Κεφάλαιο 1ο

Στοιχεία Κρυπτογραφίας

1.1 Εισαγωγή

Κρυπτογραφία (cryptography) είναι η μελέτη τεχνικών που βασίζονται σε μαθηματικά προβλήματα με δύσκολη επίλυση, 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 έναν ενιαίο επιστημονικό κλάδο.

Εφαρμογή της κρυπτογραφίας είναι η *κρυπτογράφηση*. Κρυπτογράφηση είναι ο μετασχηματισμός δεδομένων σε μορφή που να είναι αδύνατον να αναγνωσθεί χωρίς την γνώση της σωστής ακολουθίας ψηφιακών δεδομένων (bits). Η ακολουθία bit καλείται "κλειδί" και χρησιμοποιείται σε συνδυασμό με κατάλληλο αλγόριθμο / συνάρτηση. Η αντίστροφη διαδικασία είναι η *αποκρυπτογράφηση* και απαιτεί επίσης γνώση του κατάλληλου κλειδιού (ίδιου ή διαφορετικού με την κρυπτογράφηση). Σκοπός της κρυπτογράφησης είναι να εξασφαλίσει το απόρρητο των δεδομένων κρατώντας τα κρυφά από όλους όσους έχουν πρόσβαση σε αυτά.

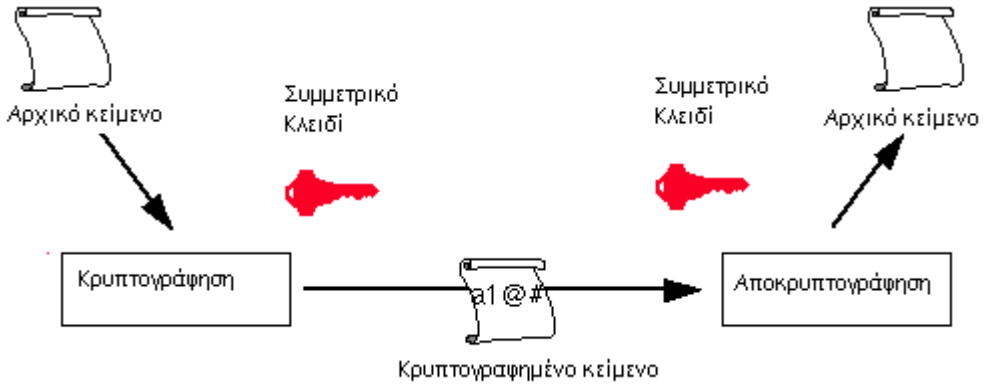
Η κρυπτογραφία εφαρμόζεται σε δεδομένα (ή μηνύματα) που διακινούνται μεταξύ οντοτήτων προκειμένου να ικανοποιηθούν οι απαιτήσεις ακεραιότητας και εμπιστευτικότητας [Schneier] που αυτά έχουν. Για παράδειγμα η κρυπτογραφία μπορεί να χρησιμοποιηθεί προκειμένου μηνύματα που μεταφέρονται

πάνω από ανοιχτά δίκτυα να προστατευθούν από υποκλοπή. Αυτό σημαίνει ότι ένα κρυπτογραφημένο μήνυμα αποτρέπει οποιονδήποτε από το να διαβάσει το μήνυμα καθώς αυτό περνάει από τους διάφορους κόμβους του δικτύου μέχρι να φτάσει στον παραλήπτη του. Όσο αφορά στην ακεραιότητα, η κρυπτογραφία μπορεί να αποτρέψει κάποιον από το να μεταβάλλει, διαγράψει ή εισάγει bits στα δεδομένα ενός μηνύματος χωρίς αυτό να γίνει αντιληπτό από τον παραλήπτη. Τα κρυπτογραφικά κλειδιά είναι επί της ουσίας μεγάλοι τυχαίοι αριθμοί που ελέγχουν την διαδικασία της κρυπτογράφησης.

Η θεωρία που παρουσιάζεται στο παρόν κεφάλαιο υποστηρίζεται από τις εργαστηριακές ασκήσεις του κεφαλαίου 5.2 προκειμένου ο αναγνώστης να έρθει σε πρώτη επαφή με τους πιο γνωστούς και διαδεδομένους αλγόριθμους και κρυπτοσυστήματα.

1.2 Συμμετρική Κρυπτογραφία

Στην παραδοσιακή κρυπτογραφία το ίδιο κρυπτογραφικό κλειδί χρησιμοποιείται για να κρυπτογραφήσει και να αποκρυπτογραφήσει την πληροφορία. Αυτό είναι πλέον γνωστό ως *μυστικό κλειδί (secret key)* και ο τύπος της κρυπτογραφίας ως *συμμετρική κρυπτογραφία* επειδή οι δύο οντότητες που θέλουν να επικοινωνήσουν, χρησιμοποιούν το ίδιο κλειδί για να την υλοποιήσουν. Ειδικότερα, οι οντότητες λαμβάνουν και οι δύο τα κλειδιά τους με χρήση ενός ασφαλούς μέσου (ενδεχομένως και εκτός δικτύου) και πρέπει να τα προστατεύσουν προκειμένου να εξασφαλίσουν ότι μόνο εξουσιοδοτημένες οντότητες μπορούν να χρησιμοποιήσουν την πληροφορία.



Σχήμα 1: *Συμμετρική κρυπτογράφηση*

Η συμμετρική κρυπτογραφία χαρακτηρίζεται από δύο βασικά μειονεκτήματα:

- όσο μεγαλώνει ο αριθμός των οντοτήτων, η διαχείριση των κλειδιών γίνεται όλο και πιο δύσκολη και
- επειδή και οι δύο οντότητες χρησιμοποιούν το ίδιο κλειδί δεν μπορεί κάποιος να αποδείξει από που ξεκίνησε το κρυπτογραφημένο μήνυμα.

Συνηθισμένοι αλγόριθμοι συμμετρικής κρυπτογραφία είναι ο Data Encryption Standard – DES (NIST 1988) [DES], ο Triple DES – 3DES [TDEA], ο Advanced Encryption Standard – AES (NIST 2001) [AES], ο RC4 [RC4], ο IDEA [IDEA], ο Camellia [Camellia] και ο Blowfish [BlowFish]. Συνοπτικές πληροφορίες για κάποιους από τους παραπάνω δίνονται στη συνέχεια.

1.2.1 Παραδείγματα Αλγορίθμων 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 αλγόριθμος κρυπτογράφησης τμημάτων (βλ. παράγραφο 1.4.3), πιο συγκεκριμένα αλγόριθμος Feistel, με μέγεθος τμήματος 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 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. Ο DESX παρουσιάζει δραματική αύξηση της αντοχής του DES σε γνωστές επιθέσεις.

AES (Advanced Encryption Standard)

Είναι ένας αλγόριθμος κρυπτογράφησης τμημάτων που προορίζεται να γίνει τυποποίηση του FIPS και να αντικαταστήσει τον DES.

RC2, RC4, RC5

Ο RC2 είναι ένας αλόγοριθμος κρυπτογράφησης τμημάτων 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 προς 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 αλγόριθμος κρυπτογράφησης ροών (βλ. και παράγραφο 1.4.4) που σχεδιάστηκε πάλι από τον 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 αλγόριθμος κρυπτογράφησης τμημάτων που αναπτύχθηκε από τον Ron Rivest για λογαριασμό της RSA Inc το 1994. Έχει πολλές παραμέτρους: μεταβλητό μήκος κλειδιού, μεταβλητό μέγεθος τμήματος και μεταβλητό αριθμό επαναλήψεων. Τυπικές επιλογές για το μέγεθος του τμήματος 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 αλγόριθμος κρυπτογράφησης τμημάτων που αναπτύχθηκε από τους Lai και Massey. Χρησιμοποιεί τμήματα μεγέθους 64 bits και κλειδιά 128 bits. Η διαδικασία της κρυπτογράφησης απαιτεί 8 σύνθετες επαναλήψεις. Παρ' όλο που δεν έχει την κατασκευή ενός κρυπτοσυστήματος Feistel, 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 έναν πολύ δυνατό αλγόριθμο που είναι απρόσβλητος στα περισσότερα είδη επιθέσεων.

