
Trying 1147
True

probablyprime[1901,10]
Trying 10
Trying 953
Trying 154
Trying 827
Trying 1005
Trying 449
Trying 245
Trying 900
Trying 1747

Trying 512
True