ΤΕΙ ΗΠΕΙΡΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ & ΔΙΟΙΚΗΣΗΣ

ΘΕΜΑ ΠΤΥΧΙΑΚΗΣ

ΜΠΕΝΕΚΗ ΔΗΜΗΤΡΑ

Α.Μ. 3460

ΕΙΣΗΓΗΤΗΣ:
ΚΑΘΗΓΗΤΗΣ
ΤΣΙΑΝΤΗΣ ΛΕΩΝΙΔΑΣ

ΑΡΤΑ 2006

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΠΡΟΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

ΕΦΑΡΜΟΓΕΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

ΠΡΟΤΕΙΝΟΜΕΝΑ ΣΥΣΤΗΜΑΤΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

ΔΗ. 3460

ΔΕΛΛΑΣ ΣΤΕΦΑΝΟΣ
ΓΑΒΑΛΑΣ ΔΗΜΗΤΡΙΟΣ
ΣΤΑΜΟΥΛΗΣ ΓΕΩΡΓΙΟΣ

ΑΘΗΝΑ 2006

ΠΕΡΙΕΧΟΜΕΝΑ **σελίδες**

1.ΕΙΣΑΓΩΓΗ:

Τα τελευταία χρόνια το Διαδίκτυο αναπτύσσεται και επεκτείνεται με εκθετικούς ρυθμούς τόσο σε επίπεδο πλήθους χρηστών, όσο και σε επίπεδο παρεχόμενων υπηρεσιών. Τεράστιος όγκος και μεγάλη ποικιλία πληροφοριών (πολιτικών, στρατιωτικών, οικονομικών) διακινείται πλέον μέσω του Διαδικτύου, γεγονός που καθιστά διαρκώς αυξανόμενη την ανάγκη προστασίας και ασφάλειας, αφού η μη εξουσιοδοτημένη πρόσβαση στις διακινούμενες πληροφορίες πιθανόν να έχει καταστρεπτικές συνέπειες.

Το πρόβλημα της ασφάλειας στα δίκτυα υπολογιστών γενικά έχει απασχολήσει έντονα τόσο τους επιστήμονες, όσο και εταιρίες ανάπτυξης λογισμικού και δικτυακών υποδομών προς την κατεύθυνση της πληρέστερης κατανόησης και επίλυσής του.

Η ασφάλεια των δικτύων και των πληροφοριακών συστημάτων είναι σήμερα, η μεγαλύτερη πρόκληση στο χώρο της Πληροφορικής. Παρά το ότι, η έρευνα στον τομέα αυτό, σημειώνει σημαντική πρόοδο ,η εμπιστοσύνη των απανταχού χρηστών δεν έχει αποκτηθεί, εφόσον καθημερινά, προκύπτουν νέα κρούσματα ανθρώπων που έχουν εξαπατηθεί.

Η ασφάλεια σήμερα βασίζεται, όπως είναι λογικό, στην κρυπτογράφηση, της οποίας η μέθοδοι ποικίλουν και έχουν αναπτυχθεί, στα βάθη των αιώνων, που τις χρησιμοποιούν οι άνθρωποι, για να προστατέψουν «ευαίσθητα» δεδομένα. Εδώ και αρκετά χρόνια λοιπόν, η κρυπτογράφηση έχει αναχθεί σε Επιστήμη (Κρυπτογραφία), η οποία βασίζεται στα Μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων.

Η Πληροφορική με τη σειρά της, τάχθηκε στις υπηρεσίες της συγκεκριμένης Επιστήμης, σαν εργαλείο, κάνοντας χρήση των εξαιρετικά υψηλών ταχυτήτων ανάλυσης δεδομένων, για να κωδικοποιεί δεδομένα. Ενώ, ταυτόχρονα χρησιμοποιεί επιτυχείς μεθόδους της κρυπτογραφίας, για την εξασφάλιση των δικτύων και των πληροφοριακών συστημάτων της. Η

κρυπτογράφηση δίνει δικαιώματα πρόσβασης σε δεδομένα, μόνο σε εξουσιοδοτημένους χρήστες. Η μέθοδος κρυπτογράφησης βασίζεται συνήθως, σε κάποιο αλγόριθμο για τον οποίο υπάρχει πάντα ένα «κλειδί». Όσο αυξάνεται ο βαθμός πολυπλοκότητας του αλγορίθμου κρυπτογράφησης, τόσο μειώνεται η πιθανότητα προσπέλασής του, ενώ η αποκρυπτογράφησή του είναι δυνατή μόνο με τη χρήση του κλειδιού.

Στις συναλλαγές, αλλά και σε πολλές άλλες ηλεκτρονικές εφαρμογές χρησιμοποιείται σήμερα η ηλεκτρονική υπογραφή, η οποία κρυπτογραφείται κατά την αποστολή και αποκρυπτογραφείται κατά την παραλαβή. Η ηλεκτρονική υπογραφή, αποτελεί στην ουσία έναν κωδικό πρόσβασης, όπως συνήθως, χρησιμοποιούμε στις ηλεκτρονικές συσκευές και για την εξασφάλιση της ακεραιότητας των συναλλαγών.

Κανένα σύστημα δεν είναι αδιάβλητο. Παρ' όλα αυτά οι ηλεκτρονικές συναλλαγές εξυπηρετούν τους πολίτες σε μεγάλο βαθμό. Οι χρήστες οφείλουν λοιπόν, να εμπιστεύονται μόνο Ιστοσελίδες με υψηλό βαθμό ασφάλειας.

2. ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΣΤΟ ΧΩΡΟ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Η κρυπτογραφία, η επιστήμη της κρυπτογράφησης και αποκρυπτογράφησης πληροφοριών, μπορεί να χαρακτηριστεί σαν ένα από τα αρχαιότερα επαγγέλματα της ανθρωπότητας, έχοντας τις ρίζες της βαθιά στο παρελθόν.

2.1 Η κρυπτογραφία κατά τους αρχαίους χρόνους

Κατά το 1900 π.Χ. στην Αίγυπτο για πρώτη φορά χρησιμοποιήθηκε μια παραλλαγή των τυπικών ιερογλυφικών της εποχής για την επικοινωνία.

Μια από τις παλαιότερες αναφορές στην κρυπτογραφία υπάρχει στην Ιλιάδα του Ομήρου, όπου αναφέρεται η αποστολή ενός κρυπτογραφημένου μηνύματος από τον Βελλερεφόντη.

Ο δίσκος της Φαιστού, 17ος αιώνας π.Χ. δεν έχει ακόμα αποκρυπτογραφηθεί. Ο Ηρόδοτος περιγράφει πώς μεταφέρονταν κρυπτογραφημένα μηνύματα από τους αγγελιοφόρους. Οι αρχαίοι Εβραίοι κρυπτογραφούσαν κάποιες λέξεις στις περγαμηνές τους.

Ο Πολύβιος ήταν ο πρώτος που χρησιμοποίησε αριθμούς σε μορφή πίνακα για την κωδικοποίηση γραμμάτων.

Η πρώτη καταγεγραμμένη χρήση της κρυπτογραφίας για επικοινωνιακούς σκοπούς είναι από τους Σπαρτιάτες το 400 π.Χ. που χρησιμοποιούσαν τον αλγόριθμο της σκυτάλης για την επικοινωνία ανάμεσα στους στρατηγούς τους. Χρησιμοποιούσαν έναν ξύλινο κύλινδρο γύρω από τον οποίο τύλιγαν μια ταινία από δέρμα και έγραφαν το μήνυμα. Όταν η ταινία ξετυλιγόταν τα γράμματα ήταν ανακατεμένα και μη αναγνώσιμα. Για να διαβάσει κάποιος το μήνυμα έπρεπε να τυλίξει την ταινία σε ένα κύλινδρο ίδιων διαστάσεων.

Οι Φαραώ συνήθιζαν να γράφουν τα μηνύματά τους στο ξυρισμένο κεφάλι κάποιου σκλάβου και να τον στέλνουν στον παραλήπτη όταν τα μαλλιά του είχαν ξαναμεγαλώσει. Αυτός δεν είχε παρά να ξυρίσει το σκλάβο για να διαβάσει το μήνυμα. Μερικές φορές απλοποιούταν η αποστολή στέλνοντας μόνο το κεφάλι. Η μέθοδος αυτή είχε προφανή προβλήματα και η αξιοπιστία της επιβαρυνόταν ακόμα περισσότερο από τη συνήθεια των σκλάβων να προσπαθούν να απελευθερωθούν από τα αφεντικά τους.

Οι Αιγύπτιοι ιερείς χρησιμοποιούσαν μέθοδο αντίστοιχη με τη σκυτάλη των Σπαρτιατών, την οποία χρησιμοποίησε και ο Ιούλιος Καίσαρας. Επίσης μεθόδους κρυπτογραφίας είχαν αναπτύξει και οι Αριστοτέλης, Πυθαγόρας και Νέρωνας.

Ο Ιούλιος Καίσαρας (100 – 44 π.Χ.) χρησιμοποίησε μια απλή αντικατάσταση στο κανονικό αλφάβητο (μετακίνηση – shift των γραμμάτων κατά μια προκαθορισμένη ποσότητα – τρία γράμματα) στις "κυβερνητικές" επικοινωνίες (Caesar cipher). Ο Αύγουστος Καίσαρας χρησιμοποίησε την ίδια μέθοδο μετακινώντας κατά ένα γράμμα

2.2 Η κρυπτογραφία από το μεσαίωνα μέχρι τον 20ο αιώνα

Οι πρώτοι που κατάλαβαν καλά τις αρχές της κρυπτογραφίας και της κρυπτανάλυσης ήταν οι Άραβες. Κατασκεύασαν και χρησιμοποίησαν αλγόριθμους αντικατάστασης και μετατόπισης και ανακάλυψαν τη χρήση της συχνότητας των χαρακτήρων και των πιθανοτήτων στην κρυπτανάλυση. Έτσι το 1412 ο Al-Kalka-Shandi συμπεριέλαβε την περιγραφή αρκετών κρυπτογραφικών συστημάτων στην εγκυκλοπαίδεια Subh al-a'sha και έδωσε σαφείς οδηγίες και παραδείγματα για την κρυπτανάλυση κρυπτογραφημένων κειμένων χρησιμοποιώντας τη συχνότητα των χαρακτήρων.

Η Ευρωπαϊκή κρυπτολογία έχει τις ρίζες της το μεσαίωνα, που αναπτύχθηκε από τους Πάπα και τις Ιταλικές πόλεις κράτη, αλλά τα περισσότερα συστήματα βασίζονταν στην απλή αντικατάσταση γραμμάτων της αλφαβήτου (όπως στον αλγόριθμο του Καίσαρα). Οι πρώτοι αλγόριθμοι βασίζονταν στην αντικατάσταση των φωνηέντων. Το πρώτο Ευρωπαϊκό εγχειρίδιο κρυπτογραφίας (1379) ήταν μια συλλογή αλγορίθμων από τον Gabriele de Lavinde of Parma, για τον Πάπα. Το 1470 ο Leon Battista Alberti εξέδωσε το "Trattati in cifra", όπου περιγράφεται ο πρώτος δίσκος κρυπτογράφησης (τον οποίο είχε κατασκευάσει το 1460), χρησιμοποιώντας και την έννοια της χρήσης πολλαπλών αλφαβήτων. Επίσης στο βιβλίο αυτό περιέγραφε και τις αρχές της ανάλυσης συχνότητας των γραμμάτων.

Ο Sir Francis Bacon το 1563 περιέγραψε έναν αλγόριθμο που σήμερα φέρει το όνομά του. Ήταν ένας αλγόριθμος που χρησιμοποιούσε κωδικοποίηση 5 bits. Τον αλγόριθμο αυτό τον εξέλιξε σαν μια μέθοδο στεγανογραφίας, χρησιμοποιώντας μία μεταβολή στη μορφή των χαρακτήρων μετέφερε κάθε bit της κωδικοποίησης. Ο Blaise de Vigenere δημοσίευσε ένα βιβλίο πάνω στην κρυπτολογία το 1585, που περιέγραφε τον αλγόριθμο της πολυαλφαβητικής αντικατάστασης. Ακολούθησαν και άλλα βιβλία πάνω στην κρυπτογραφία με εξελίξεις των αλγορίθμων.

Τα μυστικά της κρυπτολογίας φυλάσσονταν στα μοναστήρια ή στα μυστικά αρχεία των βασιλιάδων και λίγες μέθοδοι γίνονταν ευρέως γνωστές.

Κατά την αναγέννηση η κρυπτολογία έγινε χωριστή επιστήμη και ταυτόχρονα οι εφαρμοστές της αναζητούσαν μια γενική γλώσσα.

Το 1600 ο Καρδινάλιος Ρισελιέ χρησιμοποιούσε μια κάρτα με τρύπες για να γράψει το μήνυμά του. Όταν τελείωνε γέμιζε τα κενά με λέξεις ώστε να μοιάζει με ένα κανονικό γράμμα. Για την αποκωδικοποίηση χρειαζόταν η κάρτα με την οποία είχε γραφεί το γράμμα.

Το 1776 ο Αμερικάνος Arthur Lee ανέπτυξε ένα κώδικα με βιβλίο τον οποίο σύντομα υιοθέτησε ο στρατός.

Επίσης ο Thomas Jefferson εφηύρε ένα wheel cipher το 1790 που έμελλε να μετασχηματιστεί στο Strip Cipher, M-138-A, που χρησιμοποιήθηκε από το Αμερικανικό ναυτικό κατά τον 2ο Παγκόσμιο Πόλεμο.

Ένας άλλος διάσημος κώδικας είναι ο κώδικας Μορς, που αναπτύχθηκε από τον Samuel Morse το 1832, και απλώς περιγράφει τον τρόπο κωδικοποίησης του αλφαβήτου σε μακρείς και σύντομους ήχους. Με την ταυτόχρονη ανακάλυψη του τηλέγραφου ο κώδικας Μορς βοήθησε στην επικοινωνία των ανθρώπων σε μεγάλες αποστάσεις.

Το 1860 οι μεγάλοι κώδικες χρησιμοποιούνταν συχνά στις διπλωματικές επικοινωνίες. Στη διπλωματία και κατά τις περιόδους πολέμου υπήρχε

αυξημένη χρήση της κρυπτογραφίας, χαρακτηριστικό παράδειγμα είναι τα one-time pads που χρησιμοποιούνταν ευρέως.

Στα πρώτα χρόνια της Αμερικάνικης ιστορίας έχουμε την ευρεία χρήση κωδίκων σε βιβλία. Κατά τον εμφύλιο πόλεμο έγινε εκτεταμένη χρήση αλγορίθμων μετάθεσης από το ένα μέρος και του αλγορίθμου Vigenere από το άλλο μέρος. Στην προσπάθεια αποκρυπτογράφησης των εχθρικών μηνυμάτων χρησιμοποιήθηκαν μέχρι και δημοσιεύσεις κωδικοποιημένων μηνυμάτων στις εφημερίδες, ζητώντας τη βοήθεια των αναγνωστών.

2.3 Η κρυπτογραφία τον 20ο αιώνα

Αν και η κρυπτογραφία χρησιμοποιήθηκε κατά τον 1ο Παγκόσμιο Πόλεμο, δύο από τις πιο αξιοπρόσεκτες μηχανές εμφανίστηκαν κατά τον 2ο Παγκόσμιο Πόλεμο: οι Γερμανοί χρησιμοποίησαν την Enigma machine που αναπτύχθηκε από τον Arthur Scherbius και οι Γιαπωνέζοι την Purple Machine που αναπτύχθηκε χρησιμοποιώντας τεχνικές που ανακαλύφτηκαν από τον Herbert O. Yardley.

Από όλες τις ιστορικές προσωπικότητες που συνέβαλαν στην ανάπτυξη της κρυπτογραφίας ο William Frederick Friedman, ιδρυτής των Riverbank Laboratories, κρυπτολόγος της Αμερικανικής κυβέρνησης και οδηγός του σπασίματος του κώδικα της Ιαπωνικής Purple Machine κατά τον 2ο Παγκόσμιο Πόλεμο, θεωρείται ο πατέρας της Αμερικάνικης κρυπτανάλυσης. Το 1918 έγραψε το βιβλίο «The Index of Coincidence and Its Applications in Cryptography» που ακόμα θεωρείται από αρκετούς σαν το σημαντικότερο σύγγραμμα πάνω στην κρυπτογραφία κατά τον 20ο αιώνα.

Κατά το τέλος της δεκαετίας του 1920 και τις αρχές της δεκαετίας του 1930 το FBI ίδρυσε ένα γραφείο με στόχο την αντιμετώπιση της χρήσης της κρυπτογραφίας από τους εγκληματίες. Το πρόβλημα της εποχής ήταν η

λαθραία εμπορία οινοπνευματωδών ποτών και σύμφωνα με μια αναφορά η πολυπλοκότητα της κρυπτογραφίας που χρησιμοποιούσαν οι λαθρέμποροι ήταν πιο πολύπλοκη από κάθε άλλη που είχε χρησιμοποιηθεί, ακόμα και από κυβερνήσεις ή κατά τη διάρκεια του 1ου Παγκοσμίου Πολέμου.

Τη δεκαετία του 1970 ο Dr. Horst Feistel δημιούργησε τον πρόγονο του σημερινού Data Encryption Standard (DES) με την οικογένεια ciphers, που ονομάστηκε 'Feistel ciphers', δουλεύοντας στο Watson Research Laboratory της IBM. Το 1976 η National Security Agency (NSA) σε συνεργασία με τον Feistel δημιούργησε τον αλγόριθμο FIPS PUB-46, γνωστό σήμερα σαν DES. Σήμερα, η εξέλιξή του σε triple-DES είναι το πρότυπο ασφαλείας που χρησιμοποιείται από τους οικονομικούς οργανισμούς των Ηνωμένων Πολιτειών. Επίσης το 1976 δύο συνεργάτες του Feistel, ο Whitfield Diffie και ο Martin Hellman, εισήγαγαν για πρώτη φορά την ιδέα της κρυπτογραφίας δημοσίου κλειδιού στο άρθρο "New Directions in Cryptography". Η κρυπτογραφία δημοσίου κλειδιού είναι αυτό που χρησιμοποιεί το ευρέως χρησιμοποιούμενο σήμερα PGP.

Το Σεπτέμβριο του 1977 σε άρθρο του περιοδικού «The Scientific American», οι Ronald L. Rivest, Adi Shamir και Leonard M. Adleman εισήγαγαν τον αλγόριθμο RSA για την κρυπτογραφία δημοσίου κλειδιού και τις ψηφιακές υπογραφές. Οι συγγραφείς προσφέρθηκαν να στείλουν τον αλγόριθμο σε όποιον τους έστελνε ένα φάκελο με πληρωμένα τα ταχυδρομικά έξοδα και η διεθνής ανταπόκριση ήταν τεράστια. Παρόλο που αυτό δεν άρεσε στην NSA τελικά ο αλγόριθμος δημοσιεύτηκε τον επόμενο χρόνο στην έκδοση The Communications της ACM.

Στα μέσα της δεκαετίας του 1980 ο αλγόριθμος ROT13 χρησιμοποιήθηκε από χρήστες του USENET "για να μη βλέπουν τα μηνύματά με επιλήψιμο περιεχόμενο αθώα μάτια" και λίγο αργότερα το 1990 μια ανακάλυψη από τους Xuejia Lai και James Massey οδήγησε σε ένα δυνατότερο, 128-bit key

cipher με σκοπό να αντικαταστήσει το γερασμένο DES standard. Ο αλγόριθμος IDEA (International Data Encryption Algorithm) που σχεδιάστηκε από αυτούς είχε σκοπό να είναι πιο αποδοτικός με γενικής χρήσης υπολογιστές όπως αυτούς που χρησιμοποιούνται στις επιχειρήσεις και στα νοικοκυριά.

Το FBI ανησυχώντας από την εξάπλωση της κρυπτογραφίας ανανέωσε την προσπάθειά του να έχει πρόσβαση στα μηνύματα κειμένου των Αμερικανών πολιτών. Σε απάντηση ο Phil Zimmerman εξέδωσε την πρώτη έκδοση του Pretty Good Privacy (PGP) το 1991 σαν ένα προϊόν ελεύθερα διαθέσιμο, που χρησιμοποιεί τον αλγόριθμο IDEA. Το PGP, ένα δωρεάν πρόγραμμα του παρέχει στρατιωτικού επιπέδου αλγορίθμους ασφαλείας στην κοινότητα του Internet, έχει εξελιχθεί σε πρότυπο κρυπτογραφίας λόγω της ευρείας διάδοσής του.

Τελευταία, το 1994, ο καθηγητής Ron Rivest, που βοήθησε στην ανάπτυξη του RSA, δημοσίευσε ένα νέο αλγόριθμο, το RC5.

2.4 Μηχανικοί αλγόριθμοι κρυπτογράφησης

Μια ξεχωριστή κατηγορία στο χώρο της κρυπτογραφίας αποτελούν οι συσκευές που χρησιμοποιούσαν κάποιο μηχανικό τρόπο για την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων. Παρακάτω αναφέρουμε μερικούς από αυτούς.

Jefferson cylinder: αναπτύχθηκε το 1790 και αποτελούνταν από 36 δίσκους. Ο κάθε δίσκος είχε ένα τυχαίο αλφάβητο και η σειρά των δίσκων ήταν το κλειδί αποκρυπτογράφησης.

Wheatstone disc: ανακαλύφτηκε από τον Wadsworth το 1817 και αναπτύχθηκε από τον Wheatstone το 1860. Αποτελούνταν από δύο τροχούς που χρησιμοποιούνταν για τη δημιουργία ενός πολυαλφαβητικού αλγορίθμου.

Hagelin machine: μια πραγματικά πρωτοποριακή μηχανή.

Enigma Rotor machine: μια από τις πολύ σημαντικές κατηγορίες μηχανών κρυπτογράφησης. Χρησιμοποιήθηκε πολύ κατά τον 2ο Παγκόσμιο Πόλεμο. Αποτελούνταν από μια σειρά περιστρεφόμενους τροχούς με εσωτερικές διασυνδέσεις που παρείχαν την αντικατάσταση χρησιμοποιώντας ένα αλφάβητο που συνεχώς άλλαζε. Ήταν βασισμένη σε ένα σχέδιο που αναπτύχθηκε από τον Arthur Scherbius το 1910. Αποτελείται από τρία μέρη που συνδέονταν με σύρματα. Ένα πληκτρολόγιο εισόδου, τη μονάδα κρυπτογράφησης και ενδεικτικές λυχνίες. Η μονάδα κρυπτογράφησης περιστρεφόταν κατά μια ορισμένη γωνία κάθε φορά που ένα γράμμα κρυπτογραφούνταν. Η μηχανή που χρησιμοποιήθηκε κατά τον 2ο Παγκόσμιο Πόλεμο είχε τρεις μονάδες κρυπτογράφησης.

Η αποκρυπτογράφηση της μηχανής Enigma έγινε αφού ένας Γερμανός (ο Hans-Thilo Schmidt) έδωσε κάποια βιβλία κωδικών σε ένα Γάλλο που με τη σειρά του τα έδωσε στον Poles. Βασικές τεχνικές αναπτύχθηκαν από τη Marian Rejewski και επεκτάθηκαν από την Αγγλική αντικατασκοπία με αποτέλεσμα το σπάσιμο του κώδικα. Μετά την πρώτη αποκρυπτογράφηση του κώδικα οι Γερμανοί άλλαξαν τον κώδικα, αλλά δεύτερη διαρροή και συντονισμένες προσπάθειες οδήγησαν ξανά στο σπάσιμό του.

2.5 Στεγανογραφία

Μια άλλη παραλλαγή της κρυπτογραφίας είναι η στεγανογραφία, η οποία έχει σαν στόχο την απόκρυψη κειμένου. Χαρακτηριστικές μέθοδοι είναι:

- Το μαρκάρισμα χαρακτήρων: Επιλεγμένα γράμματα του κειμένου ξαναγράφονται με μολύβι. Τα σημάδια αυτά δεν φαίνονται παρά μόνο αν το χαρτί κρατηθεί υπό γωνία σε δυνατό φως.
- Αόρατο μελάνι: Μπορούν να χρησιμοποιηθούν ουσίες που δεν αφήνουν ορατό ίχνος εκτός και θερμανθούν ή μετά από κάποια χημική επεξεργασία.
- Τρύπες βελόνας: Μικρές τρύπες βελόνας σε συγκεκριμένα γράμματα δεν είναι αρχικά ορατά εκτός και το χαρτί κρατηθεί μπροστά από φως.
- Ταινία διόρθωσης γραφομηχανής: Χρησιμοποιείται ανάμεσα στις γραμμές που γράφονται με μαύρη ταινία. Τα αποτελέσματα είναι ορατά μόνο κάτω από δυνατό φως.

Οι παραπάνω τεχνικές έχουν και σύγχρονα ανάλογα όπως οι μετασχηματισμοί των εικονοστοιχείων. Δυστυχώς όμως γενικά η στεγανογραφία απαιτεί πολύ περισσότερη προσπάθεια.

Ένας από τους πιο απλούς αλγορίθμους κρυπτογράφησης, που κατατάσσεται στη στεγανογραφία, είναι η ακροστιχίδα. Συνηθισμένη είναι η χρήση της σε ποιήματα της αναγέννησης. Χαρακτηριστική επίσης χρήση της είναι το "ΙΧΘΥΣ" που χρησιμοποιούνταν από τους Χριστιανούς για να αναφέρονται στο Χριστό χωρίς να γίνονται αντιληπτοί. Επίσης η χρήση ακροστιχίδων είναι και ένα από τα στοιχεία που έχουν οδηγήσει κάποιους στην αμφισβήτηση της αυθεντικότητας των έργων του Shakespeare.

3. ΚΡΥΠΤΟΓΡΑΦΙΑ

Κρυπτογραφία (cryptography) είναι η μελέτη τεχνικών που βασίζονται στα μαθηματικά προβλήματα δύσκολο να λυθούν.

Με άλλα λόγια είναι η επιστήμη που ασχολείται με τις αρχές τα μέσα και τις μεθόδους με τις οποίες μπορούμε να μετασχηματίσουμε έναν όγκο πληροφορίας σε μια μορφή μη κατανοήσιμη, και αργότερα να επαναφέρουμε την πληροφορία στην αρχική της μορφή.

Το Διαδίκτυο ήδη χρησιμοποιείται από εκατομμύρια χρήστες, και επεκτείνεται με εκθετικούς ρυθμούς αύξησης. Μπορεί να θεωρηθεί ένας χώρος επικοινωνίας, εκπαίδευσης και οικονομικής δραστηριότητας με διαρκώς αυξανόμενη δύναμη. Η νέα αυτή ψηφιακή κοινωνία οφείλει να παρέχει μηχανισμούς προστασίας του απαραβίαστου της προσωπικής ζωής των μελών της, το οποίο αποτελεί θεμελιώδες ανθρώπινο δικαίωμα.

Σε νομικό και κοινωνικό επίπεδο, τίθεται ζήτημα προστασίας του απορρήτου της ηλεκτρονικής αλληλογραφίας (e-mail), των συναλλαγών (αριθμός πιστωτικής κάρτας, τραπεζικό απόρρητο), του ιατρικού απορρήτου και γενικότερα το ζήτημα της προστασίας προσωπικών στοιχείων και δεδομένων του κάθε χρήστη του Διαδικτύου, που με διάφορους τρόπους μπορούν να συλλεχθούν από τρίτους και να χρησιμοποιηθούν για οποινδήποτε σκοπό χωρίς τη συγκατάθεσή του.

Σε ακαδημαϊκό επίπεδο, τίθεται θέμα προστασίας αποτελεσμάτων ακαδημαϊκής έρευνας, ευαίσθητων προσωπικών δεδομένων (βαθμολογία φοιτητών), ακαδημαϊκών μελετών και γενικότερα προστασίας των πνευματικών δικαιωμάτων (copyright) των μελών της ακαδημαϊκής κοινότητας.

Σε οικονομικό επίπεδο, η ασφάλεια και προστασία των εμπορικών πλέον δεδομένων, όπως η εξασφάλιση της εγκυρότητας των συναλλαγών μέσω της αποδοχής μίας ηλεκτρονικής υπογραφής και η ασφάλεια των συναλλαγών είναι κρίσιμα ζητήματα, που αποτελούν το υπόβαθρο της ψηφιακής παγκόσμιας αγοράς.

Η κρυπτογραφία εξασφαλίζει το απόρρητο των προσωπικών πληροφοριών και είναι η τεχνολογική πλευρά της λύσης στα προαναφερθέντα ζητήματα ασφάλειας.

3.1 Η κρυπτογραφία παρέχει 4 βασικές λειτουργίες (αντικειμενικοί σκοποί):

- ***Εμπιστευτικότητα*:** Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- ***Ακεραιότητα*:** Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.
- ***Μη απάρνηση*:** Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- ***Πιστοποίηση*:** Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητες τους καθώς και την αρχή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι η ταυτότητες τους δεν είναι πλαστές.

3.2 Ανάγκες και εφαρμογές κρυπτογράφησης

3.2.1 Ανάγκες κρυπτογράφησης

3.2.1.1 Εμπιστευτικότητα – Απόκρυψη προσωπικών δεδομένων

Η κρυπτογραφία από τα αρχαία χρόνια, οπότε και πρωτοχρησιμοποιήθηκε, είχε ένα κύριο στόχο, την **απόκρυψη της πληροφορίας** κάποιου κειμένου από μη επιθυμητά πρόσωπα. Αυτή η ανάγκη προέκυψε για δύο λόγους. Ο πρώτος λόγος ήταν η ανάγκη επικοινωνίας και μεταφοράς μυστικών, ιδιαίτερα σε περιόδους πολέμου. Ο δεύτερος λόγος ήταν η πρόθεση κάποιων να αποκρύψουν πληροφορίες – γνώσεις από τους υπολοίπους. Συνήθως επρόκειτο για ιερείς ή αξιωματούχους που ήθελαν να αποκρύψουν πληροφορίες ή γνώσεις από το λαό. Σήμερα η ανάγκη αυτή έχει επεκταθεί από την προστασία των απλών προσωπικών δεδομένων μέχρι την προστασία βιομηχανικών και κρατικών μυστικών.

Καθώς η κρυπτολογία αναπτύσσεται ο αριθμός των στόχων της έχει επεκταθεί, όπως και ο αριθμός των εργαλείων που είναι διαθέσιμα για την επίτευξη αυτών των στόχων. Η κρυπτολογία παρέχει τρόπους με τους οποίους μπορεί να βοηθήσει κάποιον να αναπτύξει εμπιστοσύνη κατά τις επικοινωνίες του και να τους δώσει τις επιθυμητές ιδιότητες, παρά τις προσπάθειες των κακόβουλων χρηστών για το αντίθετο.

Έτσι εκτός από την **απόκρυψη της πληροφορίας** ή αλλιώς την **ιδιωτικότητα (privacy)** η κρυπτογραφία ικανοποιεί και μια σειρά από άλλες ανάγκες, οι οποίες περιγράφονται με συντομία παρακάτω.

- **Ταυτοποίηση (authentication)**

Πρέπει να είναι δυνατό για τον παραλήπτη ενός μηνύματος να επιβεβαιώσει τον αποστολέα του και να μην μπορεί ένας εισβολέας να πάρει τη θέση

κάποιου άλλου χρήστη.

- **Απόδειξη γνησιότητας – υπογραφές** (signatures)

Ο παραλήπτης του μηνύματος μπορεί να πείσει κάποιον τρίτο ότι το μήνυμα που έλαβε προέρχεται από αυτόν που το υπογράφει και ο υπογράφων να πείσει για την ταυτότητά του.

- **Ακεραιότητα** (integrity)

Πρέπει να μπορεί ο παραλήπτης ενός μηνύματος να επιβεβαιώσει ότι το μήνυμα δεν έχει τροποποιηθεί κατά τη διαδρομή του και ένας εισβολέας να μην μπορεί να αντικαταστήσει ένα κανονικό μήνυμα με ένα πλαστό.

- **Μην δυνατότητα άρνησης** (nonrepudiation)

Ένας αποστολέας πρέπει να μην μπορεί να αρνηθεί ψευδώς ότι έστειλε κάποιο μήνυμα.

- **Μινιμαλισμός** (minimality)

Τίποτα δεν μεταδίδεται σε τρίτους εκτός από αυτό που σαφώς έχει οριστεί πως πρέπει να μεταδοθεί.

- **Ταυτόχρονη ανταλλαγή** (simultaneous exchange)

Τίποτα με αξία (π.χ. μια υπογραφή σε ένα συμβόλαιο) δεν μεταδίδεται πριν κάτι άλλο με αξία (π.χ. η υπογραφή του άλλου μέρους) δεν παραληφθεί.

- **Συντονισμός** (coordination)

Σε μια επικοινωνία με πολλά μέρη, οι συμμετέχοντες μπορούν να συντονίσουν τις δραστηριότητές τους προς ένα κοινό σκοπό ακόμα και με την παρουσία ανεπιθύμητων – εχθρικών μερών.

- **Όριο συνεργασίας** (collaboration threshold)

Σε μια επικοινωνία πολλών μερών οι επιθυμητές ιδιότητες διατηρούνται μέχρι ο αριθμός των ανεπιθύμητων – εχθρικών μερών δεν υπερβαίνει ένα συγκεκριμένο όριο.

Όλες αυτές είναι βασικές απαιτήσεις για κοινωνικές αλληλεπιδράσεις μέσω των υπολογιστών, που είναι ανάλογες αυτών που ισχύουν για τις διαπροσωπικές σχέσεις.

3.2.2 Εργαλεία κρυπτογραφίας

Σε υψηλό επίπεδο, τα εργαλεία που είναι διαθέσιμα για την επίτευξη αυτών των στόχων περιλαμβάνουν:

- Τυχαιότητα (randomness). Κάθε μέρος μπορεί να χρησιμοποιεί μία φυσική πηγή τυχαιότητας (όπως μια δίοδο θορύβου) για την παραγωγή "πραγματικά τυχαίων" bits με σκοπό τη δημιουργία των μυστικών του κλειδιών ή την εκτέλεση τυχαίων υπολογισμών.
- Φυσική προστασία (physical protection). Κάθε μέρος πρέπει φυσικά να προστατεύει τα μυστικά του από τους εχθρούς του. Το πιο σημαντικό του μυστικό είναι συνήθως το κλειδί που έχει τυχαία δημιουργήσει και του προσφέρει μοναδικές δυνατότητες. Αντίθετα σχεδιαστικές πληροφορίες όπως σχέδια του εξοπλισμού ή λεπτομέρειες για τον αλγόριθμο κρυπτογράφησης συνήθως θεωρούνται μη προστατεύσιμες και δεν απαιτείται μυστικότητα γι αυτές.
- Ιδιότητες καναλιού (channel properties). Ασυνήθιστες ιδιότητες του καναλιού επικοινωνίας μπορεί κάποιες φορές να γίνουν στοιχείο εκμετάλλευσης.
- Πληροφοριακή θεωρία (information theory). Κάποια συστήματα, όπως τα

one-time pads, είναι ασφαλή με μια θεωρητική έννοια, δηλαδή: ο εχθρός δεν έχει ποτέ αρκετή πληροφορία για να σπάσει τον κώδικα και όση υπολογιστική ισχύ και να διαθέτει δεν μπορεί να ξεπεράσει αυτή τη δυσκολία.

- Θεωρία υπολογιστικής πολυπλοκότητας (computational complexity theory). Η εργασία του εχθρού είναι αδύνατη υπολογιστικά, αλλά όχι θεωρητικά. Τα μοντέρνα συστήματα κρυπτογραφίας χρησιμοποιούν αυτό τον τρόπο προστασίας, ο οποίος μπορεί να αντιμετωπιστεί είτε με πάρα πολύ τύχη είτε με απίστευτα μεγάλες ποσότητες υπολογισμών.
- Κρυπτογραφικοί τελεστές (cryptographic operators). Οι υπολογιστικές αντιστοιχήσεις – όπως συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης, συναρτήσεις μιας κατεύθυνσης και γεννήτριες ψευδοτυχαίων ακολουθιών – είναι τα δομικά στοιχεία για την κατασκευή ενός κρυπτογραφικού συστήματος. Αυτές δεν χρειάζεται πάντα να είναι συναρτήσεις, αφού μπορεί να χρησιμοποιηθεί και η τυχαιοποίηση ώστε διαφορετικοί υπολογισμοί να έχουν διαφορετικά αποτελέσματα. Σύνθετοι τελεστές μπορούν να δημιουργηθούν με σύνθεση από απλούστερους.
- Πρωτόκολλα κρυπτογραφίας (cryptographic protocols). Ένα πρωτόκολλο ορίζει πώς κάθε μέρος εκκινεί και απαντά σε μηνύματα, συμπεριλαμβανομένων και λανθασμένων ή παρανόμων μηνυμάτων. Το πρωτόκολλο επίσης μπορεί να ορίζει τις απαιτήσεις αρχικοποίησης, όπως τη δημιουργία ενός καταλόγου για δημόσια κλειδιά. Κάποιο μέρος ακολουθώντας το πρωτόκολλο θα είναι προστατευμένο από συγκεκριμένους κινδύνους, ακόμα και αν τα άλλα μέρη δεν ακολουθούν το πρωτόκολλο.

Ο σχεδιασμός των πρωτοκόλλων και των τελεστών είναι ανεξάρτητος, με την έννοια ότι η υλοποίηση ενός αόριστου τύπου μπορεί να είναι ανεξάρτητη

από τη χρήση του. Ο σχεδιαστής του πρωτοκόλλου δημιουργεί πρωτόκολλα υποθέτοντας την ύπαρξη τελεστών με συγκεκριμένες ιδιότητες ασφαλείας. Ο σχεδιαστής των τελεστών προτείνει υλοποιήσεις αυτών των τελεστών και προσπαθεί να αποδείξει ότι οι τελεστές αυτοί έχουν τις επιθυμητές ιδιότητες.

Στα επόμενα κεφάλαια θα δούμε πώς συγκεκριμένοι αλγόριθμοι βοηθούν την επίτευξη των παραπάνω στόχων.

3.2.3 Εφαρμογές της κρυπτολογίας στην ιδιωτική και κοινωνική ζωή

Αν και πολλοί μπορεί να αμφιβάλουν αν έχουν κάποια προσωπική επαφή με την κρυπτολογία, οι περισσότεροι ενήλικες εξαρτώνται από αυτή για να προστατεύσουν τα ενδιαφέροντα ή τα δικαιώματά τους σε αρκετούς τομείς. Για παράδειγμα ο Προσωπικός Αριθμός Αναγνώρισης (PIN) που πρέπει να εισαχθεί σε ένα ATM, μαζί με την αντίστοιχη κάρτα, για να αποδειχθεί ότι πράγματι ο χρήστης είναι ο ιδιοκτήτης της, μπορεί να είναι αποθηκευμένος στους υπολογιστές της τράπεζας σε κρυπτογραφημένη μορφή ή ακόμα και στην ίδια την κάρτα κρυπτογραφημένος. Ο μετασχηματισμός που χρησιμοποιείται σε αυτό το είδος της κρυπτογραφίας καλείται μίας κατεύθυνσης, εννοώντας ότι για παράδειγμα είναι εύκολο να υπολογιστεί κάποιο κρυπτογραφημένο κλειδί από το PIN του πελάτη και ένα κλειδί της τράπεζας, αλλά αδύνατο να υπολογίσει κανείς το PIN, ακόμα και αν ξέρει το κλειδί της τράπεζας. Έτσι προστατεύεται ο κάτοχος της κάρτας από το να την χρησιμοποιήσει κάποιος άλλος και να έχει πρόσβαση στα τραπεζικά του στοιχεία. Παρόμοια η επικοινωνία ανάμεσα στο ATM και τα κεντρικά συστήματα της τράπεζας είναι κρυπτογραφημένη για να αποτρέψει κάποιον φιλόδοξο κλέφτη από το να υποκλέψει τα σήματα από την τηλεφωνική γραμμή και να τα χρησιμοποιήσει για να πραγματοποιήσει παράνομες αναλήψεις.

Ένα άλλο παράδειγμα είναι ο τρόπος που χρησιμοποιείται για να αποτραπούν οι πλαστογράφοι από το να κατασκευάσουν κουπόνια για τυχερά παιχνίδια, με τον αριθμό που κερδίζει. Αντίθετα με τα χαρτονομίσματα, όπου χρησιμοποιείται συνήθως η τελευταία λέξη της τεχνολογίας σε υδατογραφήματα κ.α., τα κουπόνια αυτά τυπώνονται χωρίς κάποια ιδιαίτερη τεχνική. Το μυστικό είναι ότι πάνω τους αναγράφονται δύο αριθμοί. Ο ένας από αυτούς ανακοινώνεται όταν βρεθεί ο νικητής και ο άλλος είναι μια κρυπτογραφημένη εκδοχή του ίδιου αριθμού. Έτσι ο νικητής πρέπει να δώσει αυτό τον αριθμό, κάτι που μπορεί να κάνει ένας απατεώνας μόνο αν έχει σπάσει το σύστημα κρυπτογράφησης που χρησιμοποιείται.

Τα δύο αυτά παραδείγματα παρουσιάζουν μόνο τη χρήση του χαρακτηριστικού της ταυτοποίησης που παρέχει ένα κρυπτοσύστημα. Μια νέα εφαρμογή που περιλαμβάνει όλα τα χαρακτηριστικά της κρυπτογραφίας είναι οι έξυπνες πιστωτικές κάρτες, που έχουν ένα ενσωματωμένο μικροεπεξεργαστή. Οι κάρτες αυτές που πρωτοχρησιμοποιήθηκαν στη Γαλλία το 1984 σιγά-σιγά θα αντικαταστήσουν όλες τις παλαιότερου τύπου πιστωτικές κάρτες. Η κρυπτογραφία είναι βασική για την λειτουργία αυτών των καρτών. Ο χρήστης αποδεικνύει την ταυτότητά του με τη χρήση ενός PIN κάθε φορά που η κάρτα χρησιμοποιείται. Η κάρτα και η αντίστοιχη συσκευή ανάγνωσης εκτελούν μια σειρά από κρυπτογραφημένες συναλλαγές υπογραφής με σκοπό να επιβεβαιώσουν και τα δύο μέρη ότι ο άλλος είναι νόμιμος. Αφότου αυτό γίνει η ίδια η συναλλαγή γίνεται κρυπτογραφημένα, με σκοπό να αποτραπεί πως οποιοσδήποτε, ακόμα και ο έμπορος ή ο ιδιοκτήτης της κάρτας, θα υποκλέψει τη συναλλαγή και στη συνέχεια θα διαπράξει πλαστοπροσωπία με σκοπό να εξαπατήσει το σύστημα. Αυτό το πολύπλοκο πρωτόκολλο υλοποιείται με τρόπο διαφανή προς το χρήστη, με εξαίρεση το ότι πρέπει να εισαγάγει το PIN του.

Υπάρχουν και άλλες καινούριες περιοχές όπου η κρυπτογραφία παίζει κάποιο ρόλο στην καθημερινή μας ζωή. Στο ηλεκτρονικό ταχυδρομείο για παράδειγμα ο μόνος τρόπος να δημιουργήσουμε έναν εικονικό φάκελο είναι η κρυπτογράφηση του μηνύματος. Όσο περνά ο καιρός οι βάσεις δεδομένων που περιέχουν φορολογικά δεδομένα, στοιχεία για τις πιστωτικές κάρτες και άλλα αντίστοιχα δεδομένα γίνονται πιο ανοικτές στο κοινό, με δυνατότητες προσθήκης και ανάκτησης πληροφοριών από απόσταση, με συνέπεια να είναι αναγκαία η προστασία τους μέσω κρυπτογράφησης, για να προστατευτούν τα ατομικά δικαιώματα των πολιτών. Αναγνωρίζοντας το πρόβλημα που προκύπτει από τις υποκλοπές πληροφοριών, οι κυβερνήσεις έχουν προχωρήσει στη σύσταση επιτροπών και τη θέσπιση νομοθετικών διατάξεων με σκοπό την προστασία των πολιτών. Είναι προφανές λοιπόν ότι η ασφάλεια των πληροφοριών – που γενικά σημαίνει πληροφορίες προστατευόμενες μέσω της κρυπτογραφίας – είναι ένα από τα κυριότερα προβλήματα της μεταβιομηχανικής κοινωνίας και σαν τέτοιο επιδρά σε όλους τους τομείς της δημόσιας και ιδιωτικής ζωής.

3.3 Εφαρμογές Κρυπτογραφίας

3.3.1 Απλές Εφαρμογές της Κρυπτογραφίας

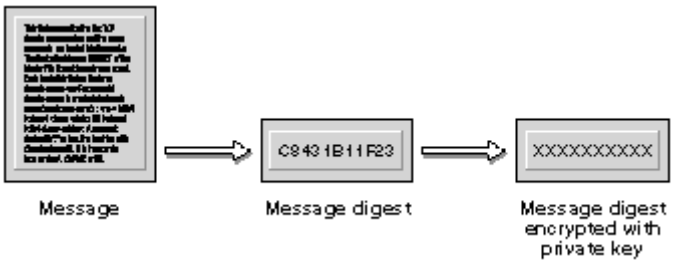
3.3.1.1 Διαφύλαξη του Απορρήτου και Κρυπτογράφηση

Η πιο φανερή εφαρμογή της κρυπτογραφίας είναι η εξασφάλιση του απορρήτου *(privacy)* μέσω της κρυπτογράφησης. Οι ευαίσθητες πληροφορίες κρυπτογραφούνται με κατάλληλο αλγόριθμο που εξαρτάται από τις ανάγκες της επικοινωνίας. Για να μπορέσει κάποιος να επαναφέρει τα κρυπτογραφημένα δεδομένα στην αρχική τους μορφή πρέπει να κατέχει το

κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση τους, εάν μιλάμε για συμμετρική κρυπτογράφηση ή την ιδιωτική κλείδα που αντιστοιχεί στην δημόσια κλείδα που το κρυπτογράφησε, εάν μιλάμε για ασύμμετρη κρυπτογράφηση.

Αξίζει να σημειώσουμε ότι υπάρχουν περιπτώσεις όπου ότι οι πληροφορίες δεν πρέπει να είναι απροσπέλαστες από όλους και γι' αυτό αποθηκεύονται με τέτοιο τρόπο ώστε η αντιστροφή της κρυπτογραφικής διαδικασίας που έχει εφαρμοστεί να είναι αδύνατη. Για παράδειγμα, σε ένα τυπικό περιβάλλον πολλών χρηστών, κανένας δεν πρέπει να έχει γνώση του αρχείου που περιέχει τους κωδικούς όλων των χρηστών. Συχνά, λοιπόν, αποθηκεύονται οι hash values των πληροφοριών (στην προηγούμενη περίπτωση θα ήταν οι κωδικοί) αντί για τις ίδιες τις πληροφορίες. Έτσι, οι χρήστες είναι σίγουροι για το απόρρητο των κωδικών τους, ενώ μπορούν να ακόμα να αποδεικνύουν την ταυτότητα τους με την παροχή του κωδικού τους. Ο υπολογιστής που έχει αποθηκευμένες τις hash values των κωδικών, σε κάθε εισαγωγή κωδικού υπολογίζει το hash του και το συγκρίνει με το αποθηκευμένο που αντιστοιχεί στον χρήστη που προσπαθεί να πιστοποιήσει τον εαυτό του.

3.3.1.2 Πιστοποίηση Ταυτότητας και Ψηφιακές Υπογραφές



Η ψηφιακή υπογραφή είναι ένα εργαλείο που παρέχει πιστοποίηση ταυτότητας *(authentication)*. Η έννοια πιστοποίηση ταυτότητας περιλαμβάνει όλες εκείνες τις διαδικασίες που είναι απαραίτητες για την επαλήθευση

συγκεκριμένων ευαίσθητων πληροφοριών, όπως την ταυτότητα του αποστολέα ενός μηνύματος, την αυθεντικότητα ενός εγγράφου, ακεραιότητα δεδομένων *(integrity)* και την ταυτότητα ενός υπολογιστή. Οι ψηφιακές υπογραφές επιτυγχάνουν την πιστοποίηση ταυτότητας, παράγοντας ένα σύνολο πληροφοριών που βασίζεται στο έγγραφο και σε ιδιωτικά στοιχεία του αποστολέα. Το σύνολο αυτό δημιουργείται μέσω μιας hash function και της ιδιωτικής κλείδας του αποστολέα.

Ας δούμε πως λειτουργεί μία ψηφιακή υπογραφή. Έστω δύο χρήστες, ο Α και ο Β. Όταν ο Α θέλει να στείλει ένα υπογεγραμμένο έγγραφο στον Β. Το πρώτο βήμα είναι η παραγωγή του message digest του μηνύματος. Το message digest είναι κατά κανόνα μικρότερο σε μέγεθος από το αρχικό μήνυμα. Στο δεύτερο βήμα, ο Α κρυπτογραφεί το message digest με την ιδιωτική του κλείδα. Τέλος, στέλνεί το κρυπτογραφημένο message digest στον Β μαζί με το έγγραφο. Για να μπορέσει ο Β να επαληθεύσει την υπογραφή πρέπει να γνωρίζει την δημόσια κλείδα του Α και τον hash function που χρησιμοποίησε ο Α. Πρώτα θα αποκρυπτογραφήσει το message digest με την δημόσια κλείδα του Α και θα πάρει το message digest που παρήγαγαι ο Α. Έπειτα, θα υπολογίσει το message digest του εγγράφου ξανά και θα το συγκρίνει με το παραληφθέν. Εάν τα δύο είναι ταυτόσημα τότε η υπογραφή επαληθεύτηκε επιτυχώς. Εάν δεν ταιριάζουν τότε ή κάποιος προσποιείται ότι είναι ο Α ή το μήνυμα τροποποιήθηκε κατά την μεταφορά του ή προέκυψε λάθος κατά την μετάδοση. Οποιοσδήποτε που γνωρίζει την δημόσια κλείδα του Α, την hash function και τον αλγόριθμο κρυπτογράφησης που χρησιμοποιήθηκε, μπορεί να επιβεβαιώσει το γεγονός ότι το μήνυμα προέρχεται από τον Α και ότι δεν αλλοιώθηκε μετά την υπογραφή του.

Για να έχει αποτέλεσμα η παραπάνω μέθοδος, πρέπει να τηρούνται δύο προϋποθέσεις: (α) η hash function πρέπει να είναι όσο το δυνατόν

περισσότερο μη αντιστρέψιμη και (β) τα ζεύγη δημόσιας – ιδιωτικής κλείδας να είναι συσχετισμένα με τους νόμιμους κατόχους τους. Για την εξασφάλιση της δεύτερης προϋπόθεσης υπάρχουν ψηφιακά έγγραφα που καλούνται πιστοποιητικά *(certificates)* και συνδέουν ένα άτομο με μία συγκεκριμένη δημόσια κλείδα.

3.3.2 Άλλες εφαρμογές κρυπτογραφίας

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη την μεταφορά της πληροφορίας για διάφορους λειτουργικούς σκοπούς

1. Ασφάλεια συναλλαγών σε τράπεζες δίκτυα - ATM
2. Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)
3. Σταθερή τηλεφωνία (cryptophones)
4. Διασφάλιση Εταιρικών πληροφοριών
5. Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
6. Διπλωματικά δίκτυα (Τηλεγραφήματα)
7. Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)
8. Ηλεκτρονική ψηφοφορία
9. Ηλεκτρονική δημοπρασία
10. Ηλεκτρονικό γραμματοκιβώτιο
11. Συστήματα συναγερμών
12. Συστήματα βιομετρικής αναγνώρισης
13. Έξυπνες κάρτες
14. Ιδιωτικά δίκτυα
15. Word Wide Web
16. Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
17. Ασύρματα δίκτυα (Hipperlan, bluetooth, 802.11x)

18. Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
19. Τηλεσυνδίασκεψη

4. ΣΥΜΜΕΤΡΙΚΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ

4.1 Κανόνες συμμετρικής κρυπτογραφίας

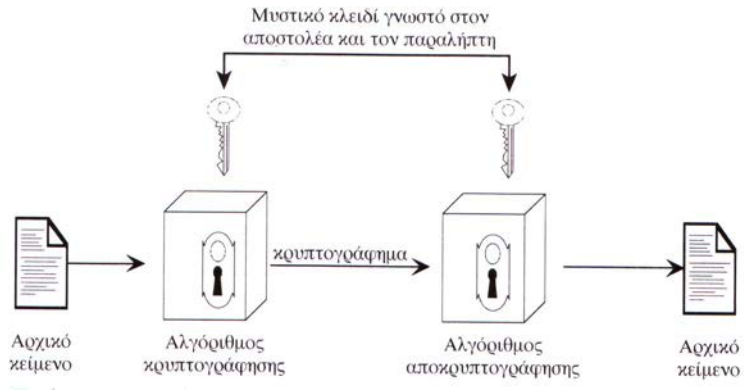
Η συμβατική κρυπτογραφία (conventional cryptography) αναφέρεται στην βιβλιογραφία και ως συμμετρική κρυπτογραφία (symmetric cryptography) ή κρυπτογραφία μυστικού κλειδιού (secret key cryptography).

Στη συμμετρική κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και κατά συνέπεια, απαιτείται κάποιο ασφαλές μέσο για τη μετάδοσή του, όπως μία προσωπική συνάντηση, κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.

Ένα σχήμα συμβατικής κρυπτογραφίας αποτελείται από πέντε επιμέρους οντότητες (σχήμα 4.1):

- Αρχικό κείμενο (plaintext): αποτελεί το αρχικό μήνυμα ή τα αρχικά δεδομένα που εισάγονται στον αλγόριθμο κρυπτογράφησης.
- Αλγόριθμος κρυπτογράφησης (encryption algorithm) πραγματοποιεί τους απαραίτητους μετασχηματισμούς του αρχικού κειμένου για την επίτευξη κρυπτογράφησης ενός μηνύματος.
- Μυστικό κλειδί (secret key): αποτελεί το μυστικό κλειδί, το οποίο εισάγεται επίσης στον αλγόριθμο κρυπτογράφησης. Οι ακριβείς αντικαταστάσεις και τα αποτελέσματα των μετασχηματισμών που επιτελούνται από τον αλγόριθμο εξαρτώνται από αυτό το μυστικό κλειδί.

- Κρυπτογράφημα ή κρυπτογραφημένο μήνυμα (ciphetext): είναι το μετασχηματισμένο μήνυμα που παράγεται ως έξοδος από τον αλγόριθμο κρυπτογράφησης. Το κρυπτογράφημα αυτό εξαρτάται τόσο σπό το αρχικό μήνυμα όσο και από το μυστικό κλειδί, συνεπώς δοθέντος ενός μηνύματος διαφορετικά κλειδιά παράγουν διαφορετικά κρυπτογραφήματα.
- Αλγόριθμος αποκρυπτογράφησης (decryption algorithm): πρόκειται για έναν αλγόριθμο που πραγματοποιεί την αντίστροφη διαδικασία, δηλαδή λαμβάνει το κρυπτογράφημα και το ίδιο μυστικό κλειδί που χρησιμοποιήθηκε στη διαδικασία της κρυπτογράφησης και παράγει το αρχικό κείμενο.



Σχήμα 4.1 Απλοποιημένο μοντέλο συμβατικής κρυπτογραφίας

Για την ασφαλή χρήση της συμβατικής κρυπτογραφίας πρέπει να πληρούνται οι ακόλουθες προϋποθέσεις:

- Απαιτείται η ύπαρξη ενός ισχυρού (strong) αλγόριθμου κρυπτογράφησης. Ως ελάχιστη απαίτηση αναφέρεται η ύπαρξη

αλγορίθμου για τον οποίο κι εάν αυτός είναι γνωστός στο δυνητικό επιτιθέμενο και υπάρχει πρόσβαση σε ένα ή περισσότερα κρυπτογραφήματα, αυτός δε δύναται ούτε να υπολογίσει το μυστικό κλειδί, ούτε να συμπεράνει το αρχικό κείμενο, δηλαδή δε δύναται να κρυπταναλύσει το κρυπτογράφημα. Αυτή η απαίτηση δηλώνεται αυστηρότερα ως ακολούθως: ο επιτιθέμενος πρέπει να είναι αδύνατο να κρυπταναλύσει το κρυπτογράφημα ή να ανακαλύψει το κλειδί, ακόμη και αν κατέχει κάποια κρυπτογραφήματα μαζί με τα αντίστοιχα αρχικά μηνύματα, από τα οποία παράχθηκε καθένα από καθένα από αυτά τα κρυπτογραφήματα.

- Ο πομπός και ο δέκτης πρέπει να έχουν παραλάβει τα αντίγραφα του μυστικού κλειδιού με ασφαλή τρόπο και να διαφυλάσσουν αυτό το μυστικό κλειδί σε ασφαλές μέρος. Εάν κάποιος γνωρίζει τον αλγόριθμο και ανακαλύψει το κλειδί, τότε όλη η επικοινωνία που χρησιμοποιεί αυτό το κλειδί είναι αναγνώσιμη, συνεπώς παραβιάζεται η εμπιστευτικότητα.

Σημειώνεται ότι αδύναμο κρίκο στην ασφάλεια της συμβατικής κρυπτογραφίας αποτελεί μόνον η μυστικότητα του κλειδιού και όχι η μυστικότητα του αλγορίθμου που χρησιμοποιείται. Αυτό θεωρείται δεδομένο εάν υποτεθεί για τον επιλεγέντα αλγόριθμο ισχύει η προφανής σχεδιαστική απαίτηση να είναι αδύνατο να αποκρυπτογραφηθεί ένα μήνυμα μόνο με γνώση του κρυπτογραφήματος και του αλγορίθμου κρυπτογράφησης. Συνεπώς, δε χρειάζεται να παραμένει μυστικός ο αλγόριθμος, αλλά μόνο το μυστικό κλειδί. Το χαρακτηριστικό αυτό γνώρισμα της συμβατικής κρυπτογραφίας την καθιστά κατάλληλη για ευρεία χρήση. Το γεγονός ότι δε χρειάζεται να παραμένει μυστικός ο αλγόριθμος επιτρέπει στους κατασκευαστές να αναπτύσσουν χαμηλού κόστους υλοποιήσεις, τόσο σε λογισμικό όσο και σε υλικό, για εφαρμογές κρυπτογράφησης δεδομένων.

4.1.1 Κρυπτογράφηση

Εφαρμογή της κρυπτογραφίας είναι η κρυπτογράφηση η οποία έρχεται να εξασφαλίσει το απόρρητο των προσωπικών πληροφοριών. Πρόκειται για μία επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Το αρχικό μήνυμα ονομάζεται απλό κείμενο (plaintext), ενώ το ακατάλληλο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα (ciphertext).

Κρυπτογράφηση είναι ο μετασχηματισμός δεδομένων σε μορφή που να είναι αδύνατον να διαβαστεί χωρίς τη γνώση της σωστής ακολουθίας bit. Η ακολουθία bit καλείται «κλειδί» και χρησιμοποιείται σε συνδυασμό με κατάλληλο αλγόριθμο/ συνάρτηση. Η αντίστροφη διαδικασία είναι η αποκρυπτογράφηση και απαιτεί γνώση του κλειδιού. Σκοπός της κρυπτογράφησης είναι η εξασφάλιση το απόρρητο των δεδομένων κρατώντας τα κρυφά από όλους όσους έχουν πρόσβαση σε αυτά.

Η κρυπτογράφηση και η αποκρυπτογράφηση απαιτούν, όπως είπαμε, τη χρήση κάποιας μυστικής πληροφορίας, το κλειδί. Για μερικούς μηχανισμούς χρησιμοποιείται το ίδιο κλειδί και για την κρυπτογράφηση και για την αποκρυπτογράφηση, για άλλους όμως τα κλειδιά που χρησιμοποιούνται διαφέρουν.

Στις μέρες μας δεν είναι μόνο κρυπτογράφηση και αποκρυπτογράφηση. Εκτός από την διασφάλιση του απορρήτου (privacy), η πιστοποίηση

ταυτότητας (authentication) είναι άλλη μία έννοια που έχει γίνει μέρος της ζωής μας. Πιστοποιούμε την ταυτότητά μας καθημερινά και ανεπαίσθητα, για παράδειγμα όταν υπογράφουμε ένα έγγραφο, όταν δείχνουμε την ταυτότητα μας. Καθώς ο κόσμος εξελίσσεται σε ένα περιβάλλον που όλες οι αποφάσεις και οι συναλλαγές θα γίνονται ηλεκτρονικά, χρειαζόμαστε ηλεκτρονικές τεχνικές που θα επιτελούν την πιστοποίηση της ταυτότητάς μας.

Η κρυπτογραφία παρέχει μηχανισμούς για τέτοιες διαδικασίες. Η ψηφιακή υπογραφή συνδέει ένα έγγραφο με τον κάτοχο ενός κλειδιού έτσι ώστε όλοι όσοι είναι σε θέση να το αναγνώσουν να είναι σίγουρη για το ποιος το έχει γράψει. Επίσης, μία ψηφιακή χρονοσφραγίδα (digital timestamp) συνδέει ένα έγγραφο με την ώρα της δημιουργίας του. Τέτοιοι μηχανισμοί μπορούν να χρησιμοποιηθούν για έλεγχο πρόσβασης σε ένα σκληρό δίσκο, για ασφαλείς συναλλαγές μέσω του Διαδικτύου ή ακόμα και για σύνδεση με καλωδιακή τηλεόραση.

Τα κρυπτογραφικά συστήματα ταξινομούνται, γενικά, με βάση τρία ανεξάρτητα κριτήρια.

- Τον τύπο των διαδικασιών που χρησιμοποιούνται για το μετασχηματισμό του αρχικού κειμένου σε ένα κρυπτογράφημα.

  Το σύνολο των αλγορίθμων κρυπτογράφησης στηρίζεται σε δύο γενικές αρχές: στην αντικατάσταση (substitution) σύμφωνα με την οποία κάθε στοιχειό του αρχικού κειμένου, είτε είναι δυαδικό ψηφίο, είτε χαρακτήρας, είτε ομάδα δυαδικών ψηφίων ή χαρακτήρων, αντικαθίσταται από άλλο στοιχείο και στη μετάθεση (transposition) στην οποία τα στοιχεία του αρχικού κειμένου αναδιατάσσονται. Βασική προϋπόθεση αποτελεί η μη απώλεια οποιασδήποτε πληροφορίας, ώστε όλες οι διαδικασίες να είναι αντιστρέψιμες. Τα περισσότερα συστήματα που είναι

γνωστά ως συστήματα παραγωγής (product systems), περιλαμβάνουν πληθώρα σταδίων αντικαταστάσεων και μεταθέσεων.

- Τον αριθμό των κλειδιών που χρησιμοποιούνται.

Εάν ο πομπός και ο δέκτης χρησιμοποιούν το ίδιο κλειδί, τότε το σύστημα αναφέρεται ως συμμετρικό ή μοναδικού κλειδιού ή μυστικού κλειδιού ή συμβατικής κρυπτογραφίας. Εάν, όμως, ο πομπός και ο δέκτης χρησιμοποιούν διαφορετικά κλειδιά, τότε το σύστημα αναφέρεται ως ασύμμετρο, ή σύστημα ζεύγους κλειδιών, ή κρυπτογραφίας δημόσιου κλειδιού.

- Τον τρόπο με τον οποίο επεξεργάζεται το αρχικό κείμενο.

Ένας κωδικοποιητής τμημάτων (block cipher) επεξεργάζεται την είσοδο ενός τμήματος στοιχείων κάθε φορά, παράγοντας ένα τμήμα εισόδου. Αντίθετα, ένας κωδικοποιητής ροής (stream cipher) επεξεργάζεται κατά συνεχή τρόπο τα στοιχεία εισόδου και κάθε φορά παράγεται ως έξοδος ένα στοιχείο, με τη σειρά που καταφθάνουν τα δεδομένα.

4.1.2 Κρυπτανάλυση

Κρυπτανάλυση είναι η επιστήμη που ασχολείται με την ανάλυση και την διάσπαση των Κρυπτοσυστημάτων. Με άλλα λόγια η διαδικασία της προσπάθειας αποκάλυψης του αρχικού κειμένου ή του κλειδιού από μη εξουσιοδοτημένες οντότητες – δυνητικούς επιτιθέμενους, είναι γνωστη ως κρυπτανάλυση (cryptanalysis). Η στρατηγική που χρησιμοποιείται από τον κρυπταναλυτή εξαρτάται από τη φύση της κρυπτογράφησης και από τις πληροφορίες που είναι διαθέσιμες σε αυτόν.

Βασικός στόχος της είναι ανάλογα με της απαιτήσεις του αναλυτή κρυπτοσυστημάτων ή αλλιώς κρυπταναλυτή είναι να βρει το κλειδί ή το μήνυμα ή ένα ισοδύναμο αλγόριθμο που θα τον βοηθάει να προσδιορίζει το μήνυμα. Ένας κρυπταλγόριθμος λέγεται ότι έχει σπαστεί αν βρεθεί μια μέθοδος (πιθανοκρατική ή ντετερμινιστική) που μπορεί να βρει το μήνυμα ή το κλειδί με πολυπλοκότητα μικρότερη από την πολυπλοκότητα της επίθεσης ωμής βίας. Η πρώτη νύξη πάνω στην κρυπτανάλυση έγινε από ένα άραβα μαθηματικό τον 8ο αιώνα με την εργασία *Ανταμπ-αλ-κουταπ* ή αλλιώς *Εγχειρίδιο των γραμματέων*.

Πίνακας 4.1: Τύποι επιθέσεων σε κρυπτογραφημένα μηνύματα.

ΤΥΠΟΣ ΕΠΙΘΕΣΗΣ	ΣΤΟΙΧΕΙΑ ΓΝΩΣΤΑ ΣΤΟΝ ΚΡΥΠΤΑΝΑΛΥΤΗ
Επίθεση κρυπτογραφήματος (cipher text – only attack)	Αλγόριθμος κρυπτογράφησης Κρυπτογράφημα
Επίθεση γνωστού αρχικού κειμένου (known – plaintext attack)	Αλγόριθμος κρυπτογράφησης Κρυπτογράφημα Ένα ή περισσότερα ζεύγη (αρχικού κειμένου, κρυπτογραφήματος), παραγόμενα από το μυστικό κλειδί.
Επίθεση επιλεγμένου αρχικού κειμένου (chosen – ciphertext attack)	Αλγόριθμος κρυπτογράφησης Κρυπτογράφημα Αρχικό κείμενο επιλεγμένο από τον

	κρυπταναλυτή, σε συνδυασμό με το αντίστοιχο κρυπτογράφημα που παράγεται με το μυστικό κλειδί
Επίθεση επιλεγμένου κρυπτογραφήματος (chosen – ciphertext attack)	Αλγόριθμος κρυπτογράφησης Κρυπτογράφημα Επιλεγμένο από τον κρυπταναλυτή κρυπτογράφημα, μαζί με το αντίστοιχο αποκρυπτογραφημένο αρχικό κείμενο, που παράχθηκε με το μυστικό κλειδί
Επίθεση επιλεγμένου κειμένου (chosen - text attack)	Αλγόριθμος κρυπτογράφησης Κρυπτογράφημα Επιλεγμένο από τον κρυπταναλυτή μήνυμα αρχικού κειμένου, μαζί με το αντίστοιχο κρυπτογράφημα, που παράχθηκε με το μυστικό κλειδί. Επιλεγμένο από τον κρυπταναλυτή κρυπτογράφημα, μαζί με το αντίστοιχο αποκρυπτογραφημένο αρχικό κείμενο, που παράχθηκε με το μυστικό κλειδί.

Στον πίνακα 4.1 παρουσιάζονται συνοπτικά διάφοροι τύποι επιθέσεων κρυπτανάλυσης, οι οποίοι διαφοροποιούνται, μεταξύ άλλων, με βάση τη ποσότητα και το είδος της πληροφορίας που είναι γνωστή στον κρυπταναλυτή. Το πρόβλημα της κρυπτανάλυσης παρουσιάζει σημαντικές δυσκολίες όταν είναι γνωστό στον επιτιθέμενο μόνον το κρυπτογράφημα. Σε μερικές περιπτώσεις δεν είναι γνωστός ούτε ο αλγόριθμος κρυπτογράφησης, αλλά στη γενική περίπτωση μπορεί να υποτεθεί ότι ο αντίπαλος γνωρίζει τον αλγόριθμο που χρησιμοποιείται.

Μία κλασική επίθεση υπό αυτές τις περιστάσεις αποτελεί η προσέγγιση της εξαντλητικής αναζήτησης κλειδιών (brute-force attack), όπου ο επιτιθέμενος δοκιμάζει διαδοχικά όλα τα στοιχεία από το πεδίο όλων των πιθανών κλειδιών. Εάν το μέγεθος του κλειδιού είναι μεγάλο, η επίθεση αυτού του είδους θεωρείται πρακτικά ατελέσφορη. Κατά συνέπεια, ένας επιτιθέμενος για να είναι αποτελεσματικός θα πρέπει να αξιοποιήσει ανάλυση του κρυπτογραφήματος εφαρμόζοντας διάφορες στατιστικές δοκιμές σε αυτό. Ο επιτιθέμενος για να χρησιμοποιήσει αυτή την προσέγγιση θα πρέπει να γνωρίζει τον τύπο του αρχικού κειμένου που χρησιμοποιείται, π.χ. ένα απλό κείμενο σε συγκεκριμένη γλώσσα, ένα εκτελέσιμο αρχείο σε περιβάλλον συγκεκριμένου λειτουργικού συστήματος, ένα αρχείο με πηγαίο κώδικα σε συγκεκριμένη γλώσσα προγραμματισμού κλπ.

Η άμυνα σε επίθεση κρυπτογραφήματος (ciphertext only attack) αποτελεί γενικά εύκολη υπόθεση, επειδή ο αντίπαλος διατηρεί μικρή ποσότητα πληροφοριών με την οποία μπορεί να ασχοληθεί. Παρόλα αυτά, σε πολλές περιπτώσεις ο κρυπταναλυτής μπορεί να διαθέτει και περισσότερες πληροφορίες. Ο κρυπταναλυτής μπορεί να έχει τη δυνατότητα να καταγράψει ένα ή περισσότερα αρχικού κειμένου, καθώς επίσης και τα αντίστοιχα κρυπτογραφήματα. Σε άλλη περίπτωση, μπορεί να γνωρίζει ότι συγκεκριμένα πρότυπα αρχικού κειμένου θα εμφανιστούν σε ένα μήνυμα. Για παράδειγμα,

ένα αρχείο postscript αρχίζει πάντοτε με το ίδιο πρότυπο, ή μπορεί να υπάρξει μία τυποποιημένη επικεφαλίδα ή ένα λογότυπο σε ένα ηλεκτρονικό μήνυμα μεταφοράς κεφαλαίων. Τα προαναφερόμενα παραδείγματα αποτελούν επιθέσεις γνωστών μηνυμάτων. Με αυτή τη γνώση ο αναλυτής μπορεί να είναι σε θέση να συμπεράνει το κλειδί, με βάση τον τρόπο που μετασχηματιστικέ το γνωστό αρχικό κείμενο.

Αντίστοιχη με την επίθεση γνωστών μηνυμάτων (known plaintext attack) είναι η επίθεση πιθανής-λέξης (probable-world attack). Εάν ο επιτιθέμενος ασχολείται με την κρυπτανάλυση κάποιου μηνύματος αγνώστου περιεχομένου μπορεί να μην κατανοεί επακριβώς το περιεχόμενο του μηνύματος. Παρόλα αυτά, εάν ο επιτιθέμενος αναζητά συγκεκριμένες πληροφορίες, τότε κάποια τμήματα του μηνύματος μπορούν να θεωρηθούν γνωστά. Για παράδειγμα, εάν διαβιβάζεται ολόκληρο λογιστικό αρχείο, ο επιτιθέμενος μπορεί να είναι σε θέση να γνωρίζει τη θέση κάποιων λέξεων- κλειδιών στην επικεφαλίδα του αρχείου. Άλλο παράδειγμα αποτελεί ο πηγαίος κώδικας ενός προγράμματος που αναπτύχθηκε από κάποια εταιρεία και ο οποίος μπορεί να περιλαμβάνει δήλωση πνευματικών δικαιωμάτων σε κάποια συγκεκριμένη θέση.

Εάν ο κρυπταναλυτής μπορεί με κάποιο τρόπο να παραπλανήσει το πηγαίο σύστημα ώστε να παρεμβάλλει ένα μήνυμα που έχει επιλέξει ο ίδιος, τότε είναι πιθανή μία επίθεση επιλεγμένων μηνυμάτων. Γενικά εάν ο κρυπταναλυτής είναι σε θέση να επιλέγει τα μηνύματα για κρυπτογράφηση τότε μπορεί σκόπιμα να επιλέγει πρότυπα που αναμένεται να τον υποβοηθήσουν στην αποκάλυψη της δομής του κλειδιού.

Στον πίνακα 4.1 εμφανίζονται και άλλοι δύο τύποι επίθεσης, η επίθεση επιλεγμένου κρυπτογραφήματος (chosen ciphertext attack)και η επίθεση επιλεγμένου κειμένου (chosen text attack), επιθέσεις οι οποίες δεν επιχειρούνται συχνά ως τεχνικές κρυπτανάλυσης, μπορούν όμως να αποτελέσουν δυνητικούς τρόπους επίθεσης.

Ένα σχήμα κρυπτογράφησης θεωρείται υπολογιστικά ασφαλές (computationally secure) εφόσον το κρυπτογράφημα που παράγεται πληροί ένα τουλάχιστον από τα ακόλουθα κριτήρια:

- Το κόστος της παραβίασης του κρυπτομηνύματος να υπερβαίνει την αξία των τελικά λαμβανόμενων πληροφοριών από τη διαδικασία της κρυπτανάλυσης.
- Ο χρόνος που απαιτείται για τη διάσπαση του κρυτομηνύματος πρέπει να υπερβαίνει την ωφέλιμη διάρκεια ζωής των λαμβανόμενων πληροφοριών.

Ο υπολογισμός της απαιτούμενης προσπάθειας για την επιτυχή κρυπτανάλυση ενός κρυπτογραφήματος θεωρείται ιδιαίτερα δύσκολη διαδικασία. Παρόλα αυτά, θεωρώντας ότι δεν υπάρχει μαθηματική σχεδιαστική αδυναμία στον αλγόριθμο κρυπτογράφησης, προτείνεται η προσέγγιση της εξαντλητικής αναζήτησης κλειδιών και είναι δυνατόν να πραγματοποιηθούν κάποιες ρεαλιστικές εκτιμήσεις εφόσον αφορά το κόστος και τον απαιτούμενο χρόνο. Η εξαντλητική αναζήτηση περιλαμβάνει την εξαντλητική (exhaustive) δοκιμή κάθε πιθανού κλειδιού μέχρις ότου υπάρξει μία κατανοητή απόδοση του κρυπτογραφήματος στο αρχικό κείμενο. Στατιστικά πρέπει να δοκιμαστούν τα μισά κλειδιά – στοιχεία από το πεδίο των πιθανών κλειδιών ώστε να επιτευχθεί κρυπτανάλυση. Στον πίνακα 2.2 καταγράφεται ο χρόνος που αντιστοιχεί σε διαφορετικά μεγέθη κλειδιών. Το μέγεθος του κλειδιού των 56-bit χρησιμοποιείται στον αλγόριθμο DES (Data Encryption Standard). Στα αποτελέσματα που εμφανίζονται για κάθε μέγεθος κλειδιού, θεωρήθηκε ότι χρειάζεται χρόνος 1μs για να εκτελεστεί μία μόνο αποκρυπτογράφηση, χρόνος ο οποίος αντιστοιχεί σε μία λογική τάξη μεγέθους ισχύος των σημερινών επεξεργαστών. Με μαζική χρήση παράλληλων μικροεπεξεργαστών είναι δυνατό να επιτευχθούν ρυθμοί επεξεργασίας οι οποίοι είναι κατά πολλές τάξεις μεγέθους μεγαλύτεροι. Παράλληλα, η αξιοποίηση κβαντικών υπολογιστών (quantum computers) στην

κατεύθυνση της επέκτασης των παράλληλων υπολογισμών με αξιοποίηση του φαινομένου της κβαντικής επαλληλίας (quantum superposition), μπορεί θεωρητικά να απειλήσει τη ρωμαλεότητα των σύγχρονων κρυπτογραφικών συστημάτων, αλλά αυτό με τη σειρά του θα μπορούσε, απλώς, να οδηγήσει σε απαίτηση για διπλασιασμό του μεγέθους των κρυπτογραφικών κλειδιών. Στον πίνακα 4.2 παρατίθενται τα αποτελέσματα για ένα σύστημα που μπορεί να επεξεργαστεί 10^6 κλειδιά ανά μs. Με τη συγκεκριμένη απόδοση ο αλγόριθμος Data Encryption Standard – DES ουσιαστικά δεν μπορεί να θεωρηθεί υπολογιστικά ασφαλής.

4.1.2.1 Ταξινόμηση Μοντέλων αξιολόγησης ασφάλειας

Υπάρχουν 4 βασικά μοντέλα για την αξιολόγηση των αλγορίθμων: 1) Ασφάλεια άνευ όρων, 2) υπολογιστική ασφάλεια, 3) θεωρία πολυπλοκότητας και 4) αποδείξιμη ασφάλεια.

- Ασφάλεια άνευ όρων (Τέλεια Ασφάλεια)

Αυτή η μέτρηση εστιάζεται στην διάκριση αν ένα κρυπτοσύστημα έχει ασφάλεια άνευ όρων. Η βασική υπόθεση είναι ότι όσο και αν κρυπτοκείμενο και αν κατέχει ο αντίπαλος δεν υπάρχει αρκετή πληροφορία για να ανακτήσει το ανοικτό κείμενο(μοναδική λύση) όσο υπολογιστική ισχύ (άπειρη) και αν έχει στην διάθεση του. Χαρακτηριστικό παράδειγμα το σημειωματάριο μίας χρήσης (one time pad).

- Υπολογιστική ασφάλεια (Πρακτική Ασφάλεια)

Αυτή η μέτρηση εστιάζεται στην υπολογιστική προσπάθεια [παράγοντας εργασίας] που χρειάζεται για να διασπαστεί ένα κρυπτοσύστημα. Στόχος των

συγχρόνων συστημάτων να έχουν μεγάλο παράγοντα δυσκολίας ώστε να μην είναι χρονικά δυνατό να διασπαστούν με τα διαθέσιμα ή τα <μελλοντικά> μέσα.

- Ασφάλεια – θεωρία πολυπλοκότητας

Αυτή η μέτρηση εστιάζει στην ταξινόμηση της υπολογιστικής ικανότητας του αντιπάλου υπολογιστικών προβλημάτων ανάλογα με τους πόρους που απαιτούνται για την επίλυση τους. Οι πόροι αναφέρονται:

- Το μέγεθος δεδομένων που χρειάζονται σαν είσοδο στην επίθεση
- Τον υπολογιστικό χρόνο που χρειάζεται για να εκτελεστεί η επίθεση
- Το μέγεθος του χώρου αποθήκευσης που χρειάζεται για την επίθεση
- Το πλήθος των επεξεργαστών

- Αποδείξιμη ασφάλεια

Αυτή η μέτρηση εστιάζεται στην απόδειξη ισοδυναμίας του μαθηματικού μοντέλου του κρυπτοσυστήματος με κάποιο πολύ γνωστό δύσκολο στην επίλυση του πρόβλημα (θεωρίας αριθμών). Χαρακτηριστικό παράδειγμα η παραγοντοποίηση μεγάλων ακεραίων.

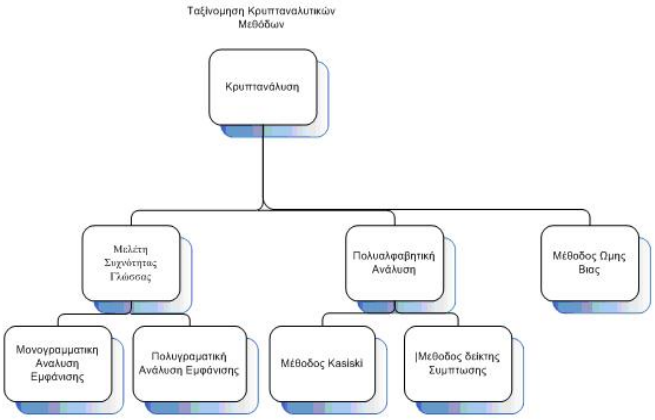
Πίνακας 4.2: Μέσος χρόνος, που απαιτείται για εξαντλητική αναζήτηση κλειδιών

Μήκος Κλειδιού (bits)	Αριθμός των πιθανών κλειδιών	Απαιτούμενος χρόνος για κρυπτανάλυση με ρυθμό δοκιμών 1 αποκρυπτογράφηση/μs	Απαιτούμενος χρόνος για κρυπτανάλυση με ρυθμό δοκιμών 10^6 αποκρυπτογραφήσεις/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs =35.8 λεπτά	2.15 ms
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs=1142 χρόνια	10 ώρες
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs=5.4 ×1024 χρόνια	5.4 × 10^{18} χρόνια

168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs=5.9 × 1036 χρόνια	5.9×10^{30} χρόνια

4.1.2.2 Κρυπτανάλυση Κλασσικών Κρυπτοσυστημάτων

Υπάρχουν διάφοροι τύποί κρυπταναλυτικών επιθέσεων για τα κλασσικά κρυπτοσυστήματα ή περισσότερες βασίστηκαν πάνω στην γλωσσική δομή του μηνύματος. Στις νεότερες μορφές Κρυπτανάλυσης Κλασσικών Κρυπτοσυστημάτων παρατηρείται ή είσοδος της στατιστικής στην ανάλυση.



- Μέθοδος Ωμής Βίας
- Ανάλυση Συχνότητας Γλώσσας
- Μέθοδος Κασισκι
- Μέθοδος Δείκτης Σύμπτωσης
- Μέθοδος Αμοιβαίου Δείκτη Σύμπτωσης

4.1.2.3 Κρυπτανάλυση Μοντέρνων Κρυπτοσυσημάτων

- Διαφορική Κρυπτανάλυση (Differential Cryptanalysis)
- Γραμμική Κρυπτανάλυση (Linear Cryptanalysis)

- Κλειδοσχεσιακή Κρυπτανάλυση (Releted Key Cryptanalysis)
- Κρυπτανάλυση Ισοτίμων (Cryptanalysis mod n)
- Κρυπτανάλυση τετραγώνου (Square Cryptanalysis)
- Στατιστική κρυπτανάλυση (Statistical Cryptanalysis)

4.1.2.4 Κρυπτανάλυση συγκεκριμένων αλγορίθμων

Κρυπτανάλυση του Diffie-Hellman

Το πρωτόκολλο Diffie-Hellman είναι ευάλωτο σε μια επίθεση παρεμβαλλόμενου προσώπου (man-in-the-middle attack). Σε αυτή την επίθεση ένας αντίπαλος η Carol, εμποδίζει την δημόσια τιμή της Alice να σταλεί στον Bob και στέλνει την δική της σ' αυτόν. Όταν ο Bob στέλνει την δική του τιμή, η Carol την αντικαθιστά με την δική της και την στέλνει στην Alice. Η Carol και η Alice συμφωνούν σε ένα μυστικό κλειδί και η Carol και ο Bob συμφωνούν σε άλλο. Μετά την ανταλλαγή αυτή η Carol μπορεί να αποκρυπτογραφήσει οποιοδήποτε μήνυμα στέλνεται από τους άλλους δύο και πιθανόν να το αλλάξει και να το επαναμεταδώσει στους αντίστοιχους παραλήπτες. Η αδυναμία του αλγορίθμου οφείλεται στο γεγονός ότι το πρωτόκολλο δεν πιστοποιεί τους συμμετέχοντες σ' αυτήν την διαδικασία. Ορισμένες πιθανές λύσεις συμπεριλαμβάνουν την χρήση ηλεκτρονικών υπογραφών και άλλων ειδών πρωτοκόλλων.

Κρυπτανάλυση του DES

Παρόλο που ο DES αναπτύχθηκε στην δεκαετία του 70, μετά από 20 χρόνια ανάλυσης του αλγορίθμου θεωρείται ακόμα ασφαλής. Η πιο πρακτική επίθεση εναντίον του είναι η brute-force, σύμφωνα μ' αυτή δοκιμάζεται η αποκρυπτογράφηση με όλα τα δυνατά κλειδιά και γίνεται έλεγχος στο πιο κατανοητό αποτέλεσμα της αποκρυπτογράφησης. Το πρόβλημα εδώ είναι το μήκος του κλειδιού. Δοθέντος αρκετού ποσού χρημάτων και χρόνου, μια

brute-force επίθεση με ένα 56 bit κλειδί μπορεί να έχει αποτελέσματα, γι' αυτό πρόσφατα έχει αναπτυχθεί μια καινούργια μορφή του DES η οποία λέγεται triple-DES ή 3DES και έχει γίνει αρκετά δημοφιλής. Με τον 3DES, ο αρχικός αλγόριθμος DES εφαρμόζεται τρεις φορές με δύο ή και τρία διαφορετικά κλειδιά. Αυτού του είδους η κρυπτογράφηση θεωρείται ότι δεν παραβιάζεται, λαμβάνοντας ακόμα υπόψη και τα υψηλού επιπέδου τεχνολογικά επιτεύγματα που υπάρχουν.

Κρυπτανάλυση του Blowfish

Μετά από μια πρόκληση με έπαθλο $1000 για το σπάσιμο του αλγορίθμου το 1995 βρέθηκαν κάποια ασθενή κλειδιά, μία επίθεση ενάντια στην έκδοση τριών κύκλων του αλγορίθμου και μια διαφορική επίθεση σε κάποιες παραλλαγές του. Παρόλα αυτά ακόμα μπορεί να θεωρείται ασφαλής και ο Schneier έχει προσκαλέσει τους κρυπταναλυτές να συνεχίσουν να ερευνούν τον αλγόριθμό του.

Κρυπτανάλυση του RSA

Η κρυπτανάλυση του αλγορίθμου RSA είναι ακόμα σε εξέλιξη. Μέχρι στιγμής έχουν βρεθεί κάποιες στατιστικές ανωμαλίες στους αλγορίθμους που χρησιμοποιούνται, οι οποίες όμως βρίσκονται ακόμα υπό μελέτη.

Μπορεί οι χρήστες του RSA να ξεμείνουν από διαφορετικούς πρώτους αριθμούς?

Υπάρχουν τόσοι πρώτοι αριθμοί που οι χρήστες του RSA δεν θα ξεμείνουν ποτέ. Το θεώρημα των πρώτων αριθμών λέει ότι οι πρώτοι αριθμοί μικρότεροι ή ίσοι του n είναι ασυμπτοτικά n/logn. Αυτό σημαίνει πως ο αριθμός των πρώτων αριθμών μήκους 512 bits ή λιγότερων είναι της τάξης του 10^{150}, που είναι μεγαλύτερος από τον αριθμό των ατόμων στο γνωστό σύμπαν. Παρόλα αυτά επειδή η εύρεσή τους δεν είναι απλή δουλειά ήδη έχουν

εμφανιστεί εταιρείες που πουλάνε πρώτους αριθμούς.

Κρυπτανάλυση του DSA

Ο αλγόριθμος DSA βασίζεται στη δυσκολία υπολογισμού του λογαρίθμου και βασίζεται σε μεθόδους που προτάθηκαν από τους Schnorr και ElGamal. Ο αλγόριθμος γενικά θεωρείται ασφαλής όταν το κλειδί είναι αρκετά μεγάλου μεγέθους. Ο DSS αρχικά προτάθηκε από το NIST με ένα κλειδί σταθερού μεγέθους 512 bits. Μετά από αρκετή κριτική ότι αυτό το μήκος κλειδιού δεν είναι αρκετά ασφαλές, ειδικά για μακροχρόνια χρήση, το NIST ανασκεύασε το DSS για να υποστηρίζει κλειδιά ως 1024 bits.

Το συγκεκριμένο πρόβλημα διακριτού αλγορίθμου που χρησιμοποιείται στο DSA είναι ο υπολογισμός διακριτών λογαρίθμων σε συγκεκριμένες υποομάδες στο πεπερασμένο πεδίο GF(p) για κάποιο πρώτο αριθμό p. Το πρόβλημα αυτό προτάθηκε για χρήση στην κρυπτογραφία το 1989 από τον Schnorr. Αν και δεν έχουν αναφερθεί επιθέσεις σε αυτού του τύπου το πρόβλημα, είναι απαραίτητη περαιτέρω ανάλυση για την πλήρη κατανόηση της δυσκολίας του προβλήματος. Κάποιοι ερευνητές έχουν προειδοποιήσει για την ύπαρξη πρώτων αριθμών που αποτελούν «τρύπα» στον DSA, και θα μπορούσαν να οδηγήσουν σε εύκολο σπάσιμο του κλειδιού. Οι αριθμοί αυτοί είναι αρκετά σπάνιοι και μπορούν να αποφευχθούν με κατάλληλες τεχνικές δημιουργίας κλειδιών.

Κρυπτανάλυση του PGP

Ο αλγόριθμος PGP αποτελεί το πιο ευρέως χρησιμοποιούμενο σύστημα κρυπτογραφίας. Κατά καιρούς έχουν παρουσιαστεί πολλές φήμες για την ασφάλεια του συστήματος. Αυτές ξεκινούν από την κυβέρνηση των ΗΠΑ να τοποθετεί κερκόπορτες στο πρόγραμμα, μέχρι την NSA να μπορεί με ευκολία

να σπάσει τους χρησιμοποιούμενους αλγορίθμους. Παρακάτω περιγράφονται οι τρόποι επίθεσης σε κάθε ένα από τα υποσυστήματά του.

1. **Συμμετρικός αλγόριθμος – IDEA.** Ο μόνος γνωστός τρόπος επίθεσης είναι η brute-force επίθεση.
2. **Ο μη συμμετρικός αλγόριθμος – RSA.** Υπάρχουν αρκετοί τρόποι επίθεσης στον RSA. Ονομαστικά αυτοί είναι: Brute-force επίθεση, εσωτερικές επιθέσεις, επιθέσεις επιλεγμένου κρυπτογραφημένου μηνύματος, χαμηλή κρυπτογράφηση εκθέτη, επίθεση συγχρονισμού, ανάλυση των παραγομένων λαθών κ.α.
3. **Το one-way hash – MD5.** Η κύρια μέθοδος επίθεσης είναι η Brute-force επίθεση, ενώ έχει χρησιμοποιηθεί και η διαφορική κρυπταννάλυση.
4. **Η γεννήτρια ψευδοτυχαίων αριθμών.** Γενικώς δεν υπάρχουν επιτυχημένες μέθοδοι επίθεσης.

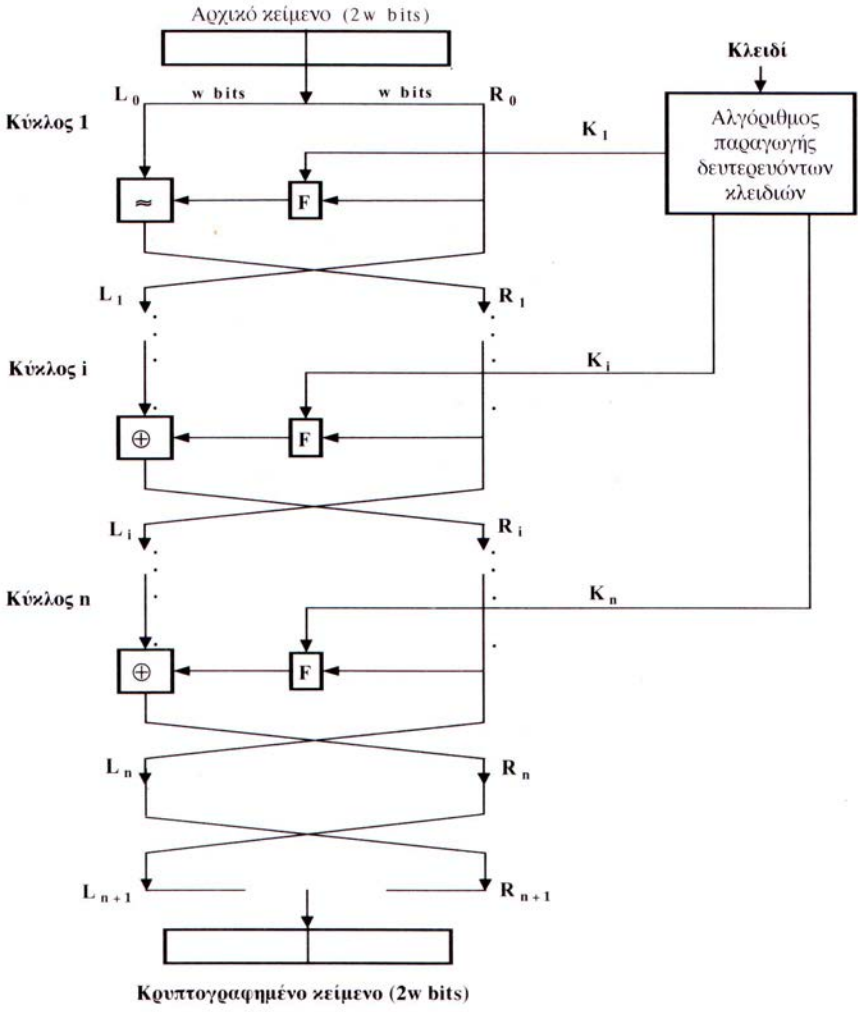
Εκτός από τις παραπάνω εξειδικευμένες επιθέσεις υπάρχουν και οι παρακάτω γενικές επιθέσεις:

1. **Παθητικές επιθέσεις (snooping).**
2. **Παρακολούθηση των πλήκτρων που πατώνται.**
3. **Van Eck Snooping.**
4. **Παρακολούθηση της μνήμης**
5. **Παρακολούθηση της προσωρινής μνήμης του δίσκου**
6. **Παρακολούθηση πακέτων**
7. **Trojan Horse**

Γενικά πάντως το PGP, παρά την μεγάλη δημοσιότητα που έχει λάβει και τις εκτεταμένες προσπάθειες επίθεσης, παραμένει ένα από τα ασφαλέστερα συστήματα επικοινωνίας σήμερα.

4.1.3 Η Δομή Κρυπτογραφίας του FEISTEL

Σχεδόν το σύνολο των συμβατικών αλγορίθμων κρυπτογραφίας τμηματων δεδομένων, συμπεριλαμβανομένου και του DES, διατηρούν μία δομή που περιγράφηκε πρώτα από τον H. Feistel της IBM το 1973. Η δομη που παρουσιάζει στο Σχήμα 4.2. Οι είσοδοι στον αλγόριθμο κρυπτογράφησης είναι ένα τμήμα αρχικού κειμένου μήκους 2 λέξεων και ένα κλειδί K. το τμήμα αρχικού κειμένου διαιρείται σε δύο ίσα τμήματα, L_0 και R_0. Τα δύο τμήματα των δεδομένων ακολουθούν n επαναληπτικά βήματα επεξεργασίας και στη συνέχεια συνδυάζονται για να παράγουν το τμήμα κρυπτογραφήματος. Κάθε κύκλος i λαμβάνει ως εισόδους τα L_{i-1} και R_{i-1} που παράγονται από τον προηγούμενο κύκλο, καθώς επίσης και ένα υποκλειδί K_i (subkey) που παράγεται από το αρχικό κλειδί K. Γενικά, τα υπολειδιά K_i είναι διαφορετικά από το K και διαφορετικα μεταξύ τους, ενώ παράγονται από το κλειδί και έναν αλγόριθμο παραγωγής υποκλειδιών.



Σχήμα 4.2 Κλασικό δίκτυο Feistel

Τα επαναληπτικά βήματα ακολουθούν την ίδια δομή: Στα δεδομένα που βρίσκονται στην αριστερή πλευρά πραγματοποιείται μία αντικατάσταση. Η αντικατάσταση επιτυγχάνεται με την εφαρμογή μιας συνάρτησης F (round function) στα δεδομένα της δεξιάς πλευράς και έπειτα συνδυάζοντας την συνάρτησης με τα δεδομένα της αριστερής πλευράς με τον τελεστή Exclusive-OR – XOR. Η συνάρτηση F έχει την ίδια γενική δομή για κάθε κύκλο, αλλά παραμετροποιείται από το υποκλειδί K_f του εκάστοτε κύκλου. Μετά από

αυτή την αντικατάσταση, εκτελείται μία αντιμετάθεση των πλευρών των δεδομένων.

Η ακριβής υλοποίηση ενός δικτύου Feistel εξαρτάται από την επιλογή των ακόλουθων παραμέτρων και χαρακτηριστικών:

- Μέγεθος των τμημάτων (block size): Όσο μεγαλύτερο είναι το μέγεθος των τμημάτων τόσο αυξάνεται ο βαθμός ασφάλειας και μειώνεται η ταχύτητα κρυπτογράφησης και αποκρυπτογράφησης. Τυπικό μέγεθος τμήματος είναι τα 64-bit και αποτελεί το συνηθέστερο στο σχεδιασμό των τμημάτων κρυπτογράφησης.
- Μέγεθος κλειδιού (key size): Όσο μεγαλύτερο είναι το μέγεθος κλειδιού τόσο εξασφαλίζεται υψηλότερος βαθμός ασφάλειας, αλλά μειώνεται η ταχύτητα κρυπτογράφησης και αποκρυπτογράφησης. Τυπικό μέγεθος κλειδιού στους σύγχρονους αλγόριθμους είναι 128 bit.
- Αριθμός κύκλων (number of rounds): Βασικό χαρακτηριστικό της δομής Feistel αποτελεί το γεγονός ότι κάθε κύκλος προσφέρει ανεπαρκή ασφάλεια, αλλά η διαδοχή των επαναληπτικών βημάτων προσφέρει αυξημένη ασφάλεια. Τυπικό μέγεθος για τον αριθμό των κύκλων είναι 16 κύκλοι.
- Αλγόριθμος παραγωγής δευτερευόντων κλειδιών (subkey generation algorithm): μεγαλύτερη πολυπλοκότητα στον αλγόριθμο πρέπει να οδηγεί σε μεγαλύτερη δυσκολία στην κρυπτανάλυση.
- Συνάρτηση κύκλου (round cycle): Μεγαλύτερη πολυπλοκότητα, σε γενικές γραμμές, σημαίνει μεγαλύτερη ρωμαλεότητα σε κρυπταναλυτικές επιθέσεις.

Επιπλέον αναφέρονται άλλες δύο παράμετροι που λαμβάνονται υπόψη κατά το σχεδιασμό μιας δομής Feistel:

- Λογισμικό ταχείας κρυπτογράφησης και αποκρυπτογράφησης (fast software encryption and decryption): Σε αρκετές περιπτώσεις η κρυπτογράφηση ενσωματώνεται με τρόπο ώστε να αποκλείεται η δυνατότητα υλοποίησης σε υλικό, κατά συνέπεια η ταχύτητα της εκτέλεσης του αλγορίθμου αποβαίνει σημαντικός παράγοντας.
- Ευκολία ανάλυσης (ease of analysis): Αν και είναι επιθυμητή η επίτευξη υψηλού βαθμού δυσκολίας κατά την κρυπτανάλυση ενός αλγορίθμου, υπάρχει σημαντικό όφελος εάν επιτευχθεί εύκολη ανάλυση του αλγορίθμου. Εάν ο αλγόριθμος μπορεί να εξηγηθεί συνοπτικά και με σαφήνεια, τότε είναι ευκολότερο να εξεταστεί για τυχόν κρυπταναλυτικά σημεία ευπάθειας και επομένως να αναπτυχθεί υψηλότερο επίπεδο ασφάλειας. Για παράδειγμα ο αλγόριθμος DES δεν έχει εύκολη προς ανάλυση λειτουργικότητα.

Η αποκρυπτογράφηση κατά Feistel είναι ουσιαστικά διαδικασία όμοια με τη διαδικασία κρυπτογράφησης και ο κανόνας που ακολουθείται είναι ο ακόλουθος: Ως είσοδοι χρησιμοποιούνται τόσο το κρυπτογράφημα όσο και τα υποκλειδιά K_i με αντίστροφη σειρά. Αναλυτικά χρησιμοποιείται το K_n στον πρώτο κύκλο, το K_{n-1} στο δεύτερο κύκλο κλπ., έως ότου χρησιμοποιηθεί το K_1 στον τελευταίο κύκλο. Το χαρακτηριστικό αυτό είναι πράγματι σημαντικό, αφού δε χρειάζεται εφαρμογή δύο διαφορετικών αλγορίθμων, ενός για την κρυπτογράφηση και ενός για την αποκρυπτογράφηση.

4.2 Συμβατικοί Αλγόριθμοι Κρυπτογραφίας

Οι ευρύτερα χρησιμοποιούμενοι συμβατικοί αλγόριθμοι κρυπτογραφίας ακολουθούν τη λογική της κρυπτογράφησης τμημάτων και αποκαλούνται κωδικοποιητές τμημάτων (block ciphers): η κρυπτογράφηση τμημάτων

επεξεργάζεται την είσοδο του αρχικού κειμένου σε σταθερού μεγέθους τμήματα και παράγει κρυπτογραφήματα ίδιου μεγέθους για οποιοδήποτε τμήμα αρχικού κειμένου. Οι πιο σημαντικοί συμβατικοί αλγόριθμοι, που ακολουθούν τη λογική της κρυπτογράφησης τμημάτων, έχουν οδηγήσει στην ανάπτυξη του DES και του Triple DES ή 3DES. Ακολούθως επεξηγούνται οι αλγόριθμοι αυτοί και ο αλγόριθμός AES (Advanced Encryption Standard), ενώ παρουσιάζεται και μία συνοπτική επισκόπηση άλλων δημοφιλών συμβατικών αλγορίθμων κρυπτογράφησης.

4.2.1 Data Encryption Standard

Το σχήμα κρυπτογράφησης που έχει χρησιμοποιηθεί ευρύτατα είναι το Data Encryption Standard – DES, που σχεδιάστηκε από την IBM και υιοθετήθηκε το 1977 από το National Institute of Standards and Technology – NIST, USA, ως Federal Information Processing Standard 46 – FIPS PUB 46. Ο αλγόριθμος που έχει υλοποιηθεί στο σύστημα DES αναφέρεται ως Data Encryption Algorithm – DEA.

- Περιγραφή του Αλγορίθμου

Η γενική δομή της κρυπτογράφησης DES παρουσιάζεται στο σχήμα 4.3. Το αρχικό κείμενο είναι μεγέθους 64-bit και το κλειδί έχει μήκος 56-bit. Τα απλά κείμενα μεγαλύτερου μεγέθους επεξεργάζονται σε τμήματα των 64-bit.

Η αριστερή πλευρά στο Σχήμα 4.3 παρουσιάζει τα τρία στάδια της επεξεργασίας του αρχικού κειμένου. Στην αρχή, το κείμενο των 64-bit ακολουθεί έναν αρχικό μετασχηματισμό (initial permutation – IP) στα πλαίσια του οποίου τα bits αναδιατάσσονται για να παραχθεί η μετασχηματισμένη είσοδος. Ακολουθεί ένα στάδιο που αποτελείται από 16 επαναλήψεις της ίδιας λειτουργίας. Η έξοδος της τελευταίας επανάληψης, δηλαδή της δέκατης

έκτης, αποτελείται από 64-bit που αποτελούν συνάρτηση του αρχικού κειμένου και του κλειδιού. Το αριστερό μισό τμήμα και το δεξί μισό τμήμα της εξόδου αντιμετατίθενται, ώστε να παραχθεί η αρχική έξοδος (preoutput). Η τιμή αυτή τροποποιείται με βάση έναν μετασχηματισμό που είναι ο αντίστροφος του αρχικού μετασχηματισμού (inverse initial permutation – IP), ώστε να παραχθεί το κρυπτογράφημα των 64-bit.

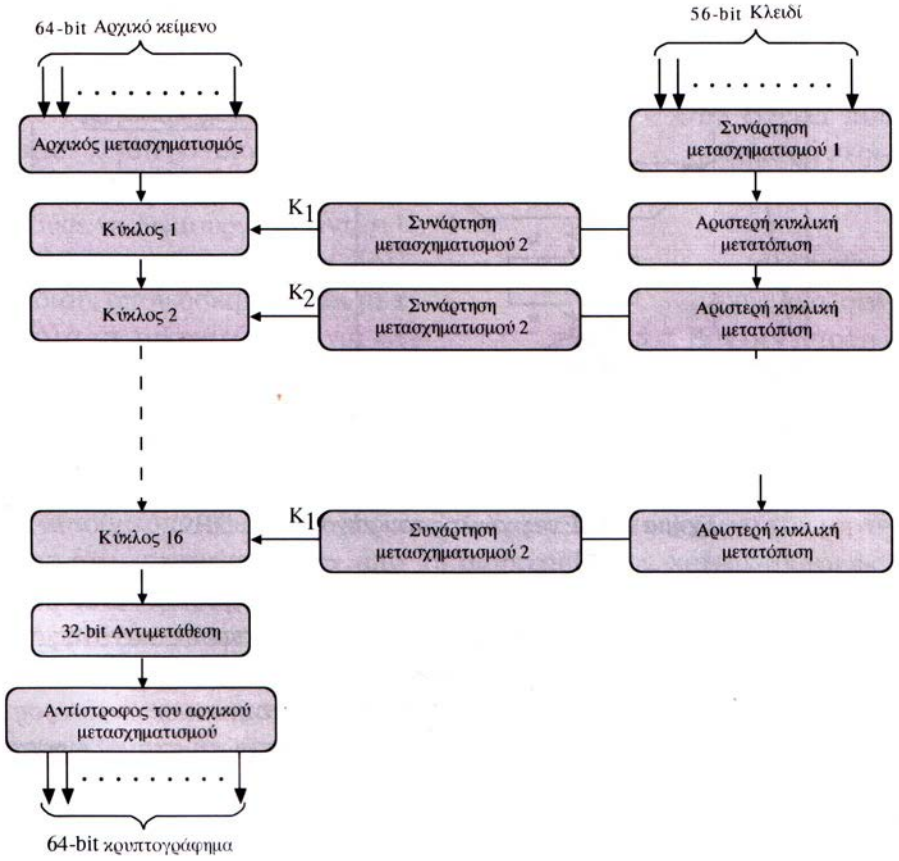
Το τμήμα της δεξιάς πλευράς του Σχήματος 4.3 παρουσιάζει τον τρόπο με τον οποίο χρησιμοποιείται το κλειδί των 56-bit. Αρχικά, το κλειδί τροποποιείται από μία συνάρτηση μετασχηματισμού. Κατόπιν, για κάθε μία από τις 16 επαναλήψεις, παράγεται ένα υποκλειδί K_i από τον συνδυασμό μιας αριστερής κυκλικής μετατόπισης και ενός μετασχηματισμού. Η συνάρτηση μετασχηματισμού παραμένει ίδια για κάθε επανάληψη, αλλά κάθε φορά παράγεται διαφορετικό υποκλειδί, λόγω της επανειλημμένης μετατόπισης των ψηφίων του κλειδιού.

Στο Σχήμα 4.4 εξετάζεται με περισσότερες λεπτομέρειες ο αλγόριθμος για μία μόνο επανάληψη. Η μετασχηματισμένη είσοδος των 64-bit συμετέχει σε 16 επαναλήψεις, παράγοντας μία ενδιάμεση τιμή των 64-bit στο τέλος κάθε επανάληψης. Το αριστερό μισό τμήμα σε συνδυασμό με το δεξί μισό τμήμα οποιασδήποτε ενδιάμεσης τιμής 64-bit αντιμετωπίζονται ως ξεχωριστές ποσότητες 32-bit, οι οποίες περιγράφονται ως L (Left – Αριστερή) και R (Right – Δεξιά). Συνοπτικά, η επεξεργασία κάθε επανάληψης μπορεί να περιγράφει με τους παρακάτω τύπους:

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

όπου το $\oplus$ συμβολίζει την πράξη XOR.

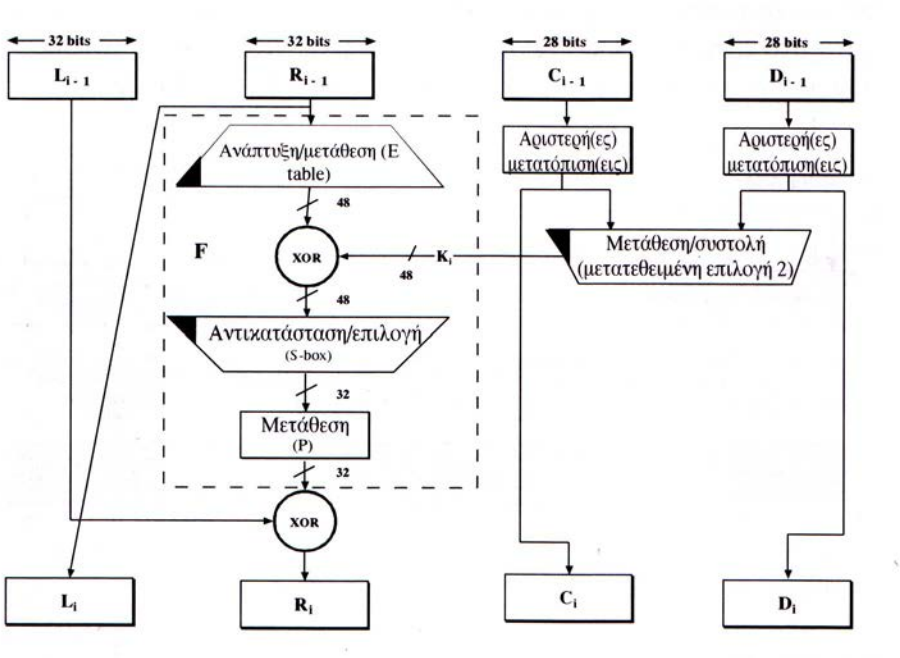
Η αριστερή έξοδος μιας επανάληψης L_i είναι ίση με τη δεξιά είσοδο σε αυτήν την επανάληψη R_{i-1}. Η δεξιά έξοδος R_i είναι το αποτέλεσμα της εφαρμογής του XOR μεταξύ του L_{i-1} και μιας σύνθετης συνάρτησης F των R_{i-1} και K_i. Η σύνθετη συνάρτηση περιλαμβάνει διαδικασίες μετάθεσης και αντικατάστασης. Η λειτουργία αντικατάστασης, η οποία αναφέρεται στο Σχήμα 4.3 ως "S-box", απλώς απεικονίζει κάθε συνδυασμό 48 εισαγόμενων bit σε ένα συγκεκριμένο τύπο των 32-bit εξόδου.



Σχήμα 4.3 Γενική περιγραφή του αλγορίθμου κρυπτογράφησης DES

Στο σχήμα 4.3, το κλειδί των 56-bit που χρησιμοποιείται ως είσοδος στον αλγόριθμο τροποποιείται με μία μετάθεση. Το προκύπτον κλειδί των 56-bit

αντιμετωπίζεται στη συνέχεια ως δύο ποσότητες των 28-bit, αναφερόμενες ως C_0 και D_0. Σε κάθε επανάληψη, τα C και D υποβάλλονται χωριστά σε μία αριστερή κυκλική μετατόπιση, ή περιστροφή 1 ή 2 bit. Οι τιμές που έχουν υποστεί μετατοπίσεις χρησιμοποιούνται ως είσοδοι στην επόμενη επανάληψη. Επιπλέον χρησιμοποιούνται ως είσοδοι σε μία άλλη συνάρτηση μετασχηματισμού, που παράγει έξοδο 48-bit, η οποία ακολούθως λειτουργεί ως είσοδος στη συνάρτηση $F(R_{i-1}, K_1)$.



Σχήμα 4.4 Ένας κύκλος του αλγορίθμου DES

Η διαδικασία της αποκρυπτογράφησης με τον αλγόριθμο DES είναι ουσιαστικά ίδια με τη διαδικασία κρυπτογράφησης, αφού ο κανόνας που ακολουθείται είναι: το κρυπτογράφημα χρησιμοποιείται ως είσοδος στον αλγόριθμο DES, αλλά τα κλειδιά K_i τοποθετούνται σε αντίστροφη σειρά. Ουσιαστικά, το K_{16} χρησιμοποιείται στην πρώτη επανάληψη, το K_{15} στη

δεύτερη επανάληψη, κλπ., έως ότου χρησιμοποιηθεί το K_1 στη δέκατη έκτη και τελευταία επανάληψη.

4.2.2 Triple Data Encryption Standard

Το TDES ή TDEA ή συνηθέστερα 3DES προτάθηκε αρχικά από τον W. Tuchman και το 1985 προτυποποιήθηκε στο ANSI X9.17, ώστε να χρησιμοποιηθεί σε οικονομικές εφαρμογές. Το 1999, με τη δημοσίευσή του ως FIPS PUB 46-3, το DES ενσωματώθηκε ως τμήμα της προτυποποίησης κρυπτογράφησης δεδομένων DES.

Το TDES ακολούθησε τον αλγόριθμο 2DES, ο οποίος δεν αξιοποιήθηκε ευρέως αφού θεωρήθηκε ευάλωτος στις κρυπταναλυτικές επιθέσεις τύπου ενδιάμεσου (man-in-the-middle attack).

Είναι μια παραλλαγή του DES όπου το μήνυμα κρυπτογραφείται και αποκρυπτογραφείται διαδοχικά με διαφορετικά κλειδιά για την ενίσχυση του βασικού αλγόριθμου. Υπάρχουν τέσσερις διαφορετικοί τρόποι για να επιτευχθεί αυτό:

- DES-EEE3 *(Encrypt-Encrypt-Encrypt)*: πραγματοποιούνται τρεις συνεχόμενες κρυπτογραφήσεις με το τρία διαφορετικά κλειδιά.
- DES-EDE3 *(Encrypt-Decrypt-Encrypt)*: το μήνυμα διαδοχικά κρυπτογραφείται, αποκρυπτογραφείται και τέλος κρυπτογραφείται με χρήση τριών διαφορετικών κλειδιών.
- DES-EEE2: είναι η ίδια με την πρώτη διαδικασία εκτός του ότι απαιτούνται δύο διαφορετικά κλειδιά.
- DES-EDE2: είναι η ίδια με την δεύτερη διαδικασία εκτός του ότι απαιτούνται δύο κλειδιά.

Τα επιπλέον κλειδιά δημιουργούνται από το κοινό μυστικό κλειδί με κατάλληλο αλγόριθμο. Από αυτούς τους τρόπους, ο πιο ασφαλής είναι ο DES-EEE3, με την τριπλή κρυπτογράφηση και τα τρία διαφορετικά κλειδιά.

Το TDES χρησιμοποιεί τρία κλειδιά και τρεις εκτελέσεις του αλγορίθμου DES. Ο αλγόριθμος ακολουθεί τη διαδοχή: κρυπτογράφηση, αποκρυπτογράφηση, κρυπτογράφηση (EDE – encryption – decryption – encryption) (Σχήμα 4.5a):

$$C = E_{K3}[D_{K2}[E_{K1}[P]]]$$

όπου:

C = κρυπτογραφία

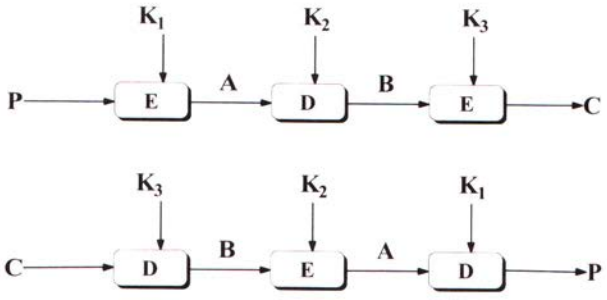
P = αρχικό κείμενο

$E_K[X]$ = κρυπτογράφηση του X με χρήση του κλειδιού K

$D_K[Y]$ = αποκρυπτογράφηση του X με χρήση του κλειδιού K.

Η αποκρυπτογράφηση ακολουθεί ακριβώς την ίδια διαδικασία με τα κλειδιά σε αντίστροφη χρήση (Σχήμα 4.5b):

$$P = D_{K1}[E_{K2}[D_{K3}[C]]]$$



Σχήμα 4.5 TDES

Αξίζει να σημειωθεί ότι η ύπαρξη της αποκρυπτογράφησης στο δεύτερο στάδιο της κρυπτογράφησης TDES δεν παρουσιάζει κάποια κρυπτογραφική χρησιμότητα, απλώς επιτρέπει στους χρήστες του TDES να αποκρυπτογραφήσουν τα στοιχεία που κρυπτογραφούνται από τους χρήστες του απλού DES:

$$C = E_{K1}[D_{K1}[E_{K1}[P]]] = E_{K1}[P]$$

Το TDES, με την υποστήριξη τριών διαφορετικών κλειδιών, διαθέτει κλειδί μήκους 168-bit. Στα πλαίσια του FIPS 46-3 επιτρέπεται, επίσης, η χρήση δύο κλειδιών K1, K2, με K1=K3. Το γεγονός αυτό εξασφαλίζει μήκος κλειδιού 112-bit. Το FIPS 46-3 περιλαμβάνει τις ακόλουθες οδηγίες για το TDES:

- Το TDES αποτελεί τον εγκεκριμένο συμβατικό αλγόριθμο κρυπτογράφησης ως FIPS.
- Το DES, που χρησιμοποιεί σημαντικό κλειδί των 56-bit, επιτρέπεται στα συστήματα διαχείρισης δικτύων για επίτευξη συμβατότητας προς τα κάτω. Τα νέα συστήματα, όμως, πρέπει να υποστηρίξουν το TDES.
- Οι κυβερνητικές οργανώσεις των ΗΠΑ που χρησιμοποιούν DES ενθαρρύνονται για τη μετάβαση σε TDES.
- Είναι αναμενόμενο ότι το TDES και το Advanced Encryption Standard – AES θα συνυπάρξουν ως FIPS εγκεκριμένοι αλγόριθμοι, μέχρι την οριστική μετάβαση στο AES.

Ο TDES αποτελεί έναν εξαιρετικό αλγόριθμο, ο οποίος επειδή προέρχεται από τον DES παρουσιάζει την ίδια ρωμαλεότητα με αυτόν σε κρυπταναλυτικές επιθέσεις. Επιπλέον, με μήκος κλειδιού 168-bit οι επιθέσεις τύπου εξαντλητικής αναζήτησης είναι πρακτικά ατελέσφορες. Συνεπώς ο TDES

αναμένεται ότι θα αξιοποιείται ολοένα και περισσότερο τα επόμενα χρόνια, μέχρι την ολοκληρωτική μετάβαση στις επερχόμενες υλοποιήσεις του AES.

4.2.3 Advanced Encryption Standard

Σύμφωνα με όσα προαναφέρθηκαν, αν η ασφάλεια αποτελούσε το μοναδικό κριτήριο επιλογής του αλγορίθμου, τότε το TDES θα ήταν μία εξαιρετικά κατάλληλη επιλογή για έναν τυποποιημένο αλγόριθμο κρυπτογράφησης για τα επόμενα χρόνια.

Όμως, κύριο μειονέκτημα του TDES αποτελεί το γεγονός ότι ο αλγόριθμος είναι σχετικά αργός σε υλοποιήσεις με χρήση λογισμικού. Το σύστημα DES σχεδιάστηκε για υλοποίηση με χρήση υλικού τη δεκαετία το '70 και δε φαίνεται να παράγει αποδοτικό κώδικα λογισμικού. Ο TDES, που περιλαμβάνει τρεις φορές περισσότερους γύρους από τον DES, είναι προφανώς πολύ βαρύτερος. Επιπλέον μειονέκτημα αποτελεί η απαίτηση των DES και TDES για χρησιμοποίηση τμημάτων μεγέθους 64-bit. Για γενικότερους λόγους αποδοτικότητας και ασφάλειας, είναι επιθυμητό μεγαλύτερο μέγεθος τμήματος. Κατά συνέπεια ο TDES δεν μπορεί να θεωρηθεί αποτελεσματικός προϊόντος του χρόνου.

Για την αντιμετώπιση των προβλημάτων αυτών, ήδη από το 1997 το NIST εξέδωσε μία πρόσκληση υποβολής προτάσεων για νέο Προηγμένο Πρότυπο Κρυπτογράφησης (Advanced Encryption Standard – AES), διάδοχο του DES και προσδιόρισε ότι το AES θα πρέπει να αποτελεί κωδικοποίηση τμημάτων με συμμετρικό σύστημα κρυπτογράφηση, μήκους τμήματος 128-bit, 192-bit και 256-bit. Τα κριτήρια συγκριτικής αξιολόγησης των υποψηφίων αλγορίθμων εντάχθηκαν σε τρεις κατηγορίες:

- Στην ασφάλεια των αλγορίθμων: τα κριτήρια που εντάσσονται σε αυτήν την κατηγορία περιλάμβαναν τη ρωμαλεότητα των αλγορίθμων σε

κρυπταναλυτικές επιθέσεις, την ορθότητα του μαθηματικού τους φορμαλισμού, τη σχετική συγκριτική ασφάλεια του αλγορίθμου σε σχέση με τους υπόλοιπους υποψήφιους αλγορίθμους και την τυχαιότητα της συμπεριφοράς της εξόδου. Σε γενικές γραμμές οι αλγόριθμοι έπρεπε να έχουν χαρακτηριστικά ασφάλειας τουλάχιστον ισοδύναμα με του αλγόριθμου TDES, αλλά να χαρακτηρίζονται ταυτόχρονα από σημαντικά βελτιωμένη αποδοτικότητα.

- Στο κόστος: τα κριτήρια που εντάσσονταν σε αυτή την κατηγορία αναφέρονταν στις απαιτήσεις μνήμης και υπολογιστικής του αλγορίθμου, καθώς και στις απαιτήσεις περί προστασίας δικαιωμάτων πνευματικής ιδιοκτησίας και πατέντες ώστε το υπό ανάπτυξη πρότυπο να μπορεί να είναι αξιοποιήσιμο σε διεθνή κλίμακα.
- Στην απλότητα: τα κριτήρια που εντάσσονται σε αυτήν την κατηγορία περιλάμβαναν την απλότητα, την ευελιξία – δηλαδή τη δυνατότητα του αλγορίθμου να χειρίζεται μεγέθη μυστικών κλειδιών και τμημάτων μη κρυπτογραφημένου κειμένου μεγαλύτερα από τα ελάχιστα τεθέντα – τη δυνατότητα υλοποίησης σε διάφορα περιβάλλοντα όπως υλικό, λογισμικό, υλικολογισμικό (firmware), καθώς και την παροχή συμπληρωματικών κρυπτογραφικών λειτουργιών.

Σε έναν πρώτο κύκλο αξιολόγησης έγιναν αποδεκτοί δέκα πέντε προτεινόμενοι αλγόριθμοι και σε δεύτερο κύκλο ο αριθμός των αποδεκτών αλγορίθμων μειώθηκε σε πέντε. Οι αλγόριθμοι αυτοί ήταν οι MARS, RC6, Rijndael, Serpent, Twofish. Τελικά επιλέχθηκε επισήμως ως AES ο αλγόριθμος Rijndael, ο οποίος είχε υποβληθεί από τους Βέλγους κρυπτογράφους J. Daemen και V. Rijmen και έλαβε την οριστική του σχεδιαστική μορφή στο τέλος του καλοκαιριού του 2001.

4.3 Λοιποί Συμμετρικοί Κωδικοποιητές Τμημάτων

4.3.1 Blowfish

Ο Blowfish είναι ένας 64-bit block cipher που αναπτύχθηκε από τον Schneier. Είναι ένας αλγόριθμος Feistel και κάθε επανάληψη αποτελείται από μια μετατροπή που εξαρτάται από το κλειδί και μια αντικατάσταση που εξαρτάται από το κλειδί και τα δεδομένα. Όλες οι λειτουργίες του βασίζονται σε πράξεις XOR και προσθέσεις λέξεων των 32-bit. Το κλειδί έχει μεταβλητό μήκος (μέγιστο 448 bits) και χρησιμοποιείται για τη δημιουργία αρκετών πινάκων υποκλειδιών. Αυτός ο αλγόριθμος σχεδιάστηκε ειδικά για μηχανές 32-bit και είναι αρκετά γρηγορότερος από τον DES.

4.3.2 International Data Encryption Algorithm (IDEA)

Ο IDEA είναι η δεύτερη έκδοση ενός block αλγόριθμου κρυπτογράφησης ο οποίος σχεδιάστηκε και παρουσιάστηκε από τους Lai και Massey. Είναι ένας 64-bit επαναληπτικός αλγόριθμος με ένα 128-bit κλειδί και 8 γύρους. Η δομή του αλγορίθμου έχει σχεδιαστεί για την εύκολη υλοποίηση τόσο στο λογισμικό όσο και στο υλικό, και η ασφάλεια του έγκειται στην χρησιμοποίηση τριών ασύμβατων τύπων αριθμητικών πράξεων πάνω σε λέξεις των 16 bit. Η ταχύτητα του IDEA είναι ίδια στο λογισμικό με αυτή του DES.

Το πιο σημαντικό κρυπταναλυτικό αποτέλεσμα οφείλεται στον Daemen. Αυτός βρήκε μια μεγάλη τάξη από 2^{51} αδύνατα κλειδιά για τα οποία η χρήση ενός από αυτά κατά την διάρκεια της κρυπτογράφησης μπορούσε να ανιχνευθεί και το κλειδί να βρεθεί. Ωστόσο, επειδή υπάρχουν 2^{128} πιθανά κλειδιά το προηγούμενο αποτέλεσμα δεν έχει επιπτώσεις στην ασφάλεια του αλγορίθμου. Ο IDEA γενικά θεωρείται ασφαλής και τόσο η ανάπτυξη του αλγορίθμου όσο και η θεωρητική του βάση έχουν ευρέως συζητηθεί.

Η πιο σπουδαία χρήση του IDEA είναι η εφαρμογή του στο δωρεάν παρεχόμενο πακέτο κρυπτογράφησης, το Pretty Good Privacy (PGP).

4.3.3 RC2, RC4, RC5

Ο RC2 είναι ένας block cipher με κλειδί μεταβλητού μήκους που σχεδιάστηκε από τον Ron Rivest για την RSA Inc. Τα αρχικά σημαίνουν "Ron's Code" ή "Rivest's Cipher". Είναι γρηγορότερος από τον DES και στόχος της σχεδίασης ήταν να λειτουργήσει για αντικατάσταση του DES. Μπορεί να γίνει περισσότερο ή λιγότερο ασφαλής από τον DES, ανάλογα με το μήκος του κλειδιού. Έχει μέγεθος block ίσο με 64 bits και είναι έως και τρεις φορές ταχύτερος από τον DES.

Ο RC4 είναι ένας stream cipher που σχεδιάστηκε πάλι από την Ron Rivest για λογαριασμό της RSA Inc. Έχει μεταβλητό μήκος κλειδιού και λειτουργεί στο επίπεδο του byte. Θεωρείται εξαιρετικά ασφαλής και οι υλοποιήσεις του σε λογισμικό τρέχουν πολύ γρήγορα. Χρησιμοποιείται για κρυπτογράφηση τοπικά αποθηκευμένων αρχείων και για την διασφάλιση της επικοινωνίας μεταξύ δύο απομακρυσμένων σημείων μέσω του πρωτοκόλλου SSL.

Ο RC5 είναι ένας γρήγορος block cipher από τον Ron Rivest για λογαριασμό της RSA Inc το 1994. Έχει πολλούς παραμέτρους: μεταβλητό μήκος κλειδιού, μεταβλητό μέγεθος block και μεταβλητό αριθμό επαναλήψεων. Τυπικές επιλογές για το μέγεθος του block είναι 32 bits (για πειραματικές εφαρμογές), 64 bits (για αντικατάσταση του DES) και 128 bits. Ο αριθμός των επαναλήψεων μπορεί να είναι από 0 έως και 255. Ο RC5 είναι πολύ απλός στην λειτουργία, πράγμα που τον κάνει εύκολο στην ανάλυση.

4.4 Διανομή Κρυπτογραφικών Κλειδιών

Για να επιτευχθεί αποτελεσματική λειτουργία στη συμβατική κρυπτογράφηση, τα δύο συμβαλλόμενα μέρη πρέπει να διαμοιράζονται τη γνώση του ίδιου μυστικού κλειδιού, το οποίο πρέπει να είναι προσπελάσιμο σε τρίτους. Επιπλέον είναι επιθυμητές οι συχνές τροποποιήσεις του κλειδιού ώστε να περιοριστούν τα δεδομένα που ενδεχομένως αποκαλυφθούν εάν κάποιος ανακαλύψει το κλειδί. Συνεπώς η ισχύς οποιουδήποτε κρυπτογραφικού συστήματος στηρίζεται στην τεχνική διανομής κλειδιών (key distribution), ένας όρος που αναφέρεται στον τρόπο μεταφοράς ενός κλειδιού μεταξύ δύο συμβαλλόμενων μερών που επιθυμούν να ανταλλάξουν δεδομένα, χωρίς να επιτρέπουν σε τρίτους να ανακαλύψουν το μυστικό αυτό κλειδί. Η διανομή κλειδιών μπορεί να επιτευχθεί με διάφορους τρόπους.

Για δύο συμβαλλόμενα μέρη Α και Β:

- Ένα κλειδί θα μπορούσε να επιλεγεί από τον Α και να παραδοθεί με φυσικό τρόπο στον Β.
- Ένας έμπιστος τρίτος θα μπορούσε να επιλέξει το κλειδί και να το παραδώσει με φυσικό τρόπο στους Α και Β.
- Εάν ο Α και ο Β έχουν χρησιμοποιήσει πρόσφατα κάποιο κλειδί που παραμένει μυστικό, θα μπορούσε ο ένας να διαβιβάσει στον άλλο το νέο κλειδί, κρυπτογραφώντας το με το παλαιό κλειδί.
- Εάν οι Α και Β διατηρούν μία κρυπτογραφημένη σύνδεση με έναν τρίτο Γ, ο Γ θα μπορούσε να παραδώσει ένα κλειδί μέσω της κρυπτογραφημένης σύνδεσης στους Α και Β.

Οι δύο πρώτοι τρόποι αναφέρονται στη λογική της μη αυτοματοποιημένης παράδοσης ενός κλειδιού. Για την κρυπτογράφηση ζεύξης αποτελεί μία λογική απαίτηση, επειδή κάθε συσκευή κρυπτογράφησης ζεύξης πρόκειται να

ανταλλάξει δεδομένα μόνο με την άλλη πλευρά της ζεύξης. Για την κρυπτογράφηση από-άκρη-σε-άκρη, όμως, η μη αυτοματοποιημένη παράδοση κρίνεται ανεπαρκής. Σε ένα κατανεμημένο σύστημα, οποιοσδήποτε σταθμός μπορεί να χρειαστεί να αρχίσει την επικοινωνία με πολλούς άλλους σταθμούς, συνεπώς κάθε συσκευή χρειάζεται έναν αριθμό κλειδιών τα οποία θα παρέχονται άμεσα και δυναμικά. Το πρόβλημα είναι ιδιαίτερα δύσκολο σε έναν ευρέως κατανεμημένο σύστημα.

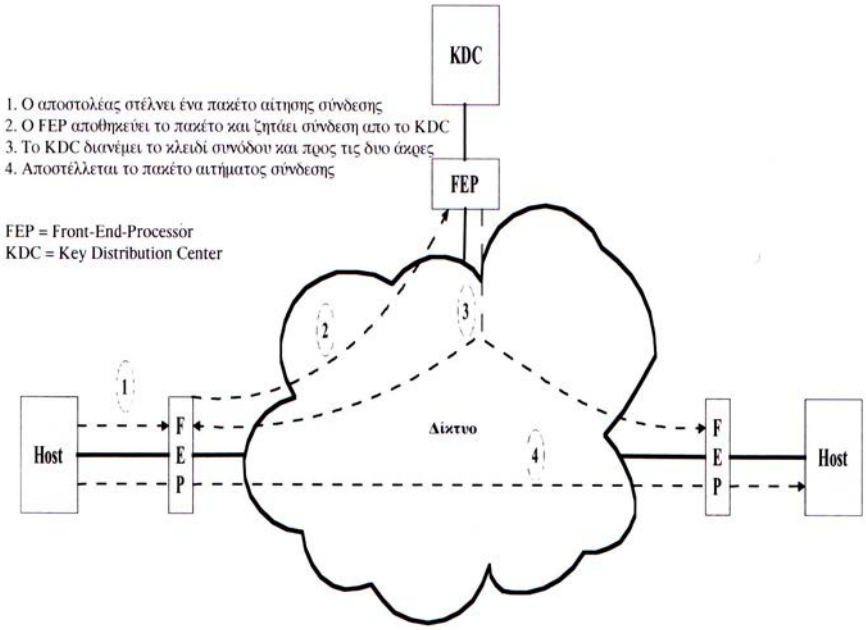
Ο τρίτος τρόπος μπορεί να πραγματοποιηθεί είτε στην κρυπτογράφηση ζεύξης, είτε στην κρυπτογράφηση από-άκρη-σε-άκρη, αλλά εάν κάποιος επιτιθέμενος καταφέρει να αποκτήσει πρόσβαση σε ένα κλειδί αποκαλύπτονται όλα τα επόμενα κλειδιά. Ακόμη και αν πραγματοποιούνται συχνές τροποποιήσεις στα κλειδιά κρυπτογράφησης ζεύξης, αυτές πρέπει να γίνουν μη αυτοματοποιημένα.

Για την παροχή κλειδιών στην κρυπτογράφηση από-άκρη-σε-άκρη ο τέταρτος τρόπος θεωρείται ως ο πλέον κατάλληλος. Στο σχήμα 2.10 (4.6) απεικονίζεται μία σχετική εφαρμογή. Στο σχήμα αυτό αγνοείται η κρυπτογράφηση ζεύξης, η οποία μπορεί να προστεθεί ή να παραληφθεί ανάλογα με τις απαιτήσεις. Για τη λειτουργία στο σχήμα 2.10, προσδιορίζονται δύο είδη κλειδιών:

- Κλειδί συνόδου (session Key): Όταν δύο συστήματα όπως σταθμοί, τερματικά κλπ. επιθυμούν να επικοινωνήσουν από-άκρη-σε-άκρη καθιερώνουν μία λογική σύνδεση. Κατά τη διάρκεια αυτής της λογικής όλα τα δεδομένα των χρηστών κρυπτογραφούνται με ένα κλειδί συνόδου μιας χρήσης. Στο τέλος της σύνδεσης το κλειδί συνόδου καταστρέφεται.
- Μόνιμο κλειδί (permanent key): μόνιμο κλειδί είναι το κλειδί που χρησιμοποιείται μεταξύ δύο οντοτήτων με σκοπό την ασφαλή διανομή κλειδιών συνόδου.

Η διαμόρφωση (configuration) συντίθεται από τα ακόλουθα στοιχεία:

- Κέντρο διανομής κλειδιού (key distribution center – KDC): Το κέντρο διανομής κλειδιών KDC προσδιορίζει τα συστήματα που επιτρέπεται να επικοινωνήσουν μεταξύ τους. Όταν χορηγηθεί η άδεια εγκατάστασης σύνδεσης σε δύο συστήματα, το KDC παρέχει ένα κλειδί συνόδου μιας χρήσης για τη συγκεκριμένη επικοινωνία.
- Μετωπικός επεξεργαστής (front-end-processor): Ένας μετωπικός επεξεργαστής επιτελεί την κρυπτογράφηση από-άκρη-σε-άκρη και λαμβάνει τα κλειδιά συνόδου λογαριασμό του σταθμού.



Σχήμα 4.6 Αυτόματη διανομή κλειδιών σε πρωτόκολλο προσανατολισμένο στη σύνδεση

Τα βήματα που περιλαμβάνονται στην εγκατάσταση μιας σύνδεσης είναι τα ακόλουθα:

Βήμα 1ο: Όταν ένας σταθμός επιθυμεί να εγκαταστήσει μία σύνδεση με έναν άλλο σταθμό, αποστέλλει ένα πακέτο αίτησης σύνδεσης (connection-request packet).

Βήμα 2ο: Ο FEP αποθηκεύει το πακέτο και αποστέλλει μία αίτηση στο KDC για την επίτευξη της σύνδεσης.

Βήμα 3ο: Η επικοινωνία μεταξύ του FEP και του KDC κρυπτογραφείται χρησιμοποιώντας ένα κύριο κλειδί, που γνωρίζουν μόνον οι FEP και KDC. Εάν το KDC εγκρίνει το αίτημα σύνδεσης δημιουργεί το κλειδί συνόδου και το παραδίδει στους δύο κατάλληλους FEP χρησιμοποιώντας ένα μοναδικό μόνιμο κλειδί για κάθε FEP.

Βήμα 4ο: Ο αιτών FEP έχει τη δυνατότητα να αποστείλει το πακέτο αιτήματος σύνδεσης και να πραγματοποιηθεί μία σύνδεση μεταξύ των δύο συστημάτων. Τα δεδομένα του χρήστη, που ανταλλάσσονται μεταξύ των δύο συστημάτων, κρυπτογραφούνται από τους αντίστοιχους FEP χρησιμοποιώντας το κλειδί συνόδου μιας χρήσης.

Η αυτοματοποιημένη διανομή κλειδιών παρέχει ιδιαίτερη ευελιξία και όλα εκείνα τα δυναμικά χαρακτηριστικά που απαιτούνται ώστε να μπορέσει ένας αριθμός χρηστών να προσπελάσει διάφορους σταθμούς εργασίας, ενώ επιτρέπεται και στους σταθμούς εργασίας να ανταλλάξουν δεδομένα μεταξύ τους.

Εναλλακτική προσέγγιση για τη διανομή κλειδιών μπορεί να επιτευχθεί με αξιοποίηση των δυνατοτήτων κρυπτογράφησης δημοσίου κλειδιού και την υιοθέτηση ψηφιακών φακέλων (digital envelopes).

5. ΑΣΥΜΜΕΤΡΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ

5.1 Αρχές Ασύμμετρων Κρυπτοσυστημάτων

Εξίσου σημαντική σπουδαιότητα με τα συμμετρικά κρυπτοσυστήματα έχει και η κρυπτογραφία δημόσιου κλειδιού (public-key encryption), η οποία αξιοποιείται κατά προτεραιότητα για αυθεντικοποίηση μηνυμάτων και διανομή μυστικών κλειδιών. Στις παραγράφους που ακολουθούν παρουσιάζονται οι

βασικές έννοιες της κρυπτογραφίας δημόσιου κλειδιού καθώς και θέματα διανομής κλειδιών. Ακολούθως εξετάζονται δύο βασικοί αλγόριθμοι δημόσιων κλειδιών: ο αλγόριθμος RSA και ο αλγόριθμος Diffie-Hellman, ενώ γίνεται βασική αναφορά σε θέματα ψηφιακών υπογραφών.

5.1.1 Δομή Κρυπτοσύστημάτων Δημόσιου Κλειδιού

Η κρυπτογράφηση δημόσιου κλειδιού (public-key encryption) προτάθηκε το 1976 από τους W. Diffie και M. Hellman και υπήρξε ένα εξόχως σημαντικό βήμα στην περαιτέρω διάδοση της κρυπτογραφίας. Οι αλγόριθμοι κρυπτογραφίας δημόσιου κλειδιού βασίζονται σε μαθηματικές συναρτήσεις και όχι σε απλές πράξεις με bits. Επιπλέον, η κρυπτογραφία δημόσιου κλειδιού είναι ασύμμετρη (asymmetric) συμπεριλαμβάνοντας τη χρήση ενός ζεύγους ξεχωριστών κλειδιών (key pair), σε αντίθεση με τη συμμετρική που χρησιμοποιεί μόνον ένα κλειδί. Η χρήση δύο κλειδιών επιφέρει σημαντικές τροποποιήσεις σε θέματα που σχετίζονται με την εμπιστευτηκότητα, την αυθεντικότητα και τη διανομή των κλειδιών.

Αρχικά πρέπει να σχολιαστούν κάποιες εσφαλμένες αντιλήψεις όσον αφορά την κρυπτογράφηση με δημόσιο κλειδί. Η πρώτη εσφαλμένη αντίληψη σχετίζεται με την εντύπωση ότι η κρυπτογράφηση δημόσιου κλειδιού είναι ασφαλέστερη μέθοδος σχετικά με τη συμμετρική κρυπτογράφηση, ως ανθεκτικότερη σε κρυπταναλυτικές επιθέσεις. Στην πραγματικότητα η ασφάλεια οποιουδήποτε συστήματος κρυπτογράφησης εξαρτάται από το μήκος κλειδιού και, σε κάθε περίπτωση , από την απαιτούμενη υπολογιστική ισχύ από έναν κρυπταναλυτή για να κατορθώσει να κρυπταναλύσει και αποκαλύψει με επιτυχία ένα κρυπτογραφημένο μήνυμα. Μία δεύτερη λανθασμένη αντίληψη αφορά στην επικράτηση του ασύμμετρου κρυπτοσυστήματος σε βάρος του συμμετρικού. Και τα δύο συστήματα χρησιμοποιούνται ισόρροπα και κατ'

ουδένα τρόπο δεν προβλέπεται η εγκατάλειψη του συμμετρικού συστήματος, ειδικά όταν είναι γνωστή η σημαντική χρονική επιβάρυνση που απαιτείται για την ολοκλήρωση των εκτελούμενων λειτουργιών σε περιβάλλον ασύμμετρου κρυπτοσυστήματος. Επιπλέον, υπάρχει η άποψη ότι η διανομή κλειδιών είναι εύκολη όταν χρησιμοποιείται κρυπτογραφία δημόσιου κλειδιού σε σύγκριση με τις επιπλέον χειραψίες (handshaking) που απαιτούνται με τα κέντρα διανομής κλειδιών (key distribution centers) για τη συμμετρική κρυπτογράφηση. Στην πραγματικότητα, στα ασύμμετρα συστήματα απαιτείται εκτέλεση κάποιων πρωτοκόλλων, εμπλέκεται κάποιος έμπιστος ενδιάμεσος αντιπρόσωπος και οι διαδικασίες που παρεμβάλλονται δεν είναι απλούστερες ή περισσότερο αποδοτικές από αυτές που απαιτούνται για συμμετρική κρυπτογράφηση.

Μία δομή δημόσιου κλειδιού (Σχήμα 4.7) αποτελείται από τις ακόλουθες συνιστώσες:

- Αλγόριθμος κρυπτογράφησης (encryption algorithm): ο αλγόριθμος με τον οποίο πραγματοποιούνται οι διάφοροι μετασχηματισμοί στο αρχικό μήνυμα.
- Αρχικό κείμενο (plaintext): είναι το μη κρυπτογραφημένο μήνυμα που αποτελεί στοιχείο εισόδου στον αλγόριθμο κρυπτογράφησης.
- Ζεύγος δημόσιου (public) και ιδιωτικού (private) κλειδιού: ζεύγος κλειδιών, που έχει επιλεγεί με τρόπο ώστε, το δημόσιο κλειδί του παραλήπτη να χρησιμοποιηθεί για κρυπτογράφηση και το ιδιωτικό κλειδί του παραλήπτη για αποκρυπτογράφηση. Οι ακριβείς μετασχηματισμοί πραγματοποιούνται από τον αλγόριθμο κρυπτογράφησης, εξαρτώμενοι από τις τιμές του δημόσιου και του ιδιωτικού κλειδιού που παρέχονται ως είσοδοι.
- Κρυπτογράφημα ή κρυπτογραφημένο μήνυμα (ciphertext): είναι το μήνυμα που παράγεται από τον αλγόριθμο κρυπτογράφησης ως έξοδος. Εξαρτάται από το αρχικό μήνυμα και το δημόσιο κλειδί του παραλήπτη. Για ένα

συγκεκριμένο μήνυμα από δύο διαφορετικά κλειδιά παράγονται από τη συνάρτηση κρυπτογράφησης δύο διαφορετικά κρυπτογραφημένα κείμενα.

- Αλγόριθμος αποκρυπτογράφησης (decryption algorithm): είναι ο αλγόριθμος που δέχεται ως είσοδο το κρυπτογραφημένο μήνυμα και το ιδιωτικό κλειδί και παράγει το πρωτότυπο αρχικό μήνυμα.

Όπως υποδεικνύει και το όνομά τους, το δημόσιο κλειδί αποσκοπεί σε δημόσια χρήση, ενώ το ιδιωτικό κλειδί το χρησιμοποιεί αποκλειστικά και μόνον ο κάτοχός του. Ένας γενικής χρήσης αλγόριθμος κρυπτογράφησης/ αποκρυπτογράφησης βασίζεται σε ένα δημόσιο κλειδί για κρυπτογράφηση και σε ένα άλλο, διαφορετικό αλλά μοναδικά συσχετιζόμενο κλειδί, το ιδιωτικό κλειδί, για αποκρυπτογράφηση.

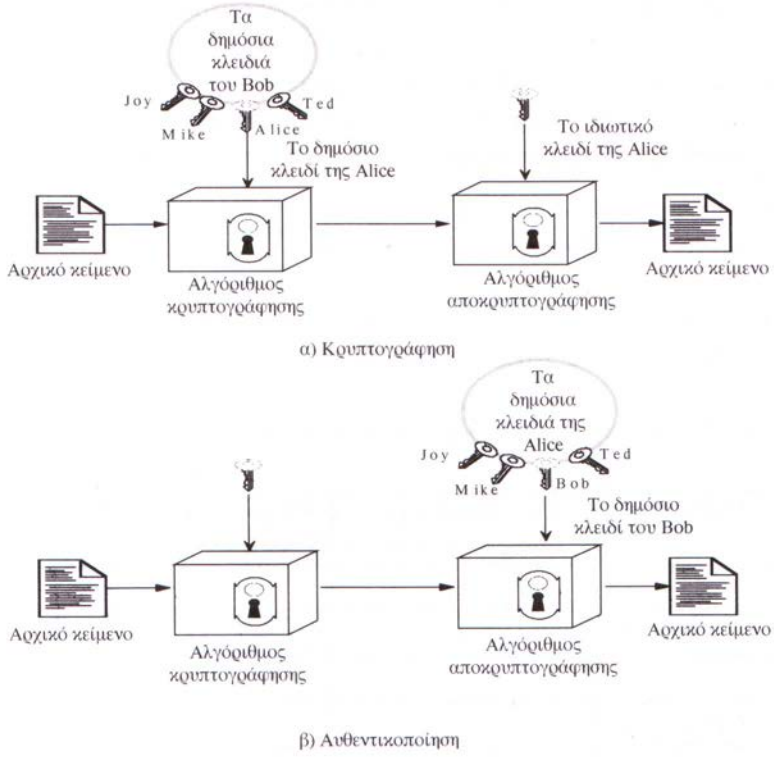
Τα βήματα που ακολουθούνται είναι τα ακόλουθα:

- Για κάθε χρήστη παράγεται ένα ζεύγος κλειδιών, το οποίο θα χρησιμοποιηθεί για την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων.
- Κάθε χρήστης τοποθετεί το δημόσιο κλειδί σε μία βάση δεδομένων ενός φορέα ή σε κάποιο άλλο προσβάσιμο αρχείο. Το άλλο κλειδί, το ιδιωτικό, διαφυλάσσεται διατηρώντας τη μυστικότητά του. Για επίτευξη στοιχειώδους λειτουργικότητας, απαιτείται κάθε χρήστης να είναι σε θέση με ευκολία να ανακτήσει τα δημόσια κλειδιά των άλλων.
- Εάν κάποιος χρήστης Bob επιθυμεί να στείλει ένα μήνυμα στην Alice και αποτελεί τεθείσα απαίτηση (requirement) η διασφάλιση της εμπιστευτικότητας του μηνύματος, τότε ο Bob κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί της Alice.
- Η Alice λαμβάνει το μήνυμα και το αποκρυπτογραφεί με το ιδιωτικό κλειδί της. Κανένας άλλος δεν μπορεί να αποκρυπτογραφήσει το μήνυμα, αφού μόνον η Alice γνωρίζει το ιδιωτικό της κλειδί, που σχετίζεται μοναδικά

με το αντίστοιχο δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση.

Προϋπόθεση αυτής της προσέγγισης είναι όλοι οι συμμετέχοντες να έχουν πρόσβαση στα δημόσια κλειδιά, ενώ τα ιδιωτικά κλειδιά να παράγονται τοπικά για τον κάθε συμμετέχοντα ώστε να διασφαλίζεται αυστηρά η μυστικότητά τους. Οποιαδήποτε στιγμή, ένας χρήστης μπορεί να τροποποιήσει το ιδιωτικό του κλειδί και ταυτοχρόνως να δημοσιεύσει το αντίστοιχο δημόσιο κλειδί, έτσι ώστε να αντικατασταθεί το προηγούμενο μη ισχύον πλέον δημόσιο κλειδί.

Το κλειδί που χρησιμοποιείται στη συμμετρική κρυπτογραφία τυπικά αναφέρεται ως μυστικό (secret) κλειδί. Το ζεύγος κλειδιών (key pair) που χρησιμοποιείται στην ασύμμετρη κρυπτογραφία περιλαμβάνει δημόσιο κλειδί (public key) και ιδιωτικό κλειδί (private key). Το ιδιωτικό κλειδί παραμένει μυστικό, αλλά αναφέρεται ως ιδιωτικό αντί μυστικό κλειδί, ώστε να αποφευχθεί εννοιολογική σύγχυση με τη συμμετρική κρυπτογραφία.



Σχήμα 4.7

5.1.2 Υποδομή Δημοσίου Κλειδιού

Η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure - PKI) είναι ένας συνδυασμός λογισμικού, τεχνολογιών κρυπτογραφίας και υπηρεσιών που επιβεβαιώνουν και πιστοποιούν την εγκυρότητα της κάθε οντότητας που εμπλέκεται σε μια συναλλαγή με το Διαδίκτυο, και παράλληλα προστατεύουν την ασφάλεια της συναλλαγής.

Η Υποδομή Δημοσίου Κλειδιού ενσωματώνει ψηφιακά πιστοποιητικά, κρυπτογραφία δημόσιου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα. Μια τυπική υλοποίηση της Υποδομής Δημοσίου Κλειδιού περιλαμβάνει την παροχή ψηφιακών πιστοποιητικών σε χρήστες, σε εξυπηρετητές, σε λογισμικό χρηστών, καθώς επίσης και εργαλείων για την διαχείριση, ανανέωση και ανάκληση των πιστοποιητικών αυτών.

5.1.2.1 Υπηρεσίες Υποδομής Δημοσίου Κλειδιού

Υπάρχουν οι εξής βασικές λειτουργίες που είναι κοινές σε όλες τις Υποδομές Δημοσίου Κλειδιού και περιγράφονται αναλυτικά στις επόμενες υποενότητες.

Εμπιστευτικότητα (Confidentiality)

Ως εμπιστευτικότητα ορίζεται η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίηση τους. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή δεδομένων. Η Υποδομή Δημοσίου Κλειδιού παρέχει κωδικοποίηση, αφού οι μηχανισμοί ελέγχου πρόσβασης υλοποιούνται κατά βάση από τον συνδυασμό μεθόδων πιστοποίησης (authentication) και εξουσιοδότησης (authorization).

Η εμπιστευτικότητα μπορεί να παρομοιασθεί με έναν αδιαφανή φάκελο. Το μήνυμα που περιλαμβάνει δεν είναι ορατό χωρίς να ανοίξει ο φάκελος. Φυσικά, ο φάκελος μπορεί να ανοιχθεί από τον οποιονδήποτε και να παραβιασθεί το απόρρητο της αλληλογραφίας. Η κρυπτογραφία είναι ένας απολύτως ασφαλής φάκελος που πολύ δύσκολα, σχεδόν ακατόρθωτα, είναι εφικτό να ανοιχτεί από οποιονδήποτε άλλον εκτός από τον νόμιμο παραλήπτη.

Πιστοποίηση (Authentication)

Πιστοποίηση είναι η επιβεβαίωση της ταυτότητας ενός ατόμου ή η επιβεβαίωση της πηγής αποστολής των πληροφοριών. Δηλαδή, το άτομο που επιθυμεί να επιβεβαιώσει την ταυτότητά ενός άλλου άτομου ή κάποιου εξυπηρετητή με το οποίο επικοινωνεί, βασίζεται στην πιστοποίηση.

Η πιστοποίηση μπορεί να υλοποιηθεί με τρεις βασικές μεθόδους:

1. Κάτι που γνωρίζουμε, π.χ. το PIN μιας τραπεζικής κάρτας ή το μυστικό κωδικό ενός λογαριασμού (password).
2. Κάτι που έχουμε στην ιδιοκτησία μας, π.χ. το κλειδί μιας πόρτας ή μια τραπεζική κάρτα.
3. Κάτι που έχουμε εκ γενετής, π.χ. δακτυλικά αποτυπώματα, φωνή κτλ.

Η Πιστοποίηση, πιο απλά, είναι ο τρόπος με τον οποίο δημοσιεύονται οι τιμές των δημόσιων κλειδιών και η πληροφορία που αντιστοιχεί στις τιμές αυτές. Ένα *πιστοποιητικό* (certificate) είναι ο τρόπος με τον οποίο η Υποδομή Δημοσίου Κλειδιού μεταδίδει τις τιμές των δημόσιων κλειδιών, ή πληροφορία που σχετίζεται με αυτά, ή και τα δύο. Γενικά, ένα πιστοποιητικό είναι μία συλλογή πληροφοριών που έχει υπογραφεί ψηφιακά από την οντότητα που το εκδίδει. Τα πιστοποιητικά αυτά χαρακτηρίζονται από το

είδος της πληροφορίας που περιέχουν. Η εκδότρια αρχή των πιστοποιητικών ονομάζεται *Αρχή Πιστοποίησης* (Certificate Authority - CA).

Ακεραιότητα (Integrity)

Ακεραιότητα είναι η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάσταση τους. Η υπηρεσία αυτή παρέχεται από μηχανισμούς κρυπτογραφίας όπως είναι οι ψηφιακές υπογραφές.

Ας υποθέσουμε την ακεραιότητα ενός διαφανούς φακέλου. Το μήνυμα που περιέχει ο φάκελος μπορεί να διαβαστεί από τον οποιονδήποτε, οπότε και παραβιάζεται η εμπιστευτικότητα, όπως αυτή ορίστηκε παραπάνω. Ο φάκελος θεωρείται ενδεικτικό στοιχείο παραβίασης. Ο παραλήπτης βλέποντας τον φάκελο είναι σε θέση να επιβεβαιώσει ότι ο φάκελος δεν έχει ανοιχθεί, παραβιαστεί ή ακόμη και αντικατασταθεί.

Μη Άρνηση Αποδοχής (Non-Repudiation)

Η Μη Άρνηση Αποδοχής συνδυάζει τις υπηρεσίες της πιστοποίησης και της ακεραιότητας που παρέχονται σε μια τρίτη οντότητα. Έτσι, ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί την δημιουργία και αποστολή του μηνύματος. Η ασύμμετρη κρυπτογραφία παρέχει ψηφιακές υπογραφές, τέτοιες ώστε μόνο ο αποστολέας του μηνύματος θα μπορούσε να κατέχει την συγκεκριμένη ψηφιακή υπογραφή, πρόκειται δηλαδή για μια αμφιμονοσήμαντη σχέση. Με αυτόν τον τρόπο, ο οποιοσδήποτε, και φυσικά και ο παραλήπτης του ψηφιακά υπογεγραμμένου μηνύματος μπορεί να επιβεβαιώσει την ψηφιακή υπογραφή του αποστολέα.

5.1.2.2 Πρότυπα Ανάπτυξης Υποδομής Δημοσίου Κλειδιού

Η Υποδομή Δημοσίου Κλειδιού υλοποιείται σύμφωνα με διεθνή πρότυπα, όπως αυτά ορίζονται από Παγκόσμιους Οργανισμούς. Όπως για παράδειγμα:

Internet Engineering Task Force, Request for Comments (IETF RFCs)

Υποδομή Δημοσίου Κλειδιού X.509 (PKIX).

Η ομάδας εργασίας PKIX (Working Group PKIX) δημιουργήθηκε το 1995 με βασικό στόχο την ανάπτυξη προτύπων Διαδικτύου (Internet Standards) αναγκαία για την υποστήριξη της Υποδομής Δημοσίου Κλειδιού.

Public-Key Cryptography Standards (PKCS)

Το 1991 δημοσιοποιήθηκαν οι πρώτες τεχνικές προδιαγραφές για πρότυπα Κρυπτογραφίας Δημοσίου Κλειδιού από τα εργαστήρια RSA με στόχο την επιτάχυνση της ανάπτυξης της Υποδομής Δημοσίου Κλειδιού. Οι τεχνικές αυτές προδιαγραφές αποτελούν σημείο αναφοράς για κάθε υλοποίηση Υποδομής Δημοσίου Κλειδιού, είναι γνωστές με το ακρωνύμιο PKCS και έναν συγκεκριμένο αριθμό π.χ. PKCS#1 RSA Cryptography Standard.

5.1.2.3 Pretty Good Privacy (PGP)

Για την κρυπτογράφηση ηλεκτρονικού ταχυδρομείου και αρχείων, δημοφιλέστερο πρόγραμμα είναι το PGP (Pretty Good Privacy). Οι αλγόριθμοι του PGP είναι γνωστοί και ασφαλείς. Ο πηγαίος κώδικάς του είναι διαθέσιμος στο κοινό, γεγονός που επέτρεψε σε ειδικούς επιστήμονες των κλάδων της πληροφορικής και της κρυπτογραφίας να το εξετάσουν και να αναζητήσουν σφάλματα ή "κερκόπορτες" (back doors). Χρησιμοποιείται εδώ και αρκετά χρόνια, και οι ειδικοί της κρυπτογραφίας το θεωρούν σε μεγάλο βαθμό

αξιόπιστο.

Το PGP αποτελεί ένα κρυπτοσύστημα που δημιουργήθηκε από τον καθηγητή Philip Zimmerman του MIT και χρησιμοποιεί τους αλγόριθμους για την κρυπτογράφηση και υπογραφή μηνυμάτων ηλεκτρονικού ταχυδρομείου. Όταν κυκλοφόρησε για πρώτη φορά, η αμερικανική κυβέρνηση προσπάθησε να απαγορεύσει τη διανομή του, με τη δικαιολογία ότι η υψηλής ποιότητας κρυπτογράφηση συμπεριλαμβάνεται στα... όπλα, και η κυβέρνηση έχει δικαίωμα να περιορίσει τη χρήση της.

Πρόκειται βέβαια για εμπορικό πρόγραμμα, μπορεί ωστόσο να χρησιμοποιηθεί χωρίς χρέωση για μη επαγγελματική χρήση. Επίσης υπάρχουν και εκδόσεις open source/free software (λογισμικό ανοιχτού/ελεύθερου κώδικα και δωρεάν διανομής), όπως το gnupgp. Το PGP ήταν αρχικά διαθέσιμο από την PGP Inc. Η εταιρία εξαγοράστηκε από τη Network Associates, η οποία ανέλαβε την εξέλιξη και τις αναβαθμίσεις του προγράμματος. Στις αρχές του 2002 η Network Associates ανακοίνωσε ότι θα σταματήσει την πώληση και υποστήριξη του PGP. Αργότερα, όμως, αποφασίσθηκε η επανασύσταση της PGP Corporation, η οποία αναπτύσσει τη νέα έκδοση (8.0) του προγράμματος και θα αναλάβει την υποστήριξή του.

Ο χρήστης προγραμμάτων τύπου PGP πρέπει αρχικά να δημιουργήσει ένα ζευγάρι κλειδιών (key pair), δημόσιο και ιδιωτικό. Παρέχει το δημόσιο κλειδί σε όλους τους παραλήπτες είτε με e-mail είτε δημοσιεύοντάς το στο Internet. Το ιδιωτικό κλειδί παραμένει κρυφό, στο σταθμό εργασίας του χρήστη, και δεν θα πρέπει να διαρρεύσει, καθώς εξασφαλίζει την αποτελεσματικότητα της κρυπτογράφησης.

Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί. Αυτή είναι μια μονόδρομη διαδικασία: αφού κρυπτογραφηθεί το μήνυμα, δεν μπορεί να

αποκρυπτογραφηθεί παρά μόνο με το ιδιωτικό κλειδί. Για το λόγο αυτό, είναι σημαντικό να μη διαρρεύσει. Επειδή και το ιδιωτικό και το δημόσιο κλειδί μπορεί να αποτελούν αρκετά μεγάλα σε όγκο αρχεία, το πρόγραμμα PGP αποθηκεύει το ιδιωτικό κλειδί στο δίσκο κρυπτογραφημένο. Κάθε φορά που ο χρήστης θέλει να το χρησιμοποιήσει, πρέπει να εισάγει την "passphrase", κωδικό που δεν αποθηκεύεται πουθενά αλλά έχει ο ίδιος απομνημονεύσει.

Κάθε χρήστης του PGP διατηρεί λίστα με τα δημόσια κλειδιά των χρηστών με τους οποίους επικοινωνεί (keyring). Για την προστασία της λίστας, την υπογράφει ο ίδιος με το ιδιωτικό του κλειδί. Κάθε κλειδί που προστίθεται στη λίστα είναι δυνατόν να φέρει έναν από τους παρακάτω χαρακτηρισμούς:

- Απολύτως Έμπιστο (Completely Trusted)
- Μερικώς Έμπιστο (Marginally Trusted)
- Μη Έμπιστο (Untrusted)
- Άγνωστο (Unknown)

Πάντως, αν και το PGP είναι σε μεγάλο βαθμό αξιόπιστο για εφαρμογές απλής ταυτοποίησης που εκτελούνται από απλούς χρήστες, δεν θεωρείται κατάλληλο για εφαρμογές ηλεκτρονικού εμπορίου και για όσες απαιτούν ισχυρή ταυτοποίηση. Τα πιστοποιητικά του PGP δεν είναι επεκτάσιμα και περιέχουν μόνο μία διεύθυνση ηλεκτρονικής αλληλογραφίας, την τιμή ενός δημόσιου κλειδιού και ένα χαρακτηρισμό βαθμού εμπιστοσύνης.

Καθώς η διεύθυνση ηλεκτρονικής αλληλογραφίας δεν μπορεί να αποτελέσει ασφαλές μέσο προσδιορισμού της ταυτότητας ενός χρήστη, το PGP δεν μπορεί να παράσχει ισχυρή ταυτοποίηση (strong authentication). Η έλλειψη επεκτασιμότητας των πιστοποιητικών του PGP τα καθιστά ακατάλληλα για άλλες εφαρμογές εκτός της ηλεκτρονικής αλληλογραφίας.

Επίσης, το συγκεκριμένο πρόγραμμα δεν υποστηρίζει μεθόδους επαλήθευσης και ανάκλησης των πιστοποιητικών. Οι διαδικασίες αυτές διεξάγονται αποκλειστικά με άμεση επικοινωνία των χρηστών. Επιπλέον, δεν παρέχει την επιλογή της ανωνυμίας, καθώς η χρήση μιας διεύθυνσης e-mail που δεν περιέχει κάποια ένδειξη για την ταυτότητα του χρήστη καθιστά αδύνατη την επικοινωνία μεταξύ των χρηστών για την επαλήθευση και ανάκληση των πιστοποιητικών.

5.1.2.4 X.509

Το X.509 σχεδιάστηκε για να παρέχει την υποδομή πιστοποίησης στις υπηρεσίες καταλόγου του X.500 (ldap). Η πρώτη έκδοση του X.509 δημοσιεύτηκε το 1988, καθιστώντας το έτσι την παλαιότερη πρόταση για μία παγκόσμια Υποδομή Δημοσίου Κλειδιού.

Το γεγονός αυτό σε συνδυασμό με την υποστήριξη του προτύπου από τον Διεθνή Οργανισμό Τυποποίησης (International Standards Organization - ISO) και την Διεθνή Ένωση Τηλεπικοινωνιών (Internation Telecommunications Union - ITU) έχουν οδηγήσει στην υιοθέτηση του X.509 από μεγάλο αριθμό οργανισμών και κατασκευαστών.

Η Visa και η Mastercard έχουν επιλέξει το X.509 για το Secure Electronic Transactions (SET) πρότυπο, και η Netscape υιοθέτησε το X.509 πρότυπο για την έκδοση των πιστοποιητικών που χρησιμοποιούνται στο Secure Sockets Layer πρωτόκολλο.

Η έκδοση 3 του X.509 επεκτείνει σε μεγάλο βαθμό την λειτουργικότητα του προτύπου και γι αυτό είναι ιδιαίτερα διαδεδομένο και χρησιμοποιείται σε πλοηγητές ιστοσελίδων (web browsers), εξυπηρετητές και προγράμματα

λογισμικού για την διαχείριση του ηλεκτρονικού ταχυδρομείου (mail server/clients) κτλ από πολλές γνωστές εταιρίες ανάπτυξης λογισμικού.

5.1.2.5 Ακαδημαϊκή Εφαρμογή Υποδομής Δημοσίου Κλειδιού

Η Υποδομή Δημοσίου Κλειδιού έχει πολλές εφαρμογές σε ένα Ακαδημαϊκό Ίδρυμα. Όπως:

Ασφαλές Ηλεκτρονικό Ταχυδρομείο

Ο χρήστης ηλεκτρονικού ταχυδρομείου που έχει αποκτήσει προσωπικό ψηφιακό πιστοποιητικό από μια Αρχή Πιστοποίησης έχει τη δυνατότητα να ανταλλάσσει κρυπτογραφημένα μηνύματα, διαφυλάσσοντας έτσι την ασφάλεια των μηνυμάτων του και το απαραβίαστο της προσωπικής του ηλεκτρονικής αλληλογραφίας.

Ο χρήστης κρυπτογραφεί το μήνυμα του με το δημόσιο κλειδί του παραλήπτη και το υπογράφει με την ψηφιακή του υπογραφή. Έτσι, μόνο ο παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα, με το ιδιωτικό του κλειδί, και να διαβάσει το περιεχόμενο του μηνύματος. Ακόμη, ο παραλήπτης είναι σίγουρος ότι ο αποστολέας είναι αυτός που δηλώνει ότι απέστειλε το μήνυμα, βασιζόμενος στην ψηφιακή υπογραφή που φέρει το μήνυμα, καθώς επίσης και ότι το περιεχόμενο του μηνύματος δεν έχει αλλοιωθεί.

Πρόσβαση σε ασφαλείς δικτυακούς τόπους

Η αποδοχή της Αρχής Πιστοποίησης συνεπάγεται την προσθήκη ψηφιακών πιστοποιητικών στον πλοηγητή (browser) του χρήστη του Διαδικτύου. Με βάση τα ιδιαίτερα χαρακτηριστικά του πιστοποιητικού αυτού,

ο χρήστης έχει τη δυνατότητα να επισκεφτεί ασφαλείς δικτυακούς τόπους και να προσπελάσει δεδομένα, χωρίς αυτά να είναι δημοσιευμένα σε κοινή θέα.

Για παράδειγμα, ασφαλείς δικτυακοί τόποι είναι οι ιστοσελίδες http://mail.auth.gr/ και http://accounts.auth.gr/ για την διαχείριση του ηλεκτρονικού ταχυδρομείου και των λογαριασμών αντίστοιχα. Τα στοιχεία που υποβάλλει ο χρήστης και τα δεδομένα που βλέπει στους παραπάνω δικτυακούς τόπους δεν είναι διαθέσιμα σε κοινή θέα.

Προστασία ευαίσθητων δεδομένων σε γραμματείες τμημάτων και διοικητικούς φορείς

Οι γραμματείες των τμημάτων ενός Ακαδημαϊκού Ιδρύματος καθώς επίσης και οι διοικητικές υπηρεσίες έχουν στη διάθεσή τους ιδιαίτερα ευαίσθητα δεδομένα που πρέπει να προστατευτούν.

Η βαθμολογία φοιτητών, τα οικονομικά στοιχεία των εργαζομένων, τα διοικητικά έγγραφα, οι πρυτανικές αποφάσεις, είναι μερικά σημαντικά δεδομένα που δεν πρέπει να είναι κοινώς προσπελάσιμα, παρά μόνο από εξουσιοδοτημένα μέλη και επίσης πρέπει να προστατεύονται από παραβιάσεις και αλλοιώσεις.

Η πιστοποίηση της ταυτότητας των χρηστών και η προστασία τέτοιου είδους δεδομένων μπορεί να επιτευχθεί με την Υποδομή Δημοσίου Κλειδιού. Με τα ψηφιακά πιστοποιητικά για τους χρήστες επιβεβαιώνεται η ταυτότητά τους και με τους μηχανισμούς κρυπτογράφησης βεβαιώνεται η ασφάλεια των δεδομένων.

Προστασία ερευνητικών δεδομένων

Η προστασία ερευνητικών αποτελεσμάτων και μελετών είναι ιδιαίτερα σημαντική σε ένα ακαδημαϊκό ίδρυμα. Τα ευαίσθητα ερευνητικά δεδομένα που αποθηκεύονται σε εξυπηρετητές πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση. Επίσης, η δικτυακή μεταφορά τους σε εξουσιοδοτημένα μέλη της ακαδημαϊκής κοινότητας πρέπει να είναι ασφαλείς.

Η Υποδομή Δημοσίου Κλειδιού παρέχει μηχανισμούς ασφαλείας για αποθήκευση και μεταφορά ερευνητικών δεδομένων. Τα ερευνητικά δεδομένα κρυπτογραφούνται, έτσι ώστε μόνο εξουσιοδοτημένα μέλη να έχουν τη δυνατότητα να τα αποκρυπτογραφήσουν και να τα αποκτήσουν.

Πρόσβαση σε ηλεκτρονικές βιβλιοθήκες

Η πρόσβαση σε ηλεκτρονικές βιβλιοθήκες είναι ένα αναγκαίο εργαλείο για την ακαδημαϊκή έρευνα και μελέτη.

Στην πλειοψηφία, οι ηλεκτρονικές βιβλιοθήκες παρέχουν τη δυνατότητα σύνδεσης χρηστών που έχουν διεύθυνση δικτύου (IP) με συγκεκριμένη μορφή (π.χ. οι χρήστες του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης μπορούν να προσπελάσουν τα ψηφιακά δεδομένα της βιβλιοθήκης του Α.Π.Θ μόνο αν έχουν διεύθυνση δικτύου της μορφής 155.207.x.y). Η λύση αυτή όχι μόνο δεν είναι ασφαλής, αλλά παρεμποδίζει και το έργο των ακαδημαϊκών μελών όταν αυτοί βρίσκονται εκτός του Ακαδημαϊκού Ιδρύματος ή συνδέονται μέσω κάποιου παροχέα δικτυακών υπηρεσιών (Internet Provider), οπότε και αποκτούν διεύθυνση δικτύου διαφορετικής μορφής.

Τα προβλήματα αυτά μπορούν να επιλυθούν με ένα πιο ευέλικτο σχήμα ταυτοποίησης των εξουσιοδοτημένων χρηστών. Η Υποδομή Δημοσίου

Κλειδιού παρέχει ψηφιακά πιστοποιητικά για κάθε χρήστη, έτσι ώστε να επιβεβαιώνεται η ταυτότητά του και να έχει τη δυνατότητα πρόσβασης σε ηλεκτρονικές βιβλιοθήκες μόνο με βάση την ακαδημαϊκή του ιδιότητα.

Πλέγμα Δεδομένων (Data GRID)

Το Πλέγμα Δεδομένων είναι μια σχετικά νέα έννοια στην νέα ψηφιακή κοινωνία και αποδεικνύεται μια πολύ ουσιώδης δομή για τα Ακαδημαϊκά Ιδρύματα. Η δικτυακή αυτή δομή επιτρέπει σε ερευνητές, εργαστήρια και πανεπιστήμια από όλο τον κόσμο να συνενώνουν τις δυνάμεις τους για να έχουν μια δυναμική συνεργασία σε διάφορες ερευνητικές περιοχές.

Βασιζόμενοι σε μια κατανεμημένη δομή που περιλαμβάνει ηλεκτρονικές βιβλιοθήκες, δικτυακούς πόρους, χώρους αποθήκευσης ψηφιακών δεδομένων, υπολογιστικά συστήματα μεγάλης ισχύος ανά τον κόσμο, τα ακαδημαϊκά μέλη έχουν το δικαίωμα να χρησιμοποιήσουν τα μέσα αυτά, ανεξάρτητα από την φυσική τους τοποθεσία, με στόχο την έρευνα.

Για παράδειγμα χιλιάδες αστρονόμοι που ανήκουν σε διάφορα ακαδημαϊκά εργαστήρια του κόσμου και εστιάζουν σε μια ερευνητική περιοχή μπορούν να δημιουργήσουν ένα Πλέγμα Δεδομένων και να διαμοιράζονται όλα τα φυσικά μέσα που χρειάζονται για την έρευνα τους, ανεξάρτητα από την χωροταξική τους θέση.

Η πρόσβαση σε ερευνητικά δεδομένα, σε αποτελέσματα μελετών, σε δικτυακούς πόρους, σε χώρους αποθήκευσης δεδομένων και γενικότερα σε μέσα που χρησιμοποιούνται για έρευνα πρέπει να περιορίζεται μόνο σε εξουσιοδοτημένα μέλη της ακαδημαϊκής κοινότητας. Αυτό επιτυγχάνεται με την Υποδομή Δημοσίου Κλειδιού και με την αντιστοίχηση ψηφιακών πιστοποιητικών σε κάθε χρήστη, ώστε να επιβεβαιώνεται η ταυτότητάς τους.

Δημιουργία ερευνητικών ιστοσελίδων με δημόσια και ιδιωτικά τμήματα

Πολλά ερευνητικά προγράμματα που εκπονούνται στα πλαίσια ακαδημαϊκών προγραμμάτων έχουν οργανωμένες ιστοσελίδες, όπου και δημοσιεύονται διάφορα στοιχεία και αποτελέσματα για το ερευνητικό έργο που επιτελείται.

Στα ερευνητικά αυτά έργα είναι πιθανό να συμμετέχουν επιστημονικοί συνεργάτες από άλλα ακαδημαϊκά ιδρύματα και να κρίνεται αναγκαία η απομακρυσμένη προσπέλαση συγκεκριμένων συνεργατών στα ερευνητικά δεδομένα. Έτσι δημιουργείται η ανάγκη να υπάρχουν ιστοσελίδες που να παρέχουν πληροφορίες και να παρουσιάζουν το ερευνητικό έργο σε κάθε ενδιαφερόμενο, αλλά παράλληλα να υπάρχει η δυνατότητα απομακρυσμένης πρόσβασης από συγκεκριμένα ακαδημαϊκά μέλη σε δεδομένα της έρευνας που δεν είναι προς κοινή δημοσίευση.

Η διάκριση των εξουσιοδοτημένων ακαδημαϊκών μελών που μπορούν να έχουν πρόσβαση σε όλα τα ερευνητικά δεδομένα και στους υπόλοιπους ενδιαφερόμενους που έχουν περιορισμένη πρόσβαση, μπορεί να υλοποιηθεί με βάση την Υποδομή Δημοσίου Κλειδιού και την χρήση πιστοποιητικών. Ανάλογα με τα χαρακτηριστικά του πιστοποιητικού του χρήστη θα επιτρέπεται η αντίστοιχη προσπέλαση στην ερευνητική ιστοσελίδα.

Υποβολή Ψηφιακά Υπογεγραμμένων Εργασιών

Σε μερικά μαθήματα δίνεται η δυνατότητα υλοποίησης ή παράδοσης εργασιών μέσα από το περιβάλλον μιας ιστοσελίδας.

Η Υποδομή Δημοσίου Κλειδιού παρέχει έναν ασφαλή τρόπο να καθοριστεί ο αποστολέας της εργασίας, ότι η εργασία δεν έχει αλλοιωθεί και έχει

υποβληθεί στο χρονικό διάστημα της ανάθεσης, όπως αυτό έχει αρχικά οριστεί
(χρονοσφράγιση-timestamp).

Υπογεγραμμένο Λογισμικό

Η Υποδομή Δημοσίου Κλειδιού παρέχει ψηφιακά πιστοποιητικά σε χρήστες για να υπογράψουν το λογισμικό που αναπτύσσουν.

Οι ψηφιακές υπογραφές που συνοδεύουν το λογισμικό είναι τέτοιες ώστε οι αποδέκτες του λογισμικού να γνωρίζουν ποιος ανέπτυξε το λογισμικό καθώς επίσης και να είναι βέβαιοι ότι μπορούν να χρησιμοποιήσουν άμεσα το λογισμικό χωρίς να παρουσιαστούν προβλήματα ασφαλείας (εγκατάσταση ηλεκτρονικών ιών).

5.1.3 Εφαρμογές Κρυπτοσυστημάτων Δημόσιου Κλειδιού

Τα συστήματα δημόσιου κλειδιού χαρακτηρίζονται από τη χρήση κρυπτογραφικών αλγορίθμων με δύο κλειδιά, εκ των οποίων το ένα παραμένει ιδιωτικό και το άλλο είναι δημόσια διαθέσιμο. Ανάλογα με τις απαιτήσεις ασφάλειας, το είδος της εφαρμογής και της υπηρεσίας που σχετίζεται και υλοποιείται, ο αποστολέας χρησιμοποιεί είτε το δικό του ιδιωτικό κλειδί, είτε το δημόσιο κλειδί του παραλήπτη, είτε και τα δύο για να πραγματοποιήσει κάποιον τύπο κρυπτογραφικών λειτουργιών.

Υπάρχουν τρεις περιπτώσεις στις οποίες χρησιμοποιείται το ζεύγος κλειδιών σε αυτά τα συστήματα:

- Κρυπτογράφηση/Αποκρυπτογράφηση (Encryption/Decryption): Ο αποστολέας κρυπτογραφεί ένα μήνυμα με το δημόσιο κλειδί του παραλήπτη και ο παραλήπτης αποκρυπτογραφεί με το ιδιωτικό κλειδί του.

- Ψηφιακή υπογραφή (Digital Signature): Ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να υπογράψει ένα μήνυμα. Η υπογραφή δημιουργείται με την εφαρμογή ενός αλγόριθμου κρυπτογράφησης στο μήνυμα ή συνηθέστερα στη σύνοψη (hash) του μηνύματος. Ο παραλήπτης αυθεντικοποιεί τον αποστολέα με χρήση του δημόσιου κλειδιού του.
- Ανταλλαγή κλειδιών (Key Exchange): δύο οντότητες συνεργάζονται ώστε να ανταλλάξουν ένα κλειδί συνόδου (session key). Για την υλοποίηση της ανταλλαγής κλειδιών είναι πιθανόν να λάβουν χώρα διάφορες ενέργειες, που αξιοποιούν το ιδιωτικό κλειδί της μιας ή και των δύο οντοτήτων που συμμετέχουν.

Αλγόριθμος	Κρυπτογράφηση/ Αποκρυπτογράφηση	Ψηφιακή Υπογραφή	Ανταλλαγή Κλειδιών
RSA	x	x	x
Diffie-Hellman	-	-	x
DSS	-	x	-
Elliptic Curve	x	x	x

Κάποιο αλγόριθμοι είναι κατάλληλοι και για τις τρεις εφαρμογές, άλλοι μόνο για δύο ή μία από αυτές. Στον πίνακα αναφέρονται οι εφαρμογές που υποστηρίζονται από τους αλγόριθμους που επεξηγούνται σε αυτό το κεφάλαιο: τον RSA και τον Diffie – Hellman. Επίσης περιλαμβάνονται ο Digital Signature Standard – DSS και η Elliptic-Curve Cryptography – ECC που επεξηγούνται σε επόμενα κεφάλαια.

5.1.4 Απαιτήσεις σε Περιβάλλον Κρυπτογραφίας Δημόσιου κλειδιού

Το κρυπτοσύστημα που απεικονίζεται στο σχήμα 4.7 βασίζεται σε έναν αλγόριθμο κρυπτογράφησης που αξιοποιεί δύο συσχετιζόμενα κλειδιά. Όταν προτάθηκε το ασύμμετρο σύστημα κρυπτογράφησης από τους W. Diffie και M. Hellman δεν υπήρχαν συγκεκριμένοι αλγόριθμοι που να το υλοποιούν. Ωστόσο, καθορίστηκαν οι συνθήκες που πρέπει να πληρεί ένας τέτοιος αλγόριθμος:

- Είναι υπολογιστικά εύκολο για κάποιο φορέα B να δημιουργήσει ένα ζεύγος κλειδιών (δημόσιο κλειδί KU_b ,ιδιωτικό κλειδί KR_b).
- Είναι υπολογιστικά εύκολο για τον αποστολέα A, γνωρίζοντας το δημόσιο κλειδί και το μήνυμα προς κρυπτογράφηση M, να δημιουργήσει το αντίστοιχο κρυπτογραφημένο μήνυμα C το οποίο προκύπτει ως εξής: $C = E_{KUb}(M)$
- Είναι υπολογιστικά εύκολο για τον παραλήπτη B να αποκρυπτογραφήσει το κρυπτογραφημένο μήνυμα C, χρησιμοποιώντας το ιδιωτικό του κλειδί, ώστε να ανακτήσει το αρχικό του μήνυμα: $M = D_{KRb}(C) = D_{KRb}[E_{KUb}(M)$
- Είναι υπολογιστικά ανέφικτο (computationally infeasible) για έναν επιτιθέμενο γνωρίζοντας το δημόσιο κλειδί KU_b να υπολογιστεί το αντίστοιχο ιδιωτικό κλειδί KR_b.
- Είναι υπολογιστικά ανέφικτο για έναν επιτιθέμενο, γνωρίζοντας το δημόσιο κλειδί KU_b και το κρυπτογραφημένο κείμενο C να ανακρήσει το αρχικό κείμενο M.

Μπορούμε, επιπλέον, να προσθέσουμε και έκτο κανόνα, ο οποίος είναι χρήσιμος, αν και δεν είναι απαραίτητος σε όλες τις εφαρμογές ασύμμετρου κρυπτοσυστήματος:

- Οποιοδήποτε από τα δύο συσχετιζόμενα κλειδιά μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση και το άλλο για την αποκρυπτογράφηση, δηλαδή ισχύει: $M = D_{KRb}[E_{KUb}(M)] = D_{KUb}[E_{KRb}(M)]$

5.2 Αλγόριθμοι για Ασύμμετρα Κρυπτοσυστήματα

Οι πιο διαδεδομένοι αλγόριθμοι για ασύμμετρα κρυπτοσυστήματα είναι ο αλγόριθμος RSA και ο αλγόριθμος των Diffie-Hellman. Σε αυτήν την ενότητα αναλύονται οι αλγόριθμοι αυτοί και στη συνέχεια παρουσιάζονται συνοπτικά δύο ακόμη αλγόριθμοι ο Digital Signature Standard (DSS) και ο Elliptic-Curve Cryptography (ECC).

5.2.1 Αλγόριθμος RSA

Ο RSA είναι ένα κρυπτοσύστημα δημοσίου κλειδιού για κρυπτογράφηση και εξακρίβωση γνησιότητας. Εφευρέθηκε το 1977 από τους Ron Rivest, Adi Shamir και Leonard Adleman. Δουλεύει ως εξής: Παίρνουμε δύο μεγάλους πρώτους αριθμούς, *p* και *q* και βρίσκουμε το γινόμενό τους *n=pq*, το *n* λέγεται διαιρέτης. Διαλέγουμε έναν αριθμό *e* ο οποίος είναι μικρότερος από τον *n* και σχετικά πρώτος με το *(p-1)(q-1)*, δηλαδή ο *e* και το *(p-1)(q-1)* δεν έχουν κοινούς διαιρέτες εκτός από το 1. Βρίσκουμε άλλον έναν αριθμό *d* τέτοιον ώστε το *(ed-1)* να είναι διαιρέσιμο από το *(p-1)(q-1)*. Οι τιμές *e* και *d* ονομάζονται **δημόσιοι** και **ιδιωτικοί δείκτες** αντίστοιχα. Το δημόσιο κλειδί είναι το ζευγάρι *(n,e)* και το ιδιωτικό το *(n,d)*. Οι παράγοντες *p* και *q* μπορεί να κρατηθούν μαζί με το ιδιωτικό κλειδί ή να καταστραφούν.

Είναι δύσκολο πιθανώς να βρεθεί το ιδιωτικό κλειδί *d* από το δημόσιο *(n,e)*. Εάν κάποιος μπορέσει να αναλύσει το *n* σε p και q, θα μπορέσει να

πάρει την τιμή *d*. Η ασφάλεια του RSA βασίζεται στην θεώρηση ότι η ανάλυση σε παράγοντες γινομένου είναι δύσκολη. Μια μέθοδος εύκολης ανάλυσης σε παράγοντες γινομένου ή κάποια άλλη εφικτή επίθεση θα μπορούσε να "σπάσει" τον RSA.

Παρακάτω παρουσιάζεται ένα απλουστευμένο παράδειγμα για το πώς δουλεύει ο αλγόριθμος για κρυπτογράφηση και εξακρίβωση γνησιότητας:

RSA κρυπτογράφηση: Ας υποθέσουμε ότι η Alice θέλει να στείλει ένα μήνυμα *m* στον Bob. Η Alice δημιουργεί το κρυπτογραφημένο μήνυμα *c* ως εξής : $c=m^e \bmod n$, όπου *e* και *n* είναι το δημόσιο κλειδί του Bob και το στέλνει στον Bob. Για την αποκρυπτογράφηση ο Bob κάνει το εξής: $m=c^d \bmod n$, η σχέση μεταξύ *e* και *d* εξασφαλίζει ότι ο Bob θα αποκρυπτογραφήσει σωστά το *m*. Εφόσον μόνο ο Bob κατέχει το *d*, μόνο αυτός μπορεί να το αποκρυπτογραφήσει.

RSA εξακρίβωση γνησιότητας: Τώρα ας υποθέσουμε ότι η Alice θέλει να στείλει ένα μήνυμα *m* στον Bob έτσι ώστε αυτός να είναι σίγουρος ότι το μήνυμα είναι αυθεντικό και προέρχεται από την Alice. Η Alice δημιουργεί μια ηλεκτρονική υπογραφή *s* ως εξής: $s=m^d \bmod n$, όπου *d, n* είναι το ιδιωτικό κλειδί της Alice, και στέλνει τα *m, s* στον Bob. Για να γίνει η επιβεβαίωση της υπογραφής ο Bob ελέγχει το μήνυμα *m* που πήρε με αυτό που βγαίνει από την πράξη $s^e \bmod n$, όπου *e,n* είναι το δημόσιο κλειδί της Alice.

5.2.2 Diffie-Hellman

Ο αλγόριθμος Diffie-Hellman είναι ένα πρωτόκολλο συμφωνίας που επιτρέπει την ανταλλαγή ενός μυστικού κλειδιού χρησιμοποιώντας τεχνικές των αλγορίθμων δημοσίου κλειδιού. Αναπτύχθηκε από τους Diffie και Hellman το 1976.

Το πρωτόκολλο έχει δύο παραμέτρους συστήματος p και g. Είναι και οι δύο δημόσιες και μπορούν να χρησιμοποιηθούν από όλους τους χρήστες σε ένα σύστημα. Η παράμετρος p είναι ένας πρώτος αριθμός και η παράμετρος g είναι ένας ακέραιος μικρότερος του p, ο οποίος είναι ικανός να παράγει κάθε αριθμό από το 1 έως το $p-1$ όταν πολλαπλασιαστεί με τον εαυτό του ορισμένες φορές modulo τον πρώτο p.

Ας υποτεθεί ότι η Alice και ο Bob θέλουν να συμφωνήσουν σε ένα μυστικό κλειδί χρησιμοποιώντας το παραπάνω πρωτόκολλο. Προχωρούν ως ακολούθως: Πρώτα η Alice παράγει μια τυχαία ιδιωτική τιμή a και ο Bob παράγει μια τυχαία ιδιωτική τιμή b. Έπειτα και οι δύο παράγουν τις δημόσιες τιμές χρησιμοποιώντας τις παραμέτρους p και g και τις ιδιωτικές τους τιμές. Η δημόσια τιμή της Alice είναι η g^a mod p και του Bob g^b mod p. Στη συνέχεια ανταλλάσσουν τις δημόσιες τιμές τους. Τελικά, η Alice υπολογίζει $k_{ab}=(g^b)^a$ mod p και ο Bob $k_{ba}=(g^a)^b$ mod p. Εφόσον $k_{ab}=k_{ba}=k$, η Alice και ο Bob τώρα έχουν μοιραστεί ένα μυστικό κλειδί k.

Η ασφάλεια του πρωτοκόλλου εξαρτάται πάνω στο πρόβλημα του διακριτού λογάριθμου. Υποτίθεται ότι είναι υπολογιστικά μη πρακτικό να

υπολογιστεί το κοινό μυστικό κλειδί k όταν δοθούν δύο δημόσιες τιμές g^a mod p και g^b mod p όταν ο πρώτος p είναι αρκετά μεγάλος.

5.2.3 Πρότυπο Ψηφιακής Υπογαφης – DSS

Το DSS χρησιμοποιεί τη συνάρτηση σύνοψης SHA-1 και παρουσιάζει μία νέα τεχνική για ψηφιακές υπογραφές, τον Αλγόριθμο Digital Signature Algorithm – DSA. Το DSS παρουσιάστηκε αρχικά το 1991, αναθεωρήθηκε το 1993 λαμβάνοντας υπόψη σχόλια σχετικά με την ασφάλεια που παρείχε, ενώ υπήρξε και μία επιπλέον αναθεώρηση το 1996. Το DSS χρησιμοποιεί έναν αλγόριθμο ο οποίος έχει σχεδιαστεί να παρέχει μόνο συνάρτηση ψηφιακής υπογραφής. Αντίθετα από το RSA, δεν μπορεί να χρησιμοποιηθεί για κρυπτογράφηση ή ανταλλαγή κλειδιών.

5.2.4 Κρυπτογραφία Ελλειπτικής Καμπύλης – ECC

Τα περισσότερα προϊόντα και πρότυπα, που χρησιμοποιούν ασύμμετρα κρυπτοσυστήματα για κρυπτογράφηση και ψηφιακή υπογραφή, χρησιμοποιούν τον αλγόριθμο RSA. Το πλήθος των bits που χρησιμοποιείται για ασφαλή χρήση του RSA έχει αυξηθεί σημαντικά τα τελευταία χρόνια και το γεγονός αυτό έχει επιβαρύνει τις αντίστοιχες εφαρμογές με συμαντικό επεξεργαστικό φόρτο. Το πρόβλημα εντείνεται σε περιβάλλον ιστοσελίδων εφαρμογών ηλεκτρονικού εμπορίου, όπου πραγματοποιούνται πολλές ασφαλείς δοσοληψίες. Τα τελευταία χρόνια έχει αρχίσει να αναπτύσσεται ένα ανταγωνιστικό σύστημα του RSA. Πρόκειται για Κρυπτογραφία Ελλειπτικής Καμπύλης (Elliptic Curve Cryptography – ECC). Ήδη, το ECC κινείται στα πλαίσια προτυποποίησης του, αφού έχει συμπεριλέβει το πρότυπο για ασύμμετρα κρυπτοσυστήματα IEEE P 1363.

Ο κύριος λόγος που καθιστά ελκυστικό το ECC συγκρινόμενο με τον αλγόριθμο RSA, είναι ότι προσφέρει το ίδιο επίπεδο ασφάλειας για μικρότερο πλήθος bits, μειώνοντας κατ, αυτόν τον τρόπο τον απαιτούμενο υπολογιστικό χρόνο και φόρτο εργασίας. Σύμφωνα με σχετικά πρόσφατες επιστημονικές ανακοινώσεις, έγινε κατορθωτό να κρυπταναλυθεί το ECC με μέγεθος κλειδιού 109 bits αξιοποιώντας αδιάκοπα την επεξεργαστική ισχύ 10.000 υπολογιστικών επί 549 ημέρες. Στην παρούσα φάση ο αλγόριθμος θεωρείται ασφαλής αν το μέγεθος του κλειδιού διατηρεί μήκος τουλάχιστον 163 bits. Από την άλλη πλευρά, αν και η θεωρία του ECC ήταν γνωστή για αρκετό καιρό, μόλις πρόσφατα έχουν ξεκινήσει να εμφανίζονται προϊόντα που χρησιμοποιούν ECC. Το γεγονός αυτό δικαιολογεί το χαμηλό επίπεδο εμπιστοσύνης προς το ECC, σχετικά με το RSA.

Το ECC σε θεωρητική βάση είναι το πιο δύσκολο να εξηγηθεί, συγκριτικά με τους αλγόριθμους RSA και Diffie-Hellman. Η αξιοποιηθείσα τεχνική βασίζεται στην χρήση ενός μαθηματικού μοντέλου, γνωστού ως ελλειπτική καμπύλη.

5.2.5 Ψηφιακές Υπογραφές

Η ασύμμετρη κρυπτογραφία παρέχει τη δυνατότητα πιστοποίησης της αυθεντικότητας ενός μηνύματος, με την παραγωγή μιας μοναδικής *ψηφιακής υπογραφής* (digital signature). Η ψηφιακή υπογραφή είναι μία ακολουθία χαρακτήρων άμεσα συσχετισμένη με το περιεχόμενο του μηνύματος και την ταυτότητα αυτού που το υπογράφει. Αποστέλλεται μαζί με το μήνυμα και ο παραλήπτης μπορεί, ελέγχοντας την υπογραφή, να βεβαιωθεί ότι το περιεχόμενο του μηνύματος δεν έχει παραποιηθεί και ότι ο αποστολέας του είναι όντως αυτός που ισχυρίζεται ότι είναι. Δηλαδή με λίγα λόγια ψηφιακή υπογραφή είναι η παραγωγή ενός ψηφιακού επιθέματος σε ένα σύνολο

δεδομένων, που πιστοποιεί την ακεραιότητα των δεδομένων και την αποδοχή του υπογράφοντος.

Η κρυπτογράφηση με το ασύμμετρο κρυπτοσύστημα μπορεί να αξιοποιηθεί και με άλλον τρόπο, από αυτόν που απεικονίζεται στο σχήμα 4.7. Υποθέτουμε ότι ο Β επιθυμεί να αποστείλει ένα μήνυμα στον Α. Στις καταγραφείσες απαιτήσεις δεν περιλαμβάνεται πλέον η εμπιστευτικότητα του κειμένου, αλλά ο Α επιθυμεί να είναι σίγουρος για την προέλευση του κειμένου, δηλαδή απαιτείται αυθεντικοποίηση (authenticity) του αποστολέα του μηνύματος. Σε αυτή την περίπτωση, ο Β κρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί. Όταν ο Α παραλάβει το κρυπτογραφημένο μήνυμα, το αποκρυπτογραφεί με το δημόσιο κλειδί του Β, εξασφαλίζοντας έτσι ότι το αρχικό μήνυμα έχει κρυπτογραφηθεί από τον Β. κανένας άλλος δεν κατέχει και δεν γνωρίζει το ιδιωτικό του Β, συνεπώς, κανένας δεν μπορεί να δημιουργήσει κρυπτογραφημένο κείμενο το οποίο να αποκρυπτογραφείται με το δημόσιο κλειδί του Β. Έτσι, όλο το κρυπτογραφημένο κείμενο αποτελεί μία ψηφιακή υπογραφή (digital signature). Επιπλέον, είναι αδύνατον να αλλοιωθεί το μήνυμα χωρίς γνώση του ιδιωτικού κλειδιού του Β, οπότε εξασφαλίζεται αυθεντικοποίηση του αποστολέα, αλλά και ακεραιότητα των δεδομένων.

Ένα πρόβλημα που δημιουργείται σε αυτή την περίπτωση αφορά το χώρο αποθήκευσης: κάθε μήνυμα πρέπει να είναι αποθηκευμένο σε μη κρυπτογραφημένη μορφή για πρακτικούς λόγους. Πρέπει, επίσης, να φυλάσσεται ένα αντίγραφο σε κρυπτογραφημένη μορφή, ώστε η προέλευση και τα περιεχόμενα να μπορούν να προσδιοριστούν εύκολα σε περίπτωση αμφισβήτησης και διαφωνίας. Ένας εύκολος τρόπος για να επιτευχθούν τα ίδια αποτελέσματα, θα ήταν να κρυπτογραφηθεί μικρό τμήμα από bits, το οποίο θα αποτελεί συνάρτηση του κειμένου. Ένα τέτοιο τμήμα ονομάζεται αυθεντικοποιητής (authenticator) και θα πρέπει να είναι αδύνατο να

τροποποιηθεί το μήνυμα, χωρίς να αλλάξει ο αυθεντικοποιητής.αν ο αυθεντικοποιητής κρυπτογραφηθεί με το ιδιωτικό κλειδί του αποστολέα, τότε χαρακτηρίζεται ως ψηφιακή υπογραφή (digital signature). Η περίπτωση αυτή φαίνεται στο σχήμα 4.8. για τη δημιουργία μιας ψηφιακής υπογραφής ενός κειμένου από μία οντότητα, συνήθως κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα η σύνοψη του μηνύματος.

Θα πρέπει να τονιστεί ότι η ψηφιακή υπογραφή δεν προσφέρει εμπιστευτικότητα για το μήνυμα, αλλά αποτελεί υπηρεσία που ικανοποιεί απαιτήσεις ακεραιότητας μηνύματος, αυθεντικοποίησης αποστολέα και μη αποποίησης αποστολής μηνύματος.

5.2.6 Διαχείριση Δημόσιων Κλειδιών

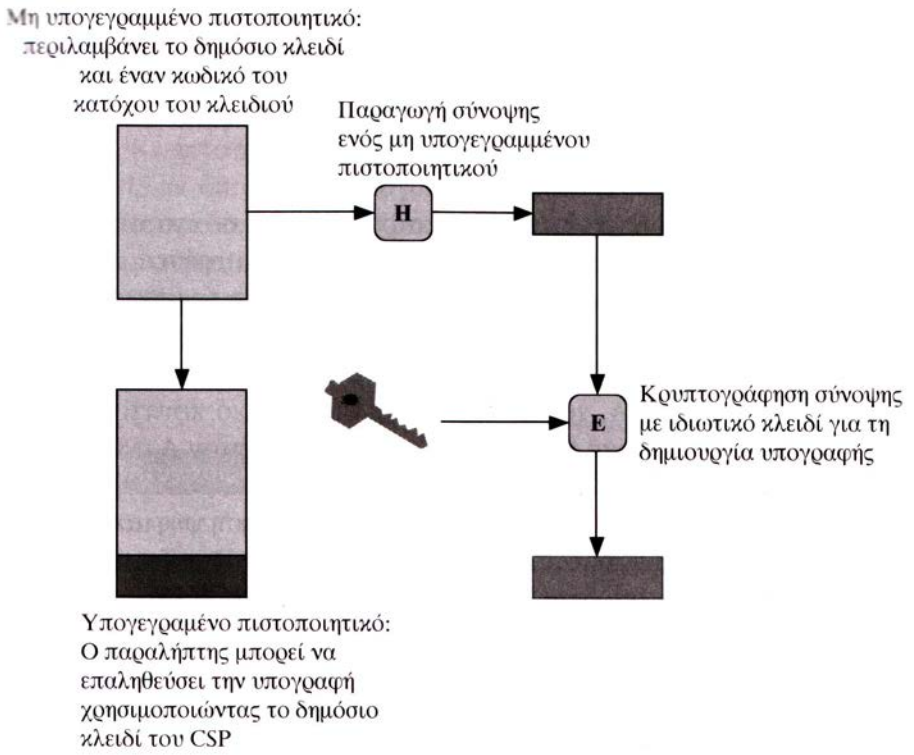
Η διανομή των δημόσιων κλειδιών αποτελεί ένα από τα σημαντικότερα προβλήματα του ασύμμετρου κρυπτοσυστήματος. Υπάρχουν δύο διαφορετικές περιπτώσεις στη διανομή των κλειδιών που παρουσιάζουν ιδιαίτερο ενδιαφέρον:

- Η διανομή των δημόσιων κλειδιών
- Η χρήση του ασύμμετρου κρυπτοσυστήματος για τη διανομή μυστικών κλειδιών, δηλαδή των κλειδιών που χρησιμοποιούνται στο συμμετρικό κρυπτοσύστημα.

5.2.6.1 Ψηφιακά Πιστοποιητικά

Για την αποτελεσματική λειτουργία του ασύμμετρου κρυπτοσυστήματος, το δημόσιο κλειδί πρέπει να μπορεί να είναι γνωστό σε όσους δυνητικά ενδιαφέρονται. Έτσι, υποθέτοντας ότι υπάρχει ένας ευρέως αποδεκτός αλγόριθμος κρυπτογράφησης και αποκρυπτογράφησης όπως ο RSA,

οποιοσδήποτε μπορεί να αποστείλει το δημόσιο κλειδί του σε κάποιον άλλο ή να το μεταδώσει προς όλους. Η μέθοδος αυτή είναι αρκετά χρήσιμη, αλλά έχει μία σημαντική αδυναμία: την αδυναμία διασφάλισης της ακεραιότητας και της αυθεντικοποίησης του αποστολέα κατά την αποστολή του μηνύματος που περιέχει το δημόσιο κλειδί. Οποιοσδήποτε μπορεί να πραγματοποιήσει μία τέτοια μετάδοση. Με τον τρόπ αυτό κάποιος Χ μπορεί να προσποιηθεί ότι είναι ο Α και να στείλει ένα δημόσιο κλειδί σε τρίτον ή να το μεταδώσει προς περισσότερες οντότητες. Μέχρι τη στιγμή που ο Α θα αντιληφθεί ότι βρίσκεται σε εξέλιξη μία απάτη, ο Χ θα έχει διαβάσει όλα τα κρυπτογραφημένα μηνύματα που προορίζονταν για τον Α, ενώ έχει τη δυνατότητα να υπογραφεί και αυθεντικοποιείται ως Α.



Σχήμα 4.8 Ψηφιακές υπογραφές

Λύση σε αυτό το πρόβλημα αποτελεί η χρήση του ψηφιακού πιστοποιητικού (digital certificate) ή απλώς πιστοποιητικού (certificate) δημόσιου κλειδιού. Συγκεκριμένα, ένα πιστοποιητικό περιλαμβάνει το δημόσιο κλειδί του χρήστη και έναν κωδικό (userID) του κατόχου του κλειδιού, υπογεγραμμένα ψηφιακά από μία Έμπιστη Τρίτη Οντότητα (Trusted Third Party – TTP), η οποία συνήθως αποκαλείται Πάροχος Υπηρεσιών Πιστοποίησης (Certification Service Provider – CSP). Ο χρήστης παρουσιάζει το δημόσιο κλειδί του στον CSP με έναν αξιόπιστο τρόπο και λαμβάνει ένα πιστοποιητικό που το περιέχει ή, στη γενική περίπτωση, ο CSP παράγει, αποθηκεύει, διανέμει και ανακαλεί, όταν απαιτείται, τα πιστοποιητικά. Οποιοσδήποτε επιθυμεί να χρησιμοποιήσει το δημόσιο κλειδί του χρήστη μπορεί να λάβει το πιστοποιητικό και να είναι σίγουρος για την ορθότητα του δημόσιου κλειδιού. Η διαδικασία αναπαρίσταται στο Σχήμα 4.8.

Το πιο διαδεδομένο σύστημα πιστοποιητικού είναι το πρότυπο ISO/ITU-T X.509, το οποίο χρησιμοποιείται σε πολλές περιπτώσεις, όπως στην ασφάλεια IP, στο TLS/SSL, στο SET, στο S/MIME κλπ.

5.2.6.2 Διανομή Μυστικών Κλειδιών με Ασύμμετρο Κρυπτοσύστημα

Όπως αναφέρθηκε σε προηγούμενες παραγράφους, σε ένα συμμετρικό κρυπτοσύστημα προκειμένου να επικοινωνήσουν δύο χρήστες πρέπει να διαμοιράζονται τη γνώση ενός μυστικού κλειδιού. Για παράδειγμα, έστω ότι ο Β θέλει να δημιουργήσει μία εφαρμογή που θα του παρέχει τη δυνατότητα να ανταλλάσει μηνύματα με χρήση υπηρεσίας ηλεκτρονικού ταχυδρομείου με τον Α, χρησιμοποιώντας συμμετρικό κρυπτοσύστημα. Θα πρέπει να βρεθεί ένας τρόπος να αποστείλει ο Β στον Α ένα μυστικό κλειδί.

Ένας πολύ διαδεδομένος τρόπος είναι η αξιοποίηση ψηφιακού φακέλου (digital envelope), δηλαδή να χρησιμοποιήσει ο Β ασύμμετρο κρυπτοσύστημα

για την αποστολή του μυστικού κλειδιού. Προφανώς απαιτείται η χρήση πιστοποιητικών και η λειτουργία PKI, ώστε να εξασφαλίζεται η αυθεντικότητα του αποστολέα Α και η ακεραιότητα του μηνύματος. Τα γενικά βήματα που θα πρέπει να ακολουθήσουν σε μία τέτοια περίπτωση είναι τα ακόλουθα:

- Ο Β ετοιμάζει το προς αποστολή μήνυμα.
- Ο Β κρυπτογραφεί το μήνυμα με συμβατικό κρυπτοσύστημα, χρησιμοποιώντας ένα μυστικό κλειδί που ο ίδιος δημιούργησε.
- Ο Β κρυπτογραφεί αυτό το μυστικό κλειδί με το δημόσιο κλειδί του Α.
- Ο Β επισυνάπτει το κρυπτογραφημένο μυστικό κλειδί στο μήνυμα και το αποστέλλει στον Α.

Ο Α είναι ο μόνος που μπορεί να αποκρυπτογραφήσει το μήνυμα και να αναγνώσει το αρχικό κείμενο. Αν ο Β έχει ανακτήσει το δημόσιο κλειδί του Α μέσω πιστοποιητικού από κάποια Έμπιστη Τρίτη Οντότητα, τότε ο Β είναι σίγουρος ότι το μυστικό κλειδί είναι ορθό.

ΣΥΝΟΨΗ

Η κρυπτογραφία και η κρυπτανάλυση ασχολούνται με τη μελέτη, την ανάλυση, την ανάπτυξη και την επαλήθευση κρυπτογραφικών μεθόδων, τεχνικών συστημάτων και πρωτοκόλλων. Αποτελούν από κοινού το επιστημονικό πεδίο της Κρυπτολογίας, τομέα εξαιρετικά κρίσιμο στην προσπάθεια διασφάλισης απαιτήσεων όπως της εμπιστευτικότητας, της ακεραιότητας, της αυθεντικοποίησης και της μη αποποίησης. Οι εφαρμογές της Κρυπτογραφίας αποτελούν το βασικό τεχνολογικό υπόβαθρο σε περιβάλλον δικτύων υπολογιστών για την υλοποίηση των μέτρων αντιμετώπισης απειλών, όπως της υποκλοπής ή τροποποίησης δεδομένων, της παράνομης αναπαραγωγής ψηφιακών εγγράφων και της παραβίασης της

ιδιωτικότητας στο ραγδαία αναπτυσσόμενο περιβάλλον της Κοινωνίας της Πληροφορίας.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η ανάπτυξη ασφαλών συστημάτων που θα είναι φιλικά προς τον χρήστη και στα οποία θα πραγματοποιείται η διακίνηση ευαίσθητων πληροφοριών χωρίς κίνδυνο υποκλοπής ή αλλοίωσης αναμένεται ότι θα συντελέσει στην αύξηση της χρήσης του internet τόσο στον τομέα των εμπορικών συναλλαγών όσο και γενικότερα στις επικοινωνίες.

Ειδικότερα η προστασία των προσωπικών δεδομένων στο πλάίσιο λειτουργίας του ηλεκτρονικού εμπορίου αποτελέι κρίσιμο παράγοντα για την επιτυχημένη εκπλήρωση των στόχων του στην κοινωνία της πληροφορίας. Οι κίνδυνοι προσβολής της προσωπικότητας μπορούν να προστατευθούν με την εφαρμογή των κατάλληλων μέτρων προστασίας κάθε εμπλεκόμενου φορέα σε μία ηλεκτρονική συναλλαγή. Τεχνικές που στοχεύουν στην ανωνυμοποίηση των καναλιών επικοινωνίας, τεχνολογίες ασφάλειας των πληροφοριών και προστασίας της ιδιωτικότητας (όπως η κρυπτογράφηση) είναι άμεσα συνδεδεμένες με ένα επιτυχημένο περιβάλλον ηλεκτρονικού επιχειρείν.

Μικρομεσαίες επιχειρήσεις που χρησιμοποιούν το διαδίκτυο ή δραστηριοποιούνται σε αυτό, δεν έχουν ουσιαστικά άλλη επιλογή από το να υιοθετούν σε μικρό ή μεγάλο βαθμό τεχνικές κρυπτογράφησης.

Βιβλιογραφικές αναφορές

Γκρίτζαλης Σ. – Κάτσικας Σ. – Γκρίτζαλης Δ. «Ασφάλεια Δικτύων Υπολογιστών» Εκδόσεις Παπασωτηρίου

Stallings W., Network Security Essentials: Applications and Standards

Διευθύνσεις στο Internet

http://www.go-online.gr/ebusiness/specials/article.html

http://noc.auth.gr/services/general/rootca/Cryptography

http://www.epmhs.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/kefalaio3.htm

http://ru6.cti.gr/bouras/lessons.php?id=4&action=ergasies