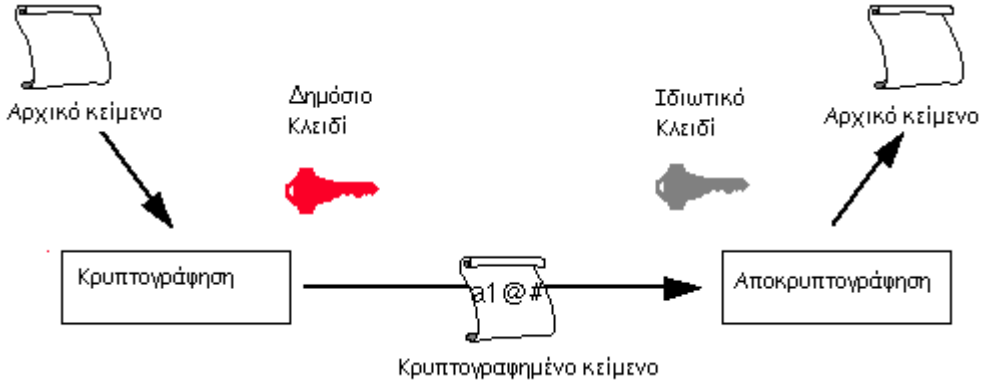
Blowfish

Ο Blowfish είναι ένας αλγόριθμος κρυπτογράφησης τμημάτων που κατασκευάστηκε από τον Schneier. Είναι ένας αλγόριθμος Feistel με μέγεθος τμήματος 64 bits και μεταβλητό μήκος κλειδιού, με μέγιστο μήκος 448 bits. Όλες οι διεργασίες βασίζονται σε πράξεις XOR και προσθέσεις λέξεων των 32 bits. Από το κλειδί παράγεται πίνακας με τα υπο-κλειδιά που χρησιμοποιούνται σε κάθε γύρο επανάληψης της κρυπτογράφησης. Έχει σχεδιασθεί για μηχανές 32-bit 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.

1.3 Κρυπτογραφία Δημοσίου Κλειδιού

Μια διαφορετική προσέγγιση της κρυπτογραφίας ονομάζεται κρυπτογραφία δημοσίου κλειδιού ή ασύμμετρη κρυπτογραφία. Αυτή η μορφή, χρησιμοποιεί δύο διαφορετικά αλλά μαθηματικά συσχετιζόμενα κλειδιά. Το ένα μπορεί να χρησιμοποιηθεί χωρίς να είναι δυνατή η εύρεση του άλλου. Στην κρυπτογραφία δημοσίου κλειδιού, το δημόσιο κλειδί μπορεί, όπως λέει και το όνομά του, να δημοσιοποιηθεί σε οποιονδήποτε θέλει να κάνει μια συναλλαγή με την οντότητα που κρατάει το ιδιωτικό κλειδί. Η διανομή του δημοσίου κλειδιού είναι εύκολη. Το ιδιωτικό κλειδί πρέπει να κρατηθεί κρυφό και να μπορεί να το χρησιμοποιήσει μόνο ο ιδιοκτήτης του. Ένας δημοφιλής αλγόριθμος κρυπτογραφίας δημοσίου κλειδιού είναι ο RSA [RSA], τον οποίο ανακάλυψαν ο R. Rivest, ο A. Shamir και ο L. Adleman. Άλλοι γνωστοί αλγόριθμοι είναι ο ElGamal [ElGamal], ο DSS [DSS] και το κρυπτοσύστημα Paillier [Paillier]. Συνοπτικές πληροφορίες για κάποιους από τους παραπάνω δίνονται στην επόμενη παράγραφο.

Στην κρυπτογραφία δημοσίου κλειδιού προκειμένου να κρυπτογραφηθούν κάποια δεδομένα, γίνεται χρήση του δημοσίου κλειδιού και το ιδιωτικό κλειδί χρησιμοποιείται μόνο για την αποκρυπτογράφησή τους. Οποιαδήποτε από τις οντότητες που γνωρίζουν το δημόσιο κλειδί μπορεί να κρυπτογραφήσει δεδομένα με παραλήπτη τον ένα και μοναδικό κάτοχο του ιδιωτικού κλειδιού.



Σχήμα 2: *Κρυπτογράφηση με κρυπτογραφία δημοσίου κλειδιού*

Η κρυπτογραφία δημοσίου κλειδιού, μπορεί επίσης να χρησιμοποιηθεί για την δημιουργία μη παραποιούμενων ψηφιακών υπογραφών βασισμένων στο ιδιωτικό κλειδί κάποιου χρήστη. Λεπτομέρειες για το πως δημιουργούνται οι ψηφιακές υπογραφές παρατίθενται στην παράγραφο 1.4.5.

Το αρνητικό χαρακτηριστικό της κρυπτογραφίας δημοσίου κλειδιού είναι το αυξημένο υπολογιστικό κόστος της. Ακόμη και με σύγχρονους υπολογιστές, θεωρείται αργή λόγω των πολύπλοκων υπολογισμών που περιλαμβάνει. Γι' αυτό το λόγο, στην πράξη, αλγόριθμοι κρυπτογραφίας δημοσίου κλειδιού χρησιμοποιούνται μόνο για την κρυπτογράφηση περιορισμένου μεγέθους πληροφορίας, όπως για παράδειγμα ένα κλειδί συμμετρικού αλγορίθμου όπως ο DES ή ο 3DES. Το δεύτερο αυτό κλειδί χρησιμοποιείται με έναν αλγόριθμο συμμετρικής κρυπτογραφίας ο οποίος αναλαμβάνει να κρυπτογραφήσει μεγαλύτερους όγκους δεδομένων με πιο αποδοτικό τρόπο (*υβριδική κρυπτογραφία*).

Προκειμένου να λειτουργήσει σωστά η κρυπτογραφία δημοσίου κλειδιού, τα ιδιωτικά κλειδιά πρέπει να προστατεύονται. Έχουν ανακαλυφθεί διάφοροι τρόποι προκειμένου να υπάρχει αυξημένο επίπεδο προστασίας, ώστε ένας χρήστης να μπορεί να μεταφέρει ασφαλώς το ιδιωτικό κλειδί του. Οι έξυπνες κάρτες (βλ. και παράγραφο 2.4.1) είναι ένας από τους πιο αποτελεσματικούς τρόπους. Οι τεχνολογίες για έξυπνες κάρτες και αναγνώστες έξυπνων καρτών για προσωπικούς υπολογιστές είναι ήδη διαθέσιμες και κυμαίνονται σε λογικά πλαίσια κόστους.

1.3.1 Παραδείγματα Αλγορίθμων Ασύμμετρης Κρυπτογραφίας

RSA

Το σύστημα RSA είναι ένα σύστημα ασύμμετρης κρυπτογραφίας που προσφέρει τεχνικές κρυπτογράφησης και ψηφιακές υπογραφές. Αναπτύχθηκε 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: λαμβάνουμε 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 και η ανακάλυψη μιας εύκολης μεθόδου επίλυσης του προβλήματος θα αχρήστευε το κρυπτοσύστημα.

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 στον χρήστη Β ένα έγγραφο m. Ο Α κρυπτογραφεί το έγγραφο με την εξής εξίσωση: $c = m^e \bmod n$, όπου (n,e) είναι το δημόσιο κλειδί του Β. Ο Β, όταν παραλάβει το μήνυμα θα εφαρμόσει την εξής εξίσωