Κεφάλαιο 1.

Βασικές έννοιες στην κρυπτογραφία

Κρυπτογραφία (cryptography) είναι η μελέτη τεχνικών που βασίζονται σε μαθηματικά προβλήματα δύσκολο να λυθούν, με σκοπό την εξασφάλιση της ασφάλειας (εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα) των δεδομένων. *Κρυπτανάλυση* (cryptanalysis) είναι η μελέτη μαθηματικών τεχνικών για την προσβολή κρυπτογραφικών τεχνικών ή υπηρεσιών ασφάλειας και *κρυπτολογία* (cryptology) είναι ο συνδυασμός της κρυπτογραφίας και κρυπτανάλυσης σε ένα ενιαίο επιστημονικό κλάδο.

Εφαρμογή της κρυπτογραφίας είναι η *κρυπτογράφηση*. 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 να εξασφαλίσει 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.

Η κρυπτογραφία παρέχει μηχανισμούς για διαδικασίες ασφάλειας, όπως η *ψηφιακή υπογραφή,* η οποία συνδέει ένα έγγραφο με τον κάτοχο ενός κλειδιού, έτσι ώστε όλοι όσοι είναι σε θέση να το αναγνώσουν, να είναι σίγουροι για το ποιος το έχει γράψει. Επίσης, μία *ψηφιακή χρονοσφραγίδα* (digital timestamp) συνδέει ένα έγγραφο με την ώρα 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.

1.1 Είδη Κρυπτογραφίας

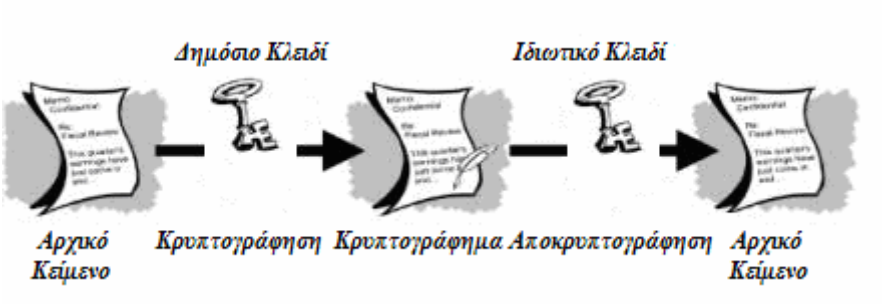
1.1.1 Ασύμμετρη Κρυπτογραφία

Η ασύμμετρη κρυπτογραφία (Public Key Cryptography) χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση. Κάθε χρήστης έχει στην κατοχή του ένα ζεύγος κλειδιών, το ένα καλείται δημόσιο κλειδί (public key) και το άλλο καλείται ιδιωτικό κλειδί (private key). Το δημόσιο κλειδί δημοσιοποιείται, ενώ το ιδιωτικό κλειδί κρατείται πάντοτε μυστικό. Το ιδιωτικό κλειδί δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στο δημόσιο κλειδί. Η ανάγκη ο αποστολέας και ο παραλήπτης να μοιράζονται το ίδιο κλειδί εξαφανίζεται και μαζί και πολλά προβλήματα που θα δούμε παρακάτω. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η διαπιστευμένη και επιβεβαιωμένη συσχέτιση των δημόσιων κλειδιών με τους κατόχους τους, ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστοπροσωπία. Η ασύμμετρη κρυπτογράφηση μπορεί να χρησιμοποιηθεί όχι μόνο για κρυπτογράφηση, αλλά και για παραγωγή ψηφιακών υπογραφών.

Το ιδιωτικό κλειδί είναι μαθηματικά συνδεδεμένο με το δημόσιο κλειδί. Τυπικά, λοιπόν, είναι δυνατόν να "σπάσει" ένα τέτοιο κρυπτοσύστημα ανακτώντας το ιδιωτικό κλειδί από το δημόσιο.

Η κρυπτογράφηση με χρήση της ασύμμετρης κρυπτογραφίας γίνεται ως εξής: όταν ο χρήστης Α θέλει να στείλει ένα μυστικό μήνυμα στο χρήστη Β, χρησιμοποιεί το δημόσιο κλειδί του Β για να κρυπτογραφήσει το μήνυμα και έπειτα το στέλνει στον Β. Ο χρήστης Β, αφού παραλάβει το μήνυμα, κάνει χρήση του ιδιωτικού του κλειδιού για να το αποκρυπτογρα-

φήσει. Κάποιος που παρακολουθεί τη σύνδεση, δεν μπορεί να αποκρυπτογραφήσει το μήνυμα. Όποιος έχει το δημόσιο κλειδί του Β, μπορεί να του στείλει μήνυμα, ενώ μόνο ο Β μπορεί να το διαβάσει, γιατί είναι ο μόνος που γνωρίζει το ιδιωτικό κλειδί.

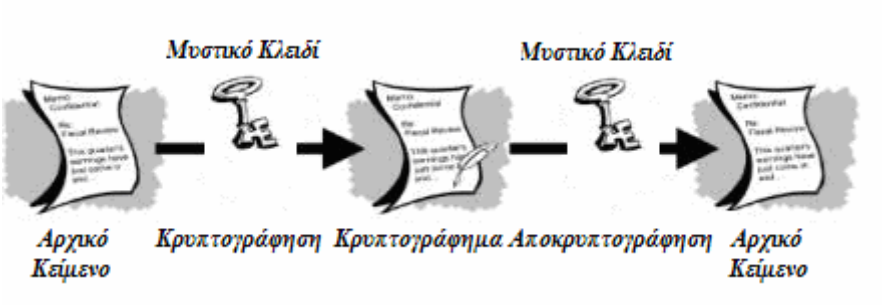


Εικόνα 1. *Ασύμμετρη Κρυπτογραφία*

Όταν ο Α θέλει να χρησιμοποιήσει την ασύμμετρη κρυπτογραφία για να υπογράψει ένα μήνυμα, τότε πραγματοποιεί ένα υπολογισμό που απαιτεί το ιδιωτικό του κλειδί και το ίδιο το μήνυμα. Το αποτέλεσμα του υπολογισμού καλείται ψηφιακή υπογραφή και μεταδίδεται μαζί με το μήνυμα. Για να επαληθεύσει την υπογραφή ο Β πραγματοποιεί ανάλογο υπολογισμό χρησιμοποιώντας το δημόσιο κλειδί του Α, το μήνυμα και την υπογραφή. Εάν το αποτέλεσμα είναι θετικό, τότε η υπογραφή είναι αυθεντική. Διαφορετικά η υπογραφή είναι πλαστή ή το μήνυμα έχει τροποποιηθεί. Αλγόριθμοι ασύμμετρης κρυπτογραφίας θα αναλυθούν στην παράγραφο 2.5.1.

1.1.2 Συμμετρική Κρυπτογραφία

Στη *συμμετρική* κρυπτογραφία (Symmetric Cryptography ή Secret -Key Cryptography) ο αποστολέας και ο παραλήπτης ενός μηνύματος γνωρίζουν και χρησιμοποιούν το ίδιο *μυστικό κλειδί* (secret key). Ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να αποκρυπτογραφήσει το μήνυμα. Αυτή η μέθοδος καλείται συμμετρική κρυπτογραφία ή κρυπτογραφία μυστικού κλειδιού. Η συμμετρική κρυπτογραφία χρησιμοποιείται όχι μόνο για κρυπτογράφηση, άλλα και για πιστοποίηση ταυτότητας. Μία τέτοια τεχνική είναι η Message Authentication Code (MAC), η οποία θα περιγραφεί στην παράγραφο 1.3.4.



Εικόνα 2. *Συμμετρική Κρυπτογραφία*

Το κύριο πρόβλημα της συμμετρικής κρυπτογραφίας είναι η συνεννόηση του αποστολέα και του παραλήπτη στο κοινό μυστικό κλειδί που θα κρυπτογραφεί και αποκρυπτογραφεί όλη τη διακινούμενη πληροφορία, χωρίς κάποιον άλλο να λάβει γνώση αυτού. Πλεονέκτημα της είναι ότι είναι ταχύτερη από την ασύμμετρη κρυπτογραφία. Συγκεκριμένοι αλγόριθμοι θα παρουσιαστούν στην παράγραφο 2.5.2.

1.1.3 Μειονεκτήματα και Πλεονεκτήματα

Το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας, όπως αναφέραμε περιληπτικά προηγουμένως, είναι η συνεννόηση και ανταλλαγή του κλειδιού, χωρίς κάποιος τρίτος να μάθει για αυτό. Η μετάδοση μέσα από το Διαδίκτυο δεν είναι ασφαλής, γιατί οποιοσδήποτε γνωρίζει για τη συναλλαγή μπορεί να καταγράψει όλη την επικοινωνία μεταξύ αποστολέα και παραλήπτη και να αποκτήσει το κλειδί. Έπειτα, μπορεί να διαβάσει, να τροποποιήσει και να πλαστογραφήσει όλα τα μηνύματα που ανταλλάσσουν οι δύο ανυποψίαστοι χρήστες. Βέβαια, μπορούν να βασισθούν σε άλλο μέσο επικοινωνίας για τη μετάδοση του κλειδιού (π.χ. τηλεφωνία), αλλά ακόμα και έτσι δεν μπορεί να εξασφαλιστεί ότι κανείς δεν παρεμβάλλεται μεταξύ της γραμμής επικοινωνίας των χρηστών. Η ασύμμετρη κρυπτογραφία δίνει λύση σε αυτό το πρόβλημα, αφού σε καμία περίπτωση δεν μεταφέρονται στο δίκτυο οι εν λόγω ευαίσθητες πληροφορίες με την αρχική τους μορφή.

Άλλο ένα ακόμα πλεονέκτημα των ασύμμετρων κρυπτοσυστημάτων είναι ότι μπορούν να παρέχουν ψηφιακές υπογραφές που δεν μπορούν να αποκηρυχθούν από την πηγή τους. Η πιστοποίηση ταυτότητας μέσω συμμετρικής κρυπτογράφησης απαιτεί την κοινή χρήση του ίδιου κλειδιού και πολλές φορές τα κλειδιά αποθηκεύονται σε υπολογιστές που

κινδυνεύουν από εξωτερικές επιθέσεις. Σαν αποτέλεσμα, ο αποστολέας μπορεί να αποκηρύξει ένα πρωτύτερα υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι το μυστικό κλειδί είχε κατά κάποιον τρόπο αποκαλυφθεί. Στην ασύμμετρη κρυπτογραφία δεν επιτρέπεται κάτι τέτοιο, αφού κάθε χρήστης έχει αποκλειστική γνώση του ιδιωτικού του κλειδιού και είναι δικιά του ευθύνη η φύλαξή του.

Μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα. Κατά κανόνα, οι διαδικασίες κρυπτογράφησης και πιστοποίησης ταυτότητας με συμμετρικό κλειδί είναι σημαντικά ταχύτερες από την κρυπτογράφηση και ψηφιακή υπογραφή με ζεύγος ασύμμετρων κλειδιών. Η ιδιότητα αυτή καλείται διασφάλιση της μη αποκήρυξης της πηγής (non-repudiation). Επίσης, τεράστιο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλειδιών από οργανισμούς Πιστοποίησης (Certificate Authority) ώστε να διασφαλίζεται η κατοχή των νόμιμων χρηστών. Όταν κάποιος επιτήδειος κατορθώσει και ξεγελάσει τον οργανισμό, μπορεί να συνδέσει το όνομά του με το δημόσιο κλειδί ενός νόμιμου χρήστη και να προσποιείται την ταυτότητα αυτού του νόμιμου χρήστη.

Σε μερικές περιπτώσεις, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη και η συμμετρική κρυπτογραφία από μόνη της είναι αρκετή. Τέτοιες περιπτώσεις είναι περιβάλλοντα κλειστά (π.χ. στρατός), που δεν έχουν σύνδεση με το Διαδίκτυο. Ένας υπολογιστής μπορεί να κρατά τα μυστικά κλειδιά των χρηστών που επιθυμούν να εξυπηρετηθούν από αυτόν, μια και δεν υπάρχει ο φόβος για κατάληψη της μηχανής από εξωτερικούς παράγοντες. Επίσης, στις περιπτώσεις που οι χρήστες μπορούν να συναντηθούν και να ανταλλάξουν τα κλειδιά ή όταν η κρυπτογράφηση χρησιμοποιείται για τοπική αποθήκευση κάποιων αρχείων, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη.

Τα δύο κρυπτοσυστήματα μπορούν να εφαρμοστούν μαζί, συνδυάζοντας τα καλά τους χαρακτηριστικά και εξαλείφοντας τα μειονεκτήματα τους. Ένα παράδειγμα τέτοιου συνδυασμού είναι οι ψηφιακοί φάκελοι, που παρουσιάζονται στην παράγραφο 1.6.4.

1.2 Κρυπτογραφικά Εργαλεία

Μέχρι τώρα αναφερθήκαμε στα δύο σημαντικότερα κρυπτοσυστήματα που ευρέως εφαρμόζονται σήμερα. Περιγράψαμε τις αρχές που τα διέ-

πουν και το είδος των κλειδιών που χρησιμοποιούν (συμμετρικά ή ασύμμετρα). Στις ακόλουθες παραγράφους θα ασχοληθούμε με τους μηχανισμούς με τους οποίους εφαρμόζεται η κρυπτογραφία γενικότερα.

1.2.1 Κώδικες Τμήματος

Ο *Κώδικας Τμήματος* (Block Cipher) είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης που μετατρέπει ένα τμήμα (block) μη κρυπτογραφημένου καθορισμένου μήκους κειμένου (plaintext), σε τμήμα (block) κρυπτογραφημένου (ciphertext). Αυτός ο μετασχηματισμός πραγματοποιείται με την βοήθεια ενός μυστικού κλειδιού που δίνεται από το χρήστη. Η αποκρυπτογράφηση γίνεται με την εφαρμογή του αντίστροφου μετασχηματισμού στο κρυπτογραφημένο κείμενο χρησιμοποιώντας το ίδιο μυστικό κλειδί. Το καθορισμένο μήκος καλείται μήκος τμήματος (block size) (64,128,196... bits). Κάθε κείμενο δίνει διαφορετικό κρυπτογραφημένο κείμενο (ciphertext).

Οι κώδικες τμήματος (block ciphers) λειτουργούν επαναληπτικά, κρυπτογραφώντας ένα τμήμα διαδοχικά αρκετές φορές. Σε κάθε γύρο, ο ίδιος μετασχηματισμός εφαρμόζεται στα δεδομένα χρησιμοποιώντας ένα υποκλειδί (subkey). Το σύνολο των υποκλειδιών προέρχεται από το μυστικό κλειδί που παρείχε ο χρήστης, με ειδική συνάρτηση. Το σύνολο των υποκλειδιών καλείται σχεδιασμός κλειδιών (key schedule).

Ο αριθμός των επαναλήψεων του επαναληπτικού κρυπτοσυστήματος εξαρτάται από το επίπεδο της επιθυμητής ασφάλειας και την απόδοση του συστήματος. Στις περισσότερες περιπτώσεις, ο αυξημένος αριθμός επαναλήψεων βελτιώνει την προσφερόμενη ασφάλεια, αλλά για μερικά κρυπτοσυστήματα ο αριθμός των επαναλήψεων για να επιτευχθεί ικανοποιητική ασφάλεια θα είναι πολύ μεγάλος για να πραγματοποιηθεί.

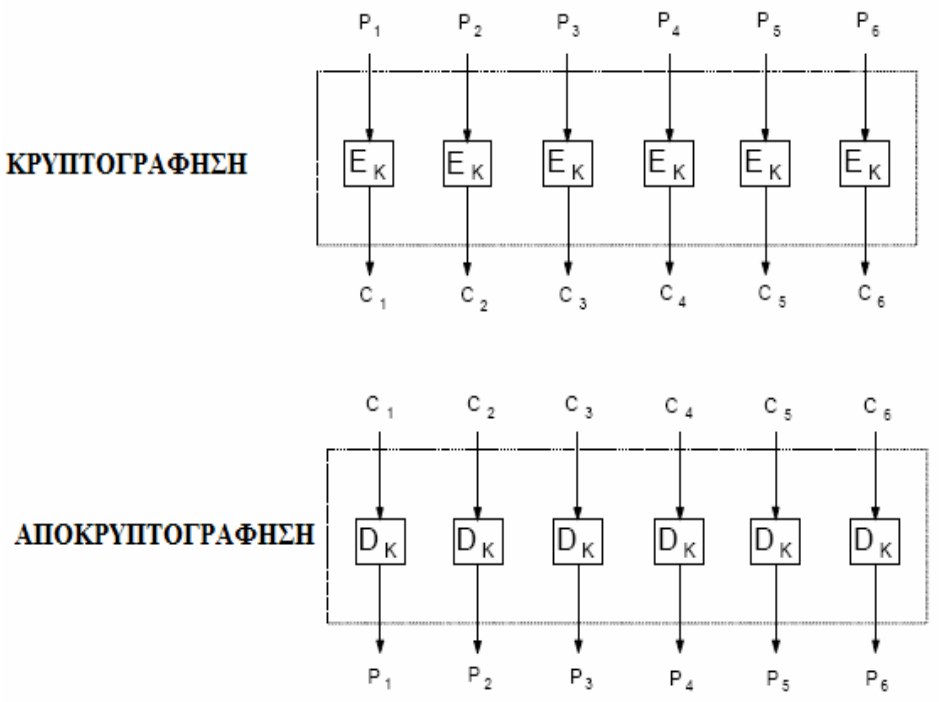
Τα Feistel κρυπτοσυστήματα είναι ειδικές περιπτώσεις επαναληπτικών κρυπτοσυστημάτων όπου το κρυπτογραφημένο κείμενο υπολογίζεται ως εξής: το κείμενο χωρίζεται στο μισό. Η συνάρτηση f εφαρμόζεται στο ένα μισό με χρήση ενός υποκλειδιού και η έξοδος της f περνάει από λογική πράξη X-OR με το άλλο μισό. Έπειτα, το αποτέλεσμα της λογικής πράξης γίνεται είσοδος της f και το προηγούμενο μισό το οποίο μετασχηματίστηκε γίνεται μία από τις εισόδους της επόμενης XOR. Η άλλη είσοδος της XOR είναι το αποτέλεσμα του δεύτερου μετασχηματισμού, ο οποίος χρησιμοποιεί νέο υποκλειδί. Ο αλγόριθμος συνεχίζεται με το ίδιο

τρόπο. Στο τέλος της τελευταίας επανάληψης, τα δύο κρυπτογραφημένα μισά συνενώνονται.

Ένα σημαντικό χαρακτηριστικό του Feistel είναι ότι η αποκρυπτογράφηση είναι δομικά ταυτόσημη με την κρυπτογράφηση. Τα υποκλειδιά χρησιμοποιούνται σε αντίστροφη σειρά στην αποκρυπτογράφηση.

1.2.2 Τρόποι Λειτουργίας

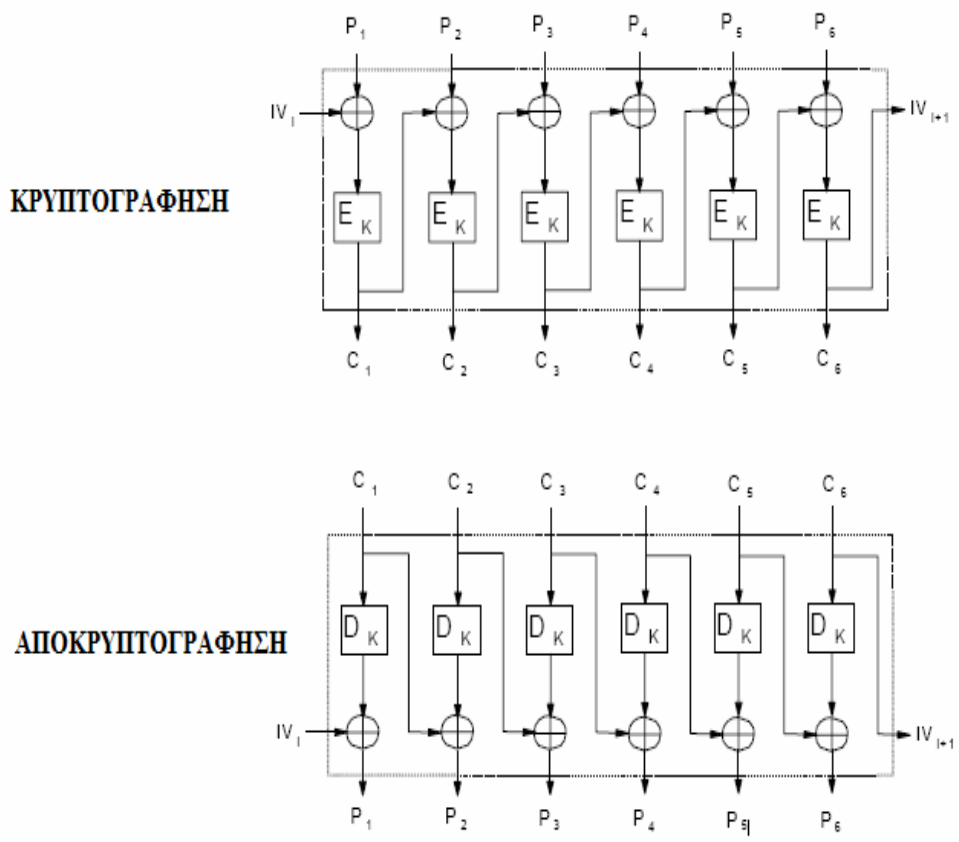
Ένας αλγόριθμος τύπου κώδικα τμήματος έχει διάφορους τρόπους λειτουργίας. Κάθε τρόπος λειτουργίας μπορεί να έχει τις δικές του ιδιότητες εκτός από αυτές που κληρονομεί από τον βασικό κρυπτοσυστήματος. Οι βασικοί τρόποι λειτουργίας είναι: ο Electronic Code Book (ECB), ο Cipher Block Chaining (CBC), ο Cipher Feedback (CFB) και ο Output Feedback (OFB).



Εικόνα 3. *Electronic Code Book (ECB)*

Σε ECB mode, το κείμενο χωρίζεται σε ισομήκη τμήματα. Κάθε μη κρυπτογραφημένο τμήμα κρυπτογραφείται ανεξάρτητα από την συνάρτηση του βασικού κώδικα τμήματος. Μειονέκτημα αυτού του τρόπου είναι ότι

ομοιότητες του αρχικού κειμένου δεν καλύπτονται. Τα αποκρυπτογραφημένα τμήματα (plaintext block) που είναι ταυτόσημα, δίνουν ταυτόσημα κρυπτογραφημένα τμήματα (ciphertext block) και το κείμενο μπορεί εύκολα να τροποποιηθεί με την αφαίρεση, πρόσθεση ή και ανακατάταξη των όμοιων κρυπτογραφημένων τμημάτων. Η ταχύτητα της κρυπτογράφησης κάθε αρχικό τμήμα είναι ίδια με την ταχύτητα του κώδικα τμήματος. Ο ECB επιτρέπει την παράλληλη παραγωγή των κρυπτογραφημένων τμημάτων για καλύτερη απόδοση.

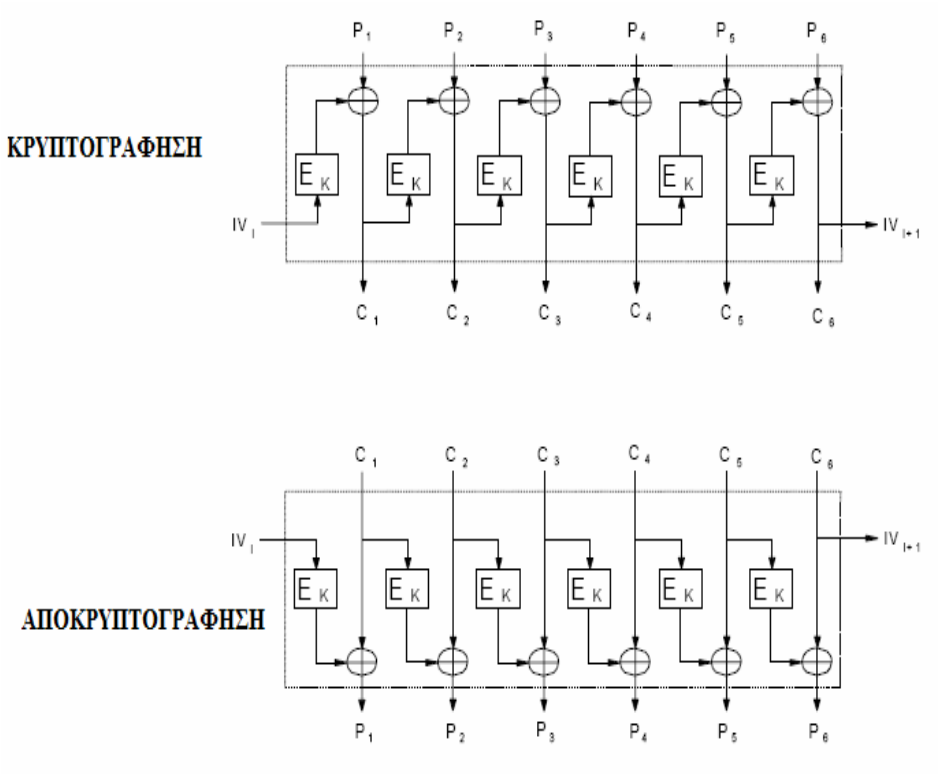


Εικόνα 4. *Cipher Block Chaining (CBC)*

Σε CBC mode, κάθε μη κρυπτογραφημένο block συνδυάζεται μέσω της λογικής πράξης XOR με το πρωτύτερα κρυπτογραφημένο block. Το αποτέλεσμα κρυπτογραφείται. Απαιτείται μια αρχική τιμή για την πρώτη XOR πράξη που καλείται Διάνυσμα Αρχικοποίησης (Initialization Vector), c_0. Τα όμοια αρχικά τμήματα καλύπτονται με την χρήση της λο-

γικής πράξης και αυξάνεται η ασφάλεια του αλγόριθμου. Η ταχύτητα της κρυπτογράφησης είναι ίδια με αυτή του κώδικα τμήματος, αλλά η διαδικασία δεν μπορεί να πραγματοποιηθεί παράλληλα παρ' όλο που η αποκρυπτογράφηση μπορεί.

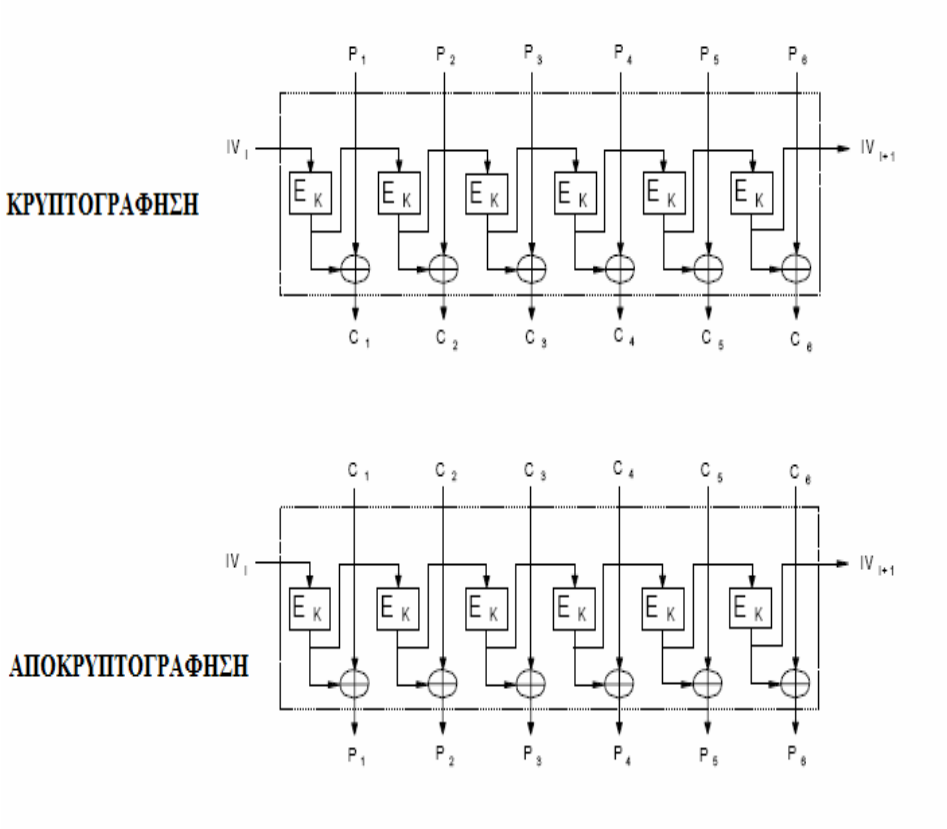
Σε CFB mode, το προηγούμενο κρυπτογραφημένο τμήμα κρυπτογραφείται και το αποτέλεσμα που παράγεται συνδυάζεται με το επόμενο αρχικό τμήμα με χρήση μιας XOR. Η έξοδος της XOR αποτελεί το νέο κρυπτογραφημένο τμήμα που θα κρυπτογραφηθεί, συνεχίζοντας την διαδικασία. Γίνεται η ποσότητα που χρησιμοποιείται για ανάδραση (feedback) να μην είναι ένα πλήρες τμήμα. Απαιτείται ένα Διάνυσμα Αρχικοποίησης c_0 για την πρώτη XOR πράξη.



Εικόνα 5. *Cipher Feedback (CFB)*

Με αυτόν τον τρόπο καλύπτονται πιθανές ομοιότητες στα αρχικά τμήματα μέσω της XOR. Γίνεται, όμως, στην πλήρη ανάδραση τα c_i και c_{i-1} να είναι ταυτόσημα. Σαν συνέπεια και το επόμενο ζεύγος κρυπτογραφημένων block θα είναι ταυτόσημα μεταξύ τους. Αυτό το πρόβλημα λύνεται

με την χρήση μερικής ανάδρασης. Η ταχύτητα της κρυπτογράφησης είναι ίδια με αυτή του block cipher και δεν επιτρέπεται παράλληλη επεξεργασία.



Εικόνα 6. *Output Feedback (OFB)*

Σε OFB mode, η διαδικασία είναι παρόμοια με αυτήν του CFB mode, με την διαφορά ότι η ποσότητα που συνδυάζεται με XOR με κάθε αρχικό τμήμα παράγεται ανεξάρτητα από τα αρχικά και κρυπτογραφημένα. Ένας Διάνυσμα Αρχικοποίησης s_0 χρειάζεται για να ξεκινήσει την διαδικασία και κάθε τμήμα si προκύπτει από την κρυπτογράφηση του προηγούμενου s_{i-1}. Η κρυπτογράφηση του αρχικού τμήματος γίνεται με τον συνδυασμό κάθε αρχικού τμήματος μέσω μιας XOR, με το κρυπτογραφημένο s.

Ο OFB mode έχει το εξής πλεονέκτημα σε σχέση με τον CFB. Τα πιθανά λάθη μετάδοσης δεν πολλαπλασιάζονται κατά την αποκρυπτογράφηση

και έτσι δεν την επηρεάζουν. Το κείμενο, όμως, μπορεί εύκολα να αλλοιωθεί με την αφαίρεση, πρόσθεση ή και ανακατάταξη όμοιων κρυπτογραφημένων τμημάτων. Δεν είναι δυνατή η παράλληλη επεξεργασία, αλλά η διαδικασία μπορεί να επιταχυνθεί με την παραγωγή των κρυπτογραφημένων s πριν τα δεδομένα να είναι διαθέσιμα για κρυπτογράφηση.

Άλλος ένας τρόπος λειτουργίας είναι ο Propagating Cipher Block Chaining (PCBC). Χρησιμοποιείται με πρωτόκολλα όπως το Kerberos version 4, ενώ δεν έχει επίσημα τυποποιηθεί ούτε χαίρει παγκόσμιας αναγνώρισης. Είναι παρόμοιος με το CBC και έχει σχεδιασθεί με σκοπό να αναπαράγει το πιθανό λάθος μετάδοσης, έτσι ώστε να γίνεται αντιληπτό και το κείμενο που προκύπτει να απορρίπτεται.

1.2.3 Κώδικες Ροής

Ο Κώδικας Ροής (stream cipher) είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης. Είναι εξαιρετικά ταχείς αλγόριθμοι, κατά πολύ ταχύτεροι από τους κώδικες τμήματος. Σε αντίθεση με τους κώδικες τμήματος που λειτουργούν με μεγάλα κομμάτια δεδομένων (blocks), οι κώδικες ροής τυπικά λειτουργούν με μικρότερες μονάδες απλού κειμένου, συνήθως με bits. Η κρυπτογράφηση ενός συγκεκριμένου κειμένου με έναν κώδικα τμήματος θα καταλήγει πάντα στο ίδιο αποτέλεσμα όταν χρησιμοποιείται το ίδιο κλειδί. Με έναν κώδικα ροής, ο μετασχηματισμός των μικρότερων αυτών μονάδων θα ποικίλει, ανάλογα με πότε αντιμετωπίζονται κατά την διάρκεια της κρυπτογράφησης.

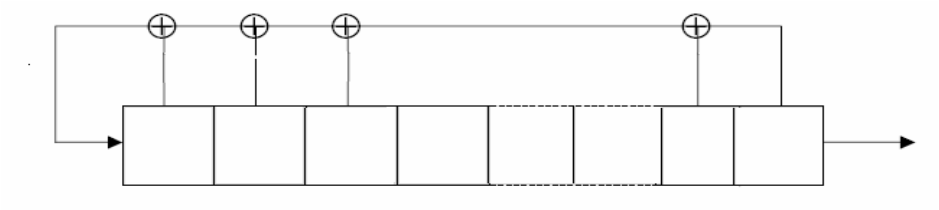
Ένας κώδικας ροής παράγει μια ακολουθία από bits που χρησιμοποιείται σαν κλειδί και καλείται keystream. Η κρυπτογράφηση επιτυγχάνεται με τον συνδυασμό του keystream με το αρχικό μη κρυπτογραφημένο κείμενο, συνήθως μέσω της XOR πράξης. Η παραγωγή του keystream μπορεί να είναι ανεξάρτητη του αρχικού κειμένου και του κρυπτογραφήματος (συγχρονισμένοι κώδικες ροής (synchronous stream cipher)) ή μπορεί να εξαρτάται από αυτά (ασύγχρονοι κώδικες ροής (self-synchronizing stream cipher)).

1.2.4 One-time Pads

Οι κώδικες ροής βασίζονται στις θεωρητικές ιδιότητες ενός one-time pad. One-time pads (καμιά φορά καλούνται και Vernam κρυπτοσυστήματα) είναι τα κρυπτοσυστήματα που χρησιμοποιούν μια ακολουθία bits (keystream) που παράγεται τελείως στην τύχη. Η ακολουθία των bits εί-

ναι του ίδιου μήκους με το μη κρυπτογραφημένο κείμενο και συνδυάζεται μέσω μιας XOR πράξης με το αυτό για την παραγωγή του κρυπτογραφήματος. Επειδή η ακολουθία των bits είναι τελείως τυχαία και είναι του ίδιου μήκους με το αρχικό κείμενο, η εύρεση του κειμένου είναι αδύνατη ακόμα και με τη διάθεση τεράστιας υπολογιστικής ισχύος. Ένα τέτοιο κρυπτοσύστημα προσφέρει τέλεια μυστικότητα και ασφάλεια και έχει χρησιμοποιηθεί σε μεγάλη κλίμακα σε καιρό πολέμου για τη διασφάλιση διπλωματικών καναλιών. Το γεγονός, όμως, ότι το μυστικό κλειδί (δηλαδή το keystream), που χρησιμοποιείται μόνο μία φορά, είναι του ίδιου μήκους με το μήνυμα, εισάγει σημαντικό πρόβλημα στη διαχείριση του κλειδιού. Παρ' όλη την ασφάλεια που προσφέρει, ο one-time pad δεν μπορεί να εφαρμοστεί στην πράξη.

Οι κώδικες ροής αναπτύχθηκαν σαν μια προσέγγιση της λειτουργίας ενός one-time pad. Βέβαια, παρά το γεγονός ότι δεν είναι σε θέση να παρέχουν τη θεωρητική ασφάλεια ενός time-pad, είναι τουλάχιστον πρακτικοί. Ο πιο ευρέως χρησιμοποιούμενος κώδικας ροής είναι ο RC4. Ενδιαφέρον παρουσιάζει το γεγονός ότι συγκεκριμένοι τρόποι λειτουργίας ενός block cipher προσομοιάζουν ένα κώδικα ροής όπως για παράδειγμα ο DES σε CFB και OFB modes. Ακόμα και έτσι, οι αυθεντικοί κώδικες ροής είναι αρκετά ταχύτεροι.



Εικόνα 7. *Γραμμικός Καταχωρητής Ολίσθησης (Linear Feedback Shift Register –LFSR-)*

Ένας μηχανισμός για την παραγωγή του keystream είναι ο Γραμμικός Καταχωρητής Ολίσθησης (Linear Feedback Shift Register (LFSR)). Ο καταχωρητής αποτελείται από μία σειρά κελιών (cells) το καθένα από τα οποία αποτελείται από ένα bit. Τα περιεχόμενα των κελιών καθορίζονται από ένα Διάνυσμα Αρχικοποίησης (Initialization Vector) που λειτουργεί σαν το μυστικό κλειδί. Το keystream δεν αποτελεί πλέον το μυστικό κλειδί (όπως στους one-time pads) λόγω του μεγέθους του. Η συμπεριφορά του καταχωρητή ρυθμίζεται από ένα ρολόι και σε κάθε χρονική στιγμή τα bits μετακινούνται μία θέση δεξιά, την στιγμή που το XOR

αποτέλεσμα μερικών από αυτών τοποθετείται στο αριστερότερο κελί. Κάθε αλλαγή του ρολογιού δίνει ένα bit εξόδου.

Η κατασκευή των LFSR είναι εύκολη τόσο υπό μορφή λογισμικού (software) όσο και υπό μορφή υλικού (hardware), ενώ η λειτουργία τους είναι ταχύτατη. Οι ακολουθίες bit, όμως, που δημιουργούνται από ένα και μοναδικό LFSR δεν είναι ασφαλείς, καθ' ότι τον τελευταίο καιρό έχει αναπτυχθεί δυνατή μαθηματική φόρμουλα που επιτρέπει την ανάλυση του μηχανισμού και εύρεση του keystream. Απαιτείται, λοιπόν, η συνδυασμένη χρήση πολλών LFSRs.

Ένας Shift Register Cascade αποτελεί ένα σύνολο από LFSRs που συνδέονται μεταξύ τους με τέτοιο τρόπο ώστε η συμπεριφορά του ενός να εξαρτάται από την συμπεριφορά του άλλου. Αυτό επιτυγχάνεται συνήθως με τη χρήση του ενός LFSR να ελέγχει το ρολόι του άλλου. Άλλο παράδειγμα τέτοιου συνδυασμού είναι ο Shrinking Generator που αναπτύχθηκε από τους Coppersmith, Krawczyk και Mansour. Βασίζεται στην αλληλεπίδραση των εξόδων δύο LFSRs. Τα bits της μιας εξόδου χρησιμοποιούνται για να καθορίσουν, μέσω κατάλληλης τεχνικής, εάν τα bits της δεύτερης εξόδου θα συμπεριληφθούν στο keystream. Είναι απλός και έχει καλά χαρακτηριστικά ασφαλείας.

1.2.5 Συναρτήσεις Κατακερματισμού

Ο όρος *συνάρτηση κατακερματισμού* (hash function) *h* υποδηλώνει ένα μετασχηματισμό που παίρνει ως είσοδο ένα μήνυμα *m* οποιουδήποτε μήκους και επιστρέφει στην έξοδο μία ακολουθία χαρακτήρων *h(m)* περιορισμένου μήκους που καλείται τιμή κατακερματισμού (hash value). Οι συναρτήσεις κατακερματισμού είναι συναρτήσεις με τις εξής ιδιότητες:

- Η είσοδος είναι οποιουδήποτε μήκους.
- Η έξοδος έχει περιορισμένο μήκος.
- Δεδομένου του *m*, ο υπολογισμός του *h(m)* είναι εύκολος.
- Η *h* είναι μη αντιστρέψιμη.
- Η h δεν είναι αμφιμονοσήμαντη (ένα προς ένα συνάρτηση).

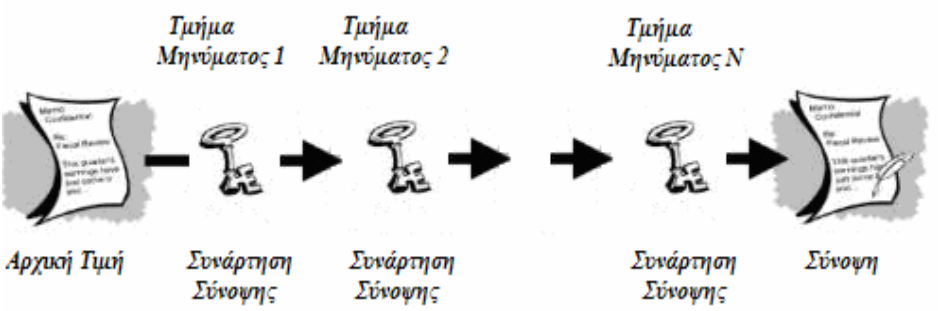
Η τιμή κατακερματισμού παρουσιάζει συνοπτικά το μεγαλύτερο μήνυμα ή έγγραφο, για αυτό καλείται και σύνοψη μηνύματος (message digest). Μπορούμε να φανταστούμε τη σύνοψη του μηνύματος σαν "ψηφιακό

αποτύπωμα" ("digital fingerprint") του εγγράφου. Παραδείγματα γνωστών συναρτήσεων κατακερματισμού είναι οι MD2, MD5 και SHA.

Εικόνα 8. *Συνάρτηση Κατακερματισμού (hash function)*

Η ψηφιακή υπογραφή των μηνυμάτων παράγεται με την εφαρμογή κρυπτογραφικών διαδικασιών στη σύνοψη του μηνύματος, το οποίο είναι πιο μικρό και εύκολο στη διαχείριση. Επιπλέον ένα μήνυμα σύνοψης μπορεί να δημοσιοποιηθεί χωρίς να αποκαλύπτει τα περιεχόμενα του αυθεντικού κειμένου.

Οι Damgard και Merkle εισήγαγαν την έννοια του *συναρτήσεων συμπίεσης* (compression function). Αυτές οι συναρτήσεις παίρνουν είσοδο καθορισμένου μήκους και δίνουν έξοδο μικρότερου, περιορισμένου μήκους. Δεδομένης μίας συνάρτησης κατακερματισμού, μια συνάρτηση συμπίεσης μπορεί να πραγματοποιηθεί με την επανειλημμένη εφαρμογή της συναρτήσεων σύνοψης, έως ότου ολόκληρο το μήνυμα έχει επεξεργαστεί. Πιο αναλυτικά, το μήνυμα τεμαχίζεται σε τμήματα (blocks), των οποίων το μέγεθος εξαρτάται από τη συνάρτηση σύνοψης και συμπληρώνεται (padded) για λόγους ασφαλείας, ώστε το μήκος του μηνύματος να είναι πολλαπλάσιο του μήκους του block. Το παρακάτω σχήμα επιδεικνύει τη λογική της διαδικασίας.



Εικόνα 9. *Συνάρτηση Συμπίεσης*

1.2.6 Message Authentication Code (MAC)

Message Authentication Code είναι ένα κώδικας (καλείται και άθροισμα ελέγχου-checksum) που συνοδεύει το μήνυμα και πιστοποιεί την ταυτότητα του αποστολέα και την ακεραιότητα του μηνύματος. Για την παραγωγή τους εφαρμόζεται στο μήνυμα ένα από τα προαναφερθέντα κρυπτογραφικά εργαλεία σε συνδυασμό με ένα μυστικό κλειδί. Σε αντίθεση με τις ψηφιακές υπογραφές, τα MACs υπολογίζονται και επαληθεύονται με το ίδιο κλειδί, έτσι ώστε να μπορούν να επαληθευθούν μόνο από τον προοριζόμενο παραλήπτη. Υπάρχουν τέσσερις τύποι MAC: (1) τα άνευ όρων ασφαλή, (2) τα βασιζόμενα σε συναρτήσεις κατακερματισμού, (3) τα βασιζόμενα σε κώδικες ροής και (4) τα βασιζόμενα σε κώδικες τμημάτων.

1. Οι Simmons και Stinson πρότειναν έναν άνευ όρων ασφαλή MAC βασισμένο στην κρυπτογράφηση με ένα one-time pad. Όπως είπαμε, όμως, επειδή το κλειδί ενός one-time pad είναι πολύ μεγάλο, δεν χρησιμοποιούνται στην πράξη, γι' αυτό το λόγο δεν θα προχωρήσουμε σε περαιτέρω ανάλυσή τους.

2. Τα MACs που βασίζονται σε συναρτήσεις κατακερματισμού χρησιμοποιούν ένα μυστικό κλειδί σε συνδυασμό με μια συνάρτηση κατακερματισμού για να παράγουν το άθροισμα ελέγχου που συνοδεύει το μήνυμα. Το κλειδί χρησιμοποιείται για να κρυπτογραφήσει τη σύνοψη μηνύματος. Ο παραλήπτης του μηνύματος, που μοιράζεται με τον αποστολέα το ίδιο κλειδί, αποκρυπτογραφεί το μήνυμα σύνοψης (message digest) και έπειτα το συγκρίνει με ένα μήνυμα σύνοψης που παράγει ο ίδιος από το μήνυμα. Εάν η σύγκριση είναι επιτυχής, τότε ο παραλήπτης σιγουρεύεται ότι τα δεδομένα δεν έχουν αλλοιωθεί. Ένα παράδειγμα είναι ο keyed-MD5.

3. Τα MACs που βασίζονται σε κώδικες ροής αναπτύχθηκαν από τους Lai, Rueppel και Woolven. Στο αλγόριθμο που ανέπτυξαν, ένας αποδεδειγμένα ασφαλής κώδικα ροής, χρησιμοποιείται για να χωρίσει το μήνυμα σε δύο substreams καθένα από τα οποία τροφοδοτείται σε ένα LFSR. Το άθροισμα ελέγχου αποτελεί την τελική κατάσταση των δύο LFSRs.

4. Τέλος, τα MAC μπορούν να δημιουργηθούν από κώδικες τμήματος, όπως τον DES-CBC. Σε αυτήν τη μέθοδο, το μήνυμα κρυπτογραφείται με εφαρμογή του αλγόριθμου κώδικα τμήματος. Το τελευταίο

κρυπτογραφημένο τμήμα που δίνει ο αλγόριθμος αποτελεί το άθροισμα ελέγχου του μηνύματος.

1.2.7 Μηχανισμοί Διαχείρισης και Ανταλλαγής Κλειδιών

Οι μηχανισμοί διαχείρισης κλειδιών (key management) και ανταλλαγής κλειδιών (key exchange), ασχολούνται με την ασφαλή παραγωγή, διανομή και αποθήκευση των κλειδιών κρυπτογράφησης. Η εύρεση απρόσβλητων μεθόδων διαχείρισης και ανταλλαγή κλειδιών είναι πολύ σημαντική στη διατήρηση της ασφάλειας της επικοινωνίας.

Η έννοια της διαχείρισης κλειδιών αναφέρεται στα ασύμμετρα κρυπτοσυστήματα. Τα χαρακτηριστικά που πρέπει να έχει ένας μηχανισμός διαχείρισης κλειδιών είναι τα ακόλουθα. Οι χρήστες πρέπει να είναι σε θέση να μπορούν να αποκτήσουν με ασφάλεια ένα ζεύγος δημόσιου – ιδιωτικού κλειδιού που θα ικανοποιεί τις ανάγκες τους για προστατευμένη επικοινωνία. Πρέπει να υπάρχει τρόπος αποθήκευσης και δημοσιοποίησης των δημόσιων κλειδιών, ενώ παράλληλα θα είναι δυνατή η ανάκτησή τους όποτε χρειάζεται. Επίσης τα δημόσια κλειδιά θα πρέπει να συσχετίζονται με σίγουρο τρόπο με την ταυτότητα του νόμιμου κατόχου. Έτσι, δεν θα μπορεί κάποιος να παρουσιάζεται σαν κάποιος άλλος, επιδεικνύοντας ένα ψεύτικο δημόσιο κλειδί. Τέλος οι χρήστες πρέπει να έχουν τη δυνατότητα να φυλάσσουν τις ιδιωτικές τους κλείδες με ασφάλεια, οι οποίες θα είναι έγκυρες μόνο για συγκεκριμένο χρονικό διάστημα.

Η ανταλλαγή κλειδιών εφαρμόζεται στα συμμετρικά κρυπτοσυστήματα όπου οι δύο επικοινωνούντες χρήστες πρέπει να αποφασίσουν για το κοινό μυστικό κλειδί και έπειτα να αποκτήσουν από ένα αντίγραφο αυτού, χωρίς κανένας άλλος να μάθει για αυτό.

1.3 Απλές Εφαρμογές της Κρυπτογραφίας

1.3.1 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 κρυπτογράφησή τους, εάν μιλάμε

για συμμετρική κρυπτογράφηση ή το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που το κρυπτογράφησε, εάν μιλάμε για ασύμμετρη κρυπτογράφηση.

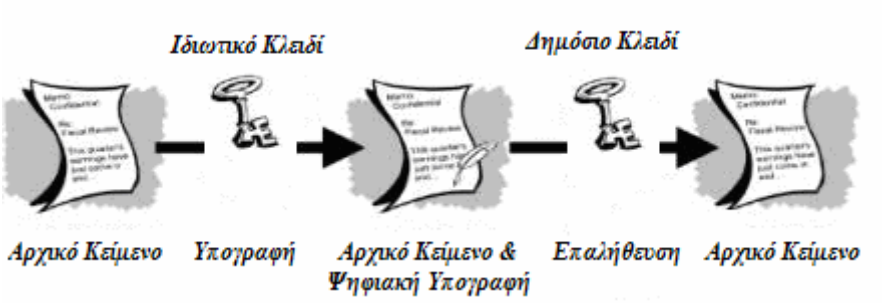
Αξίζει να σημειώσουμε ότι υπάρχουν περιπτώσεις όπου οι πληροφορίες δεν πρέπει να είναι απροσπέλαστες από όλους και γι' αυτό αποθηκεύονται με τέτοιο τρόπο, ώστε η αντιστροφή της κρυπτογραφικής διαδικασίας που έχει εφαρμοστεί, να είναι αδύνατη. Για παράδειγμα, σε ένα τυπικό περιβάλλον πολλών χρηστών, κανένας δεν πρέπει να έχει γνώση του αρχείου που περιέχει τους κωδικούς όλων των χρηστών. Συχνά, λοιπόν, αποθηκεύονται οι συνόψεις (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 αποδεικνύουν την ταυτότητα τους με την παροχή του κωδικού τους. Ο υπολογιστής που έχει αποθηκευμένες τις τιμές κατακερματισμού των κωδικών, σε κάθε εισαγωγή κωδικού υπολογίζει την τιμή κατακερματισμού του και τη συγκρίνει με το αποθηκευμένο που αντιστοιχεί στον χρήστη που προσπαθεί να πιστοποιήσει τον εαυτό του

1.3.2 Πιστοποίηση Ταυτότητας και Ψηφιακές Υπογραφές

Η ψηφιακή υπογραφή είναι ένα εργαλείο που παρέχει ακεραιότητα (integrity) των δεδομένων και 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 συνάρτηση κατακερματισμού και του ιδιωτικού κλειδιού 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 της σύνοψης του μηνύματος. Η σύνοψη είναι κατά κανόνα μικρότερο σε μέγεθος από το αρχικό μήνυμα. Στο δεύτερο βήμα, ο Α κρυπτογραφεί τη σύνοψη με το ιδιωτικό του κλειδί. Τέλος, στέλνει τη κρυπτογραφημένη σύνοψη στον Β μαζί με το έγγραφο. Για να μπορέσει ο Β να επαληθεύσει την υπογραφή πρέπει να

γνωρίζει το δημόσιο κλειδί του Α και την συνάρτηση κατακερματισμού που χρησιμοποίησε ο Α. Πρώτα θα αποκρυπτογραφήσει τη σύνοψη με το δημόσιο κλειδί του Α και θα πάρει τη σύνοψη που είχε παράγει ο Α. Έπειτα, θα υπολογίσει τη σύνοψη 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 το δημόσιο κλειδί του Α, τη συνάρτηση κατακερματισμού 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.



Εικόνα 10. *Ψηφιακή Υπογραφή*

Για να έχει αποτέλεσμα η παραπάνω μέθοδος, πρέπει να τηρούνται δύο προϋποθέσεις: (α) η συνάρτηση κατακερματισμού πρέπει να είναι όσο το δυνατόν περισσότερο μη αντιστρέψιμη και (β) τα ζεύγη δημόσιου – ιδιωτικού κλειδιού 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 ένα συγκεκριμένο δημόσιο κλειδί.

1.4 Μηχανισμοί και Αλγόριθμοι Κρυπτογραφίας

1.4.1 Αλγόριθμοι Ασύμμετρης Κρυπτογραφίας

RSA

Το σύστημα RSA είναι ένα σύστημα ασύμμετρης κρυπτογραφίας που προσφέρει τεχνικές κρυπτογράφησης και ψηφιακές υπογραφές. Αναπτύ-

χθηκε το 1977 από τους Ron Rivest, Adi Shamir και Leonard Adleman. Από τα αρχικά των επιθέτων τους προέρχεται το ακρωνύμιο RSA.

Το RSA λειτουργεί ως εξής: παίρνουμε δύο μεγάλους πρώτους αριθμούς p,q και υπολογίζουμε το γινόμενο τους n = pq. Το n καλείται modulus. Διαλέγουμε ένα αριθμό e μικρότερο του n και τέτοιο, ώστε e και (p-1)(q-1) να μην έχουν κοινούς διαιρέτες εκτός του 1. Βρίσκουμε έναν άλλο αριθμό d, ώστε (ed-1) να διαιρείται από το (p-1)(q-1). Τα ζευγάρια (n,e) και (n,d) καλούνται δημόσιο κλειδί και ιδιωτικό κλειδί, αντίστοιχα.

Είναι δύσκολο να βρεθεί το ιδιωτικό κλειδί d από το δημόσιο κλειδί e. Αυτό θα απαιτούσε την εύρεση των διαιρετέων του πρώτου αριθμού n, δηλαδή των αριθμών p και q. Ο n είναι πολύ μεγάλος και επειδή είναι πρώτος, θα έχει μόνο δύο πρώτους διαιρέτες. Άρα η εύρεση των διαιρετέων είναι πολύ δύσκολη έως και αδύνατη. Στο άλυτο αυτού του προβλήματος βασίζεται το σύστημα RSA. Η ανακάλυψη μιας εύκολης μεθόδου επίλυσης του προβλήματος, θα αχρήστευε το RSA.

Με το RSA η κρυπτογράφηση και η πιστοποίηση ταυτότητας πραγματοποιούνται χωρίς την κοινή χρήση ιδιωτικών κλειδιών. Ο καθένας χρησιμοποιεί μόνο το δικό του ιδιωτικό κλειδί ή το δημόσιο κλειδί οποιουδήποτε άλλου. Όλοι μπορούν να στείλουν ένα κρυπτογραφημένο μήνυμα ή να επαληθεύσουν μια υπογραφή, αλλά μόνο ο κάτοχος του σωστού ιδιωτικού κλειδιού μπορεί να αποκρυπτογραφήσει ή να υπογράψει ένα μήνυμα.

Κρυπτογράφηση με το RSA

Έστω ο χρήστης Α που θέλει να στείλει κρυπτογραφημένο στο χρήστη Β ένα έγγραφο. Ο Α κρυπτογραφεί το έγγραφο με την εξής εξίσωση: c = me mod n, όπου (n,e) είναι το δημόσιο κλειδί του Β. Ο Β, όταν παραλάβει το μήνυμα θα εφαρμόσει την εξής εξίσωση: m = cd mod n, όπου (n,d) το ιδιωτικό κλειδί του Β. Η μαθηματική σχέση που το e και το d εξασφαλίζει το γεγονός ότι ο Β αποκρυπτογραφεί το μήνυμα. Αφού μόνο ο Β ξέρει το d, μόνο αυτός μπορεί να αποκρυπτογραφήσει το μήνυμα.

Ψηφιακές Υπογραφές με το RSA

Ας υποθέσουμε, τώρα, ότι ο Α θέλει να στείλει μήνυμα στον Β με τέτοιο τρόπο, ώστε ο Β να είναι σίγουρος ότι το μήνυμα είναι αυθεντικό και δεν έχει μεταβληθεί. Ο Α υπογράφει το έγγραφο ως εξής: s = md mod n, όπου d και n είναι το ιδιωτικό κλειδί του Α. Για να επαληθεύσει την υπο-

γραφή ο Β εκτελεί την πράξη: m = se mod n, όπου e και n το δημόσιο κλειδί του Α.

1.4.2 Αλγόριθμοι Συμμετρικής Κρυπτογραφίας

DES (Data Encryption Standard)
Αντιπροσωπεύει την τυποποίηση Federal Information Processing Standard (FIPS) 46-1 που επίσης περιγράφει τον Data Encryption Algorithm (DEA). Αρχικά αναπτύχθηκε από την IBM, ενώ σημαντικό ρόλο στην ανάπτυξη του έπαιξε η NSA και το National Institute of Standards and Technology (NIST). Είναι ο πιο γνωστός και παγκόσμια χρησιμοποιούμενος συμμετρικός αλγόριθμος.

Ο DES είναι block cipher, πιο συγκεκριμένα Feistel cipher, με μέγεθος block 64 bit. Χρησιμοποιεί κλειδί 64 bits από τα οποία τα 8 αποτελούν bits ισοτιμίας. Όταν χρησιμοποιείται για την επικοινωνία, αποστολέας και παραλήπτης μοιράζονται το ίδιο κλειδί. Ο DES, εκτός από κρυπτογράφηση, μπορεί να χρησιμοποιηθεί στην παραγωγή MACs (σε CBC mode). Επίσης, μπορεί να χρησιμοποιηθεί για κρυπτογράφηση αρχείων αποθηκευμένα σε σκληρό δίσκο σε περιβάλλοντα ενός χρήστη. Για την διανομή των κλειδιών σε περιβάλλον πολλών χρηστών, συνδυάζεται με ασύμμετρο κρυπτοσύστημα.

Triple-DES
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.

DESX

Ο DESX είναι μια άλλη παραλλαγή του DES. Η διαφορά του DES και του DESX είναι ότι η είσοδος στο DESX περνάει από μια XOR πράξη με ένα επιπλέον κλειδί 64 bits και ομοίως η έξοδος της κρυπτογράφησης. Η αιτία ανάπτυξης του DESX είναι η δραματική αύξηση της αντοχής του DES σε γνωστές επιθέσεις.

AES (Advanced Encryption Standard)

Είναι ένας block cipher που προορίζεται να γίνει τυποποίηση του FIPS και να αντικαταστήσει τον DES.

DSS (Digital Signature Algorithm)

Το National Institute of Standards and Technology (NIST) δημοσιοποίησε το Digital Signature Algorithm (DSS), που είναι μέρος του Capstone Project της κυβέρνησης των Ηνωμένων Πολιτειών, τον Μάιο του 1994. Έχει καθιερωθεί σαν το επίσημο αλγόριθμο παραγωγής ψηφιακών υπογραφών της κυβέρνησης των Η.Π.Α.

Βασίζεται στο πρόβλημα του διακριτού λογαρίθμου και χρησιμοποιείται μόνο για παραγωγή ψηφιακών υπογραφών. Η διαφορά από τις υπογραφές του RSA είναι, ότι ενώ στο DSA η παραγωγή των υπογραφών είναι πιο γρήγορη από την επιβεβαίωσή τους, στο RSA συμβαίνει το αντίθετο: η επιβεβαίωση είναι ταχύτερη από την υπογραφή. Παρ' όλο που μπορεί να υποστηριχθεί ότι η γρήγορη παραγωγή υπογραφών αποτελεί πλεονέκτημα, επειδή ένα μήνυμα υπογράφεται μία φορά αλλά η υπογραφή του μπορεί να επαληθευτεί πολλές φορές, κάτι τέτοιο δεν ανταποκρίνεται στην πραγματικότητα.

Το DSS έχει ολοκληρωθεί σε πολλά συστήματα ασφαλείας, αν και έχει λάβει πολλές άσχημες κριτικές. Τα κυριότερα θέματα κριτικής είναι η έλλειψη ευελιξίας, η αργή επαλήθευση των υπογραφών, η αδυναμία συνεργασίας με άλλο πρωτόκολλο πιστοποίησης ταυτότητας και τέλος ότι ο αλγόριθμος δεν είχε αποκαλυφθεί.

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 κώδικας ροής 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 που αναπτύχθηκε 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.

IDEA (International Data Encryption Algorithm)
Ο IDEA είναι ένας block cipher που αναπτύχθηκε από τους Lai και Massey. Χρησιμοποιεί block μεγέθους 64 bits και κλειδιά 128 bits. Η διαδικασία της κρυπτογράφησης απαιτεί 8 σύνθετες επαναλήψεις. Παρ' όλο που δεν έχει την κατασκευή ενός Feistel κρυπτοσυστήματος, η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο που γίνεται και η κρυπτογράφηση. Έχει σχεδιαστεί για να είναι εύκολα εφαρμόσιμος τόσο σε υλικό (hardware) όσο και σε λογισμικό (software). Μερικές, όμως, αριθμητικές διεργασίες που χρησιμοποιεί ο IDEA καθιστούν τις εφαρμογές αργές, παρόμοιες σε ταχύτητα με τον DES. Ο IDEA αποτελεί ένα πολύ δυνατό αλγόριθμο που είναι απρόσβλητος από τα περισσότερα είδη επιθέσεων.

Blowfish
Ο Blowfish είναι ένας block cipher που κατασκευάστηκε από τον Schneier. Είναι ένας Feistel cipher με μέγεθος block 64 bits και μεταβλητό μήκος κλειδιού, με μέγιστο μήκος 448 bits. Όλες οι διεργασίες βασίζονται σε XOR πράξεις και προσθέσεις λέξεων των 32 bits. Από το κλειδί παράγεται πίνακας με τα subkeys που χρησιμοποιούνται σε κάθε γύρο

επανάληψης της κρυπτογράφησης. Έχει σχεδιασθεί για 32-bit μηχανές και είναι σημαντικά ταχύτερος από τον DES. Παρ' όλες τις αδυναμίες που έχουν ανακαλυφθεί καθ' όλη την διάρκεια της ύπαρξης του, θεωρείται ακόμα ασφαλής αλγόριθμος.

1.4.3 Συναρτήσεις Κατακερματισμού

SHA και SHA-1 (Secure Hash Algorithm)
Ο SHA, όπως και SHA-1, αναπτύχθηκε από το NIST. Ο SHA-1 αποτελεί επανέκδοση του SHA που διόρθωνε μια ατέλεια του τελευταίου. Ο SHA-1 είδε το φως της δημοσιότητας το 1994 και η δομή και λειτουργία του είναι παρόμοια με την αντίστοιχη του MD4 που αναπτύχθηκε από τον Ron Rivest. Είναι και αυτός μέρος του Capstone Project.

Ο SHA-1 παίρνει είσοδο μήνυμα μήκους μικρότερο από 264 bits και παράγει σύνοψη 160 bits. Είναι ελαφρά πιο αργός από τον MD5, αλλά η μεγαλύτερη σύνοψη που παράγει τον κάνουν πιο ασφαλή απέναντι σε προσπάθειες αντιστροφής του.

MD2, MD4, MD5 (Message Digest)
Όλοι αυτοί οι αλγόριθμοι είναι συναρτήσεις κατακερματισμού που έχουν αναπτυχθεί από τον Ron Rivest. Προορίζονται, κυρίως, για την παραγωγή ψηφιακών υπογραφών. Το μήνυμα πρώτα σμικρύνεται με έναν από αυτούς τους αλγόριθμους και έπειτα, η σύνοψη του μηνύματος κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα. Και οι τρεις παίρνουν στην είσοδο μήνυμα αυθαίρετου μήκους και δίνουν στην έξοδο μια σύνοψη 128 bits. Παρ' όλο που η κατασκευή τους μοιάζει αρκετά, ο MD2 είχε σχεδιαστεί για μηχανές 8 bit, σε αντίθεση με τους MD4 και MD5 που προορίζονται για μηχανές 32 bits.

Ο MD2 αναπτύχθηκε το 1989. Το μήνυμα αρχικά συμπληρώνεται με κατάλληλο αριθμό bytes, ώστε το μήκος του σε bytes να είναι διαιρέσιμο από το 16. Ένα αρχικό άθροισμα ελέγχου (checksum) των 16 bits προστίθεται στο τέλος του μηνύματος και η τελική σύνοψη παράγεται από το αποτέλεσμα της προηγούμενης ενέργειας. Η κρυπτανάλυση του MD2 έδειξε ότι είναι δυνατόν να υπάρχουν μηνύματα που παράγουν την ίδια σύνοψη, αν και μόνο αν παραλείπεται το βήμα πρόσθεσης του 16-byte checksum.

Ο MD4 αναπτύχθηκε το 1990. Το μήκος του μηνύματος συμπληρώνεται με κατάλληλο αριθμό bits, ώστε να το μήκος του σε bits συν 448 να είναι

διαιρέσιμο από το 512. Μια δυαδική αναπαράσταση του μηνύματος των 64 bits προστίθεται στο μήνυμα και το αποτέλεσμα επεξεργάζεται με τη συνάρτηση σύνοψης. Τα τμήματα που διαχειρίζεται η συνάρτηση σύνοψης έχουν μήκος 512 bits και κάθε τμήμα επεξεργάζεται πλήρως σε τρεις διακριτούς επαναληπτικούς γύρους. Ο MD4 έχει επανειλημμένα αναλυθεί με διάφορους τρόπους και δεν πρέπει να θεωρείται πλέον ασφαλής. Συγκεκριμένα, έχει αποδειχθεί ότι μπορεί να αντιστραφεί η διαδικασία και ότι υπό ορισμένες συνθήκες δεν είναι αμφιμονοσήμαντος.

Ο MD5 αναπτύχθηκε το 1991. Είναι μια κατά πολύ βελτιωμένη έκδοση του MD4, γι' αυτό είναι και λίγο πιο αργός. Η μόνη διάφορα είναι η χρήση τεσσάρων επαναλήψεων κατά την επεξεργασία του κάθε τμήματος. Οι απαιτήσεις σε μέγεθος τμήματος και μήκος μηνύματος παραμένουν οι ίδιες. Η κρυπτανάλυση του MD5 συνεχίζεται ακόμα, αλλά οι πρώτες εκτιμήσεις δείχνουν ότι έχει αρκετές αδυναμίες.

1.4.4 Αλγόριθμοι για τη Διαχείριση και Ανταλλαγή Κλειδιών

Diffie-Hellman

Το πρωτόκολλο Diffie-Hellman είναι ένας μηχανισμός ανταλλαγής κλειδιών και αναπτύχθηκε από τους Diffie και Hellman το 1976. Επιτρέπει σε δύο χρήστες να ανταλλάσσουν ένα μυστικό κλειδί μέσα από ένα μη ασφαλές δίκτυο.

Το πρωτόκολλο έχει δύο παραμέτρους: p και g. Είναι και οι δύο δημοσιοποιημένοι και μπορούν να χρησιμοποιηθούν από όλους τους χρήστες του συστήματος. Η παράμετρος p είναι ένας πρώτος αριθμός και η παράμετρος g είναι ένας ακέραιος με την εξής ιδιότητα: για οποιοδήποτε ακέραιο αριθμό n στο διάστημα [1, p-1], υπάρχει αριθμός k τέτοιος ώστε gk = n mod p.

Ας υποθέσουμε τώρα ότι δύο χρήστες, ο Α και ο Β, θέλουν να συμφωνήσουν για ένα μυστικό κλειδί. Πρώτα, ο Α παράγει μία τυχαία ιδιωτική τιμή a και ο Β μία τυχαία ιδιωτική τιμή b. Οι τιμές a και b διαλέγονται από το σύνολο [1, p-1]. Έπειτα δημιουργούν τις δημόσιες τιμές τους χρησιμοποιώντας τις παραμέτρους p και g και τις ιδιωτικές τους τιμές. Η δημόσια τιμή του Α είναι ga mod p και του Β είναι gb mod p. Στην συνέχεια ανταλλάσσουν τις δημόσιες τιμές τους. Τέλος, ο Α κάνει τον υπολογισμό gab = (gb)a mod p και Β κάνει με την σειρά του τον υπολογισμό gba = (ga)b mod p. Επειδή gab = gba = k, ο Α και Β έχουν τώρα ένα κοινό μυστικό κλειδί. Το πρωτόκολλο εξαρτάται από το γεγονός ότι είναι

αδύνατον να υπολογιστεί το κ από τις δημόσιες τιμές ga mod p και gb mod p χωρίς τη γνώση των a και b και όταν ο p είναι πολύ μεγάλος.

Οι πρώτες εκδόσεις του μηχανισμού Diffie-Hellman ήταν ευάλωτες σε επιθέσεις ενδιάμεσου (man-in-the-middle). Σε αυτή την επίθεση ο χρήστης C παρεμβάλλεται στην επικοινωνία των A και B και όταν ανταλλάσσουν τις δημόσιες τιμές τους, τις αντικαθιστά με τις δικές του. Δηλαδή όταν ο A μεταδίδει τη δημόσια τιμή του στον B, ο C την αντικαθιστά με τη δικιά του και τη στέλνει στον B. Ομοίως, όταν ο B στέλνει τη δημόσια τιμή του στον A. Σαν συνέπεια, οι C και A συμφωνούν για ένα μυστικό κλειδί και οι C και B συμφωνούν για ένα άλλο κλειδί. Έτσι ο C μπορεί να διαβάσει τα μηνύματα που μεταδίδουν ο A στον B και πιθανώς να τα τροποποιήσει πριν τα προωθήσει σε έναν από τους δύο.

Το 1992 αναπτύχθηκε μία ανανεωμένη έκδοση από τους Diffie, Van Oorschot και Wiener που υποστήριζε την πιστοποίηση της ταυτότητας των δύο πλευρών και είχε σαν σκοπό να καταπολεμήσει την επίθεση ενδιάμεσου (man-in-the-middle). Τα μηνύματα ανταλλάσσονται υπογεγραμμένα με τις ιδιωτικές κλείδες των A και B, ενώ χρησιμοποιούνται και πιστοποιητικά (βλέπε παρακάτω) για την απόκτηση των σωστών δημοσίων κλειδιών. Ο C ακόμα και αν είναι σε θέση να παρακολουθεί την επικοινωνία των A και B, δεν μπορεί να πλαστογραφήσει τα μηνύματα.

Ψηφιακοί Φάκελοι (Digital Envelopes)

Ο μηχανισμός των ψηφιακών φακέλων βρίσκει εφαρμογή στην ανταλλαγή μυστικών κλειδιών που χρησιμοποιούνται σε συμμετρικά κρυπτοσυστήματα. Ο ψηφιακός φάκελος αποτελείται από ένα μήνυμα κρυπτογραφημένο με ένα συμμετρικό κλειδί και το συμμετρικό κλειδί κρυπτογραφημένο με άλλο κλειδί. Συνήθως η κρυπτογράφηση του συμμετρικού κλειδιού γίνεται με το δημόσιο κλειδί της αντίθετης πλευράς, αλλά αυτό δεν είναι απαραίτητο. Μπορεί κάλλιστα να χρησιμοποιηθεί και ένα προσυμφωνημένο συμμετρικό κλειδί.

Ας υποθέσουμε ότι ο χρήστης B θέλει να στείλει μήνυμα στον χρήστη B. Ο A διαλέγει ένα συμμετρικό κλειδί και κρυπτογραφεί το μήνυμα με αυτό. Έπειτα κρυπτογραφεί το μυστικό συμμετρικό κλειδί με το δημόσιο κλειδί του B. Στέλνει στον B το κρυπτογραφημένο μήνυμα συνοδευόμενο από το κρυπτογραφημένο κλειδί. Όταν ο B θελήσει να διαβάσει το μήνυμα, χρησιμοποιεί το ιδιωτικό του κλειδί για να ανακτήσει το συμμετρικό κλειδί και μετά αποκρυπτογραφεί το μήνυμα με το μυστικό συμμετρικό κλειδί. Στην περίπτωση που το μήνυμα έχει παραπάνω του ενός

παραλήπτες, το μυστικό συμμετρικό κλειδί κρυπτογραφείται ξεχωριστά με το δημόσιο κλειδί του κάθε παραλήπτη. Και πάλι μεταδίδεται μόνο ένα κρυπτογραφημένο μήνυμα.

Οι χρήστες μπορούν να αλλάζουν κλειδιά όσο συχνά θέλουν, γεγονός που αυξάνει κατακόρυφα την ασφάλεια του συστήματος. Επίσης, οι ψηφιακοί φάκελοι όχι μόνο λύνουν το πρόβλημα της ανταλλαγής κλειδιών, αλλά βελτιώνουν και την απόδοση του συστήματος καθ' ότι η ασύμμετρη κρυπτογράφηση από μόνη της απαιτεί εξαιρετικά χρονοβόρα επεξεργασία. Ο πιο συνηθισμένος συνδυασμός είναι το ασύμμετρο κρυπτοσύστημα RSA με το συμμετρικό DES.

Πιστοποιητικά

Τα πιστοποιητικά είναι ψηφιακά έγγραφα που αποδεικνύουν τη σχέση μεταξύ ενός δημόσιου κλειδιού και μίας οντότητας. Επιτρέπουν, δηλαδή, την επαλήθευση του ισχυρισμού ότι ένα συγκεκριμένο δημόσιο κλειδί ανήκει σε μια συγκεκριμένη οντότητα. Τα πιστοποιητικά αποτρέπουν κάποιον να υποδυθεί κάποιον άλλο με την χρήση ψεύτικου κλειδιού.

Ας υποθέσουμε ότι ο Α χρειάζεται το δημόσιο κλειδί του Β για να μπορέσει να εγκαταστήσει μία ασφαλή συναλλαγή. Το να ζητήσει από τον Β να του στείλει το δημόσιο κλειδί του, μπορεί να θέσει την όλη επικοινωνία σε κίνδυνο. Εκτός από την παρακολούθηση της συναλλαγής και αντικατάστασης του δημόσιου κλειδιού του Β με το δημόσιο κλειδί κάποιου άλλου (επίθεση man-in-the-middle), μπορεί οποιοσδήποτε να ξεγελάσει τον Α, όταν ο Α δεν γνωρίζει και δεν μπορεί να επικοινωνήσει τηλεφωνικά με τον Β, λέγοντας πως είναι ο Β και παρουσιάζοντας ένα ψεύτικο δημόσιο κλειδί. Δηλαδή, έστω ότι ο Β υποστηρίζει ότι είναι ο πρωθυπουργός της Ελλάδος. Τότε ο Α θα νομίζει ότι συνδιαλέγεται με τον πρωθυπουργό της Ελλάδος και χρησιμοποιεί το δημόσιο κλειδί που του παρουσίασε ο Β για να στείλει στον δήθεν πρωθυπουργό εμπιστευτικά έγγραφα.

Ένα πιστοποιητικό περιέχει τις ακόλουθες πληροφορίες:

- το όνομα του κατόχου,
- το όνομα της του εκδοτικού οργανισμού – CA (βλέπε παρακάτω),
- το δημόσιο κλειδί του ονόματος που αναγράφεται στο πιστοποιητικό,
- την ημερομηνία λήξης του πιστοποιητικού,

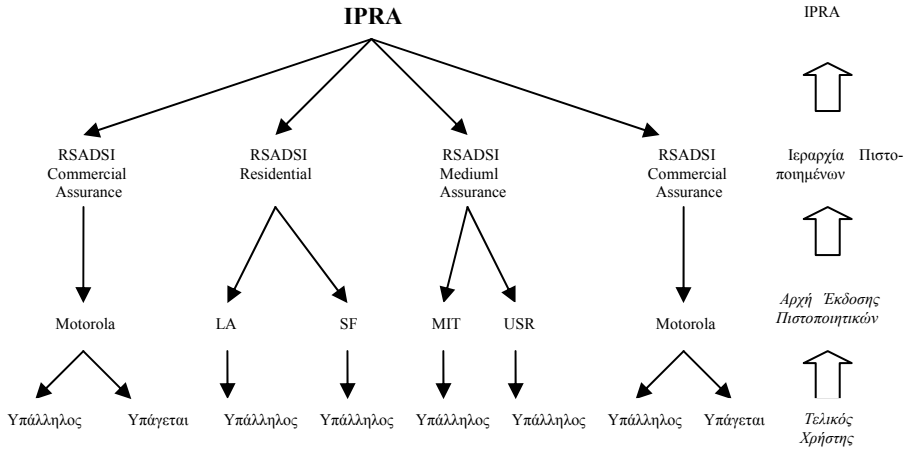
- ένα σειριακό αριθμό (serial number),
- την ψηφιακή υπογραφή του εκδοτικού οργανισμού.

Το πιστοποιητικό μεταφέρεται, συνήθως, μαζί με την ψηφιακή υπογραφή. Για την επαλήθευση της ψηφιακής υπογραφής ο παραλήπτης πρέπει να έχει το σωστό δημόσιο κλειδί του αποστολέα. Επίσης, το πιστοποιητικό στέλνεται κατά την εγκαθίδρυση μιας σύνδεσης μεταξύ δύο άκρων, για την γνωστοποίηση του δημόσιου κλειδιού κάθε πλευράς στην άλλη πλευρά και για την χρήση της στην κρυπτογράφηση της επικοινωνίας. Το πιστοποιητικό δεν χρειάζεται να αποστέλλεται κάθε φορά που ξεκινά μία συναλλαγή. Αρκεί να σταλεί μία φορά κατά την έναρξη της σύνδεσης.

1.4.5 Αρχές Έκδοσης Πιστοποιητικών

Τα πιστοποιητικά εκδίδονται από τις Αρχές Έκδοσης Πιστοποιητικών (Certification Authorities – CA), που μπορεί να είναι οποιοσδήποτε άξιος εμπιστοσύνης οργανισμός ικανός να εγγυηθεί για την ταυτότητα αυτών για τους οποίους εκδίδει πιστοποιητικά. Ένας οργανισμός μπορεί να εκδίδει πιστοποιητικά για τους υπάλληλους του ή ένα Πανεπιστήμιο για τους σπουδαστές του ή ακόμα και μια πόλη για τους κατοίκους της. Η CA πρέπει να κατέχει ένα ζεύγος ιδιωτικού – δημόσιου κλειδιού. Με το ιδιωτικό της κλειδί υπογράφει ψηφιακά τα πιστοποιητικά που εκδίδει, ενώ την εγκυρότητα του δημόσιου κλειδιού πρέπει να επικυρώνει εκδοτικός οργανισμός σε υψηλότερη θέση στην ιεραρχία των CAs.

Η ιεραρχική κατάταξη που βλέπουμε στο ακόλουθο σχήμα, έχει στην κορυφή της τον οργανισμό Internet Policy Registration Authority (IRPA) και αμέσως μετά ακολουθούν οι Policy Certification Authorities (PCAs) που δημοσιοποιούν πολιτικές ασφάλισης και έκδοσης πιστοποιητικών. Ανάλογα με το είδος των πιστοποιητικών και περιορισμών που ασκούν όσο αναφορά την χρήση τους, οι Αρχές Έκδοσης Πιστοποιητικών (CAs) που τα εκδίδουν κατατάσσονται σε μία από τις υψηλότερες σε επίπεδο, PCAs. Τέλος, έρχονται οι τελικοί χρήστες που ανάλογα με τις ανάγκες τους επιλέγουν την CA που θα πιστοποιήσει το δημόσιο κλειδί τους. Οι ανάγκες κάθε χρήστη καθορίζονται στο αν το κλειδί θα χρησιμοποιηθεί για εμπορικές συναλλαγές, για υπογραφή κυβερνητικών εγγράφων, για την απλή ανταλλαγή ηλεκτρονικού ταχυδρομείου ή ακόμα για την διασφάλιση τεχνολογικών επιτευγμάτων.



Εικόνα 11. *Ιεραρχική Κατάταξη*

Σ' αυτήν της ιεραρχία, οι οργανισμοί κάθε επιπέδου πιστοποιούν το δημόσιο κλειδί και ταυτότητα του χαμηλότερου επιπέδου. Έτσι, πολλές φορές το πιστοποιητικό για έναν χρήστη μπορεί να συνοδεύεται από μία αλυσίδα πιστοποιητικών (certificates chain) που φθάνουν ως την κορυφή της ιεραρχίας. Σε κάθε πιστοποιητικό περιέχεται η υπογραφή του ανώτερου εκδοτικού οργανισμού που έχει δημιουργηθεί με το ιδιωτικό κλειδί αυτού.

Από το σχήμα καταλαβαίνουμε ότι μια τέτοια ιεραρχική δομή μπορεί να εφαρμοστεί και στο εσωτερικό μεγάλων εταιριών. Το δημόσιο κλειδί του ανώτερου εκδοτικού οργανισμού δεν μπορεί να πιστοποιηθεί από κανέναν. Ο οργανισμός εκδίδει πιστοποιητικό για τον εαυτό του που περιέχει το δημόσιο κλειδί του και την υπογραφή του με το ιδιωτικό του κλειδί, το οποίο καλείται αρχικό πιστοποιητικό (root certificate). Αυτονόητο είναι, λοιπόν, ότι αυτός ο οργανισμός πρέπει να είναι απόλυτα έμπιστος.

Ο χρήστης που επιθυμεί να αποκτήσει ένα πιστοποιητικό, θα δημιουργήσει πρώτα ένα ζεύγος ιδιωτικού – δημόσιου κλειδιού και θα αποστείλει σε μία CA το δημόσιο κλειδί μαζί με πληροφορίες που προσδιορίζουν την ταυτότητα του χρήστη. Η CA αφού επαληθεύσει την ταυτότητα του χρήστη και σιγουρευτεί ότι η αίτηση έκδοσης πιστοποιητικού προέρχεται από τον πραγματικό χρήστη, απαντά στον χρήστη με χρήστη το πιστο-

ποιητικό του μαζί με τα ιεραρχικά δεμένα πιστοποιητικά που επιβεβαιώνουν την αυθεντικότητα του δημόσιου κλειδιού της CA.

Λίστες Ανάκλησης Πιστοποιητικών (Certificate Revocation Lists)
Μία λίστα ανάκλησης πιστοποιητικών περιέχει πιστοποιητικά που έχουν ακυρωθεί πριν από την προγραμματισμένη ημερομηνία λήξης. Υπάρχουν αρκετοί λόγοι γιατί ένα πιστοποιητικό μπορεί να ανακληθεί. Για παράδειγμα το μυστικό κλειδί που ορίζεται στο πιστοποιητικό να έχει κοινοποιηθεί καθιστώντας αυτόματα την χρήση του πιστοποιητικού μη ασφαλή ή το άτομο για το οποίο εκδόθηκε το πιστοποιητικό να μην έχει πια την δικαιοδοσία να το χρησιμοποιεί. Ας φανταστούμε την περίπτωση όπου ένας υπάλληλος μια εταιρείας έχει πιστοποιητικό που έχει εκδώσει για λογαριασμό του η εταιρεία. Εάν ο υπάλληλος απολυθεί, η εταιρεία θα ακυρώσει το πιστοποιητικό, ώστε να μην έχει τη δυνατότητα να υπογράφει έγγραφα με αυτό το κλειδί.

Κατά την επαλήθευση μιας υπογραφής, πρέπει κάθε χρήστης να συμβουλεύεται μία CRL για να διαπιστώσει εάν το εν λόγω πιστοποιητικό δεν έχει αποσυρθεί. Το αν αξίζει τον κόπο να πραγματοποιήσει τέτοιο έλεγχο, εξαρτάται από τη σημασία του εγγράφου. Οι λίστες διατηρούνται και ανανεώνονται από τις CA, και κάθε CA διαχειρίζεται τις λίστες που παρέχουν πληροφορίες για τα ανακληθέντα πιστοποιητικά που είχαν εκδοθεί από την ίδια. Επίσης, οι λίστες περιέχουν τα πιστοποιητικά των οποίων δεν έχει περάσει η ημερομηνία λήξης. Αυτά τα πιστοποιητικά δεν γίνονται δεκτά σε καμία περίπτωση.

1.5 CrypTool

Το CrypTool αποτελεί ένα πρόγραμμα με μια εξαιρετικά περιεκτική σε απευθείας σύνδεση βοήθεια που επιτρέπει στο χρήστη να χρησιμοποιήσει και να αναλύσει τις κρυπτογραφικές διαδικασίες μέσα σε ένα ενοποιημένο γραφικό περιβάλλον.

Το CrypTool αναπτύχθηκε κατά τη διάρκεια του προγράμματος συνειδητοποίησης των χρηστών της Deutsche Bank προκειμένου να αυξηθεί η κατανόηση τους σε ζητήματα ασφάλειας. Ένας περαιτέρω στόχος ήταν να δώσει τη δυνατότητα στους χρήστες να καταλάβουν τις κρυπτογραφικές διαδικασίες. Κατ' αυτό τον τρόπο, χρησιμοποιώντας το CrypTool ως μια αξιόπιστη εφαρμογή αναφοράς των διάφορων διαδικασιών κρυπτογράφησης (λόγω της χρησιμοποίησης της βιβλιοθήκης Secude), είναι δυ-

νατή και η εξέταση της κρυπτογράφησης που εφαρμόζεται σε άλλα προγράμματα.

Το CrypTool χρησιμοποιείται αυτήν την περίοδο για εκπαιδευτικούς λόγους σε επιχειρήσεις, σε σχολεία και σε πανεπιστήμια, ενώ επιπλέον διάφορα πανεπιστήμια βοηθούν στην περαιτέρω ανάπτυξη του προγράμματος.

Links:
Πληροφορίες για το CrypTool θα βρείτε:

- http://www.cryptool.org,
- http://www.cryptool.de.

Εργαστηριακές Ασκήσεις

Με τη χρήση του εργαλείου Cryptool να εκτελεστούν οι ακόλουθες ασκήσεις:

1. Δημιουργία ενός τυχαίου κειμένου.
2. Κρυπτογράφηση του κειμένου που δημιουργήθηκε με τη χρήση του κλασικού αλγόριθμου Caeser. Αποκρυπτογράφηση του κρυπτογραφήματος που προέκυψε.
3. Κρυπτογράφηση του αρχικού κειμένου την χρήση του κλασικού αλγόριθμου XOR. Αποκρυπτογράφηση του κρυπτογραφήματος που προέκυψε.
4. Κρυπτογράφηση του αρχικού κειμένου τη χρήση του συμμετρικού αλγόριθμου RC2. Αποκρυπτογράφηση του κρυπτογραφήματος που προέκυψε.
5. Κρυπτογράφηση του αρχικού κειμένου με τη χρήση του συμμετρικού αλγόριθμου DES (ECB). Αποκρυπτογράφηση του κρυπτογραφήματος που προέκυψε.
6. Κρυπτογράφηση του αρχικού κειμένου με τη χρήση του συμμετρικού αλγόριθμου DES (CCB). Αποκρυπτογράφηση του κρυπτογραφήματος που προέκυψε.
7. Κρυπτογράφηση του αρχικού κειμένου με τη χρήση του συμμετρικού αλγόριθμου AES (self extracting). Αποκρυπτογράφηση του κρυπτογραφήματος που προέκυψε.

8. Δημιουργία ενός ασύμμετρου ζεύγους κλειδιών.

9. Εμφάνιση των πληροφοριών που σχετίζονται με το ζεύγος που δημιουργήθηκε.

10. Κρυπτογράφηση του αρχικού κειμένου με τη χρήση του ασύμμετρου αλγόριθμου RSA. Αποκρυπτογράφηση του κρυπτογραφήματος που προέκυψε.

11. Κρυπτογράφηση του αρχικού κειμένου με τη χρήση υβριδικής κρυπτογραφίας.

12. Δημιουργία σύνοψης του αρχικού κειμένου (χρήση Συνάρτησης Κατακερματισμού).

13. Ψηφιακή υπογραφή του αρχικού κειμένου. Επικύρωση της ψηφιακής υπογραφής.

14. Δημιουργία κλειδιού με τη χρήση ενός κωδικού.

15. Συμπίεση του αρχικού κειμένου.

16. Στα πλαίσια του RSA να πραγματοποιηθούν ενέργειες

17. Δημιουργία πρώτων αριθμών.

18. Κρυπτογράφηση και αποκρυπτογράφηση κειμένου.

19. Παραγοντοποίηση ενός αριθμού.

20. Ψηφιακή υπογραφή με χρήση RSA.

21. Δημιουργία ψευδοτυχαίων αριθμών.

22. Πραγματοποίηση ασφαλούς ανταλλαγής κλειδιών με την χρήση του πρωτοκόλλου Diffie-Hellman.

23. Εφαρμογή επίθεσης στις ψηφιακές υπογραφές.

24. Εφαρμογή Brute-Force Ανάλυσης του DES. Ποια συμπεράσματα εξάγονται;

25. Επιλογή ενός κλασικού αλγόριθμου κρυπτογράφησης. Παρουσίαση των βασικών στοιχείων του αλγόριθμου και χρησιμοποίησή του για την κρυπτογράφηση και την αποκρυπτογράφηση ενός κειμένου.

26. Επιλογή ενός συμμετρικού αλγόριθμου κρυπτογράφησης. Παρουσίαση των βασικών στοιχείων του αλγόριθμου και χρησιμοποίησή του για την κρυπτογράφηση και την αποκρυπτογράφηση ενός κειμένου.

27. Δημιουργία ενός ασύμμετρου ζεύγους κλειδιών. Δημιουργία ενός κειμένου και κρυπτογράφηση του κειμένου αυτού με τη χρήση του ασύμμετρου αλγόριθμου RSA. Τέλος αποκρυπτογράφηση του κρυπτογραφήματος.

28. Δημιουργία ενός τυχαίου κειμένου. Κρυπτογράφηση του κειμένου με τη χρήση υβριδικής κρυπτογραφίας.

29. Επιλογή μιας Συνάρτησης Κατακερματισμού. Παρουσίαση των βασικών στοιχείων της συνάρτησης και χρήση της συνάρτησης για δημιουργία μιας σύνοψης ενός κειμένου.

30. Δημιουργία ενός τυχαίου κειμένου. Ψηφιακή υπογραφή κειμένου και επικύρωση της ψηφιακής υπογραφής.

31. Δημιουργία ενός τυχαίου κειμένου. Ψηφιακή υπογραφή με χρήση RSA.

Αναφορές

1. C.Adams, S.Loyd. (1999). Understanding Public-Key Infrastructure, Macmillan Technical Publishing.

2. Menezes, P. van Oorschot, and S.A. Vanstone. (1997). "Handbook of Applied Cryptography" CRC Press.

3. Schneier B. (1996). Applied Cryptography, John Wiley and Sons Inc.

4. L.G.Pierson, (2000). Comparing Cryptographic Modes of Operation using Flow Diagrams, Sandia National Laboratories. Available at *http://csrc.nist.gov/CryptoToolkit/modes/workshop1/presentations/slides-pierson.pdf*.

5. RSA Laboratories. (2000). Frequently Asked Questions about Today's Cryptography. Available at http://www.rsa.com/rsalabs/node.asp?id=2152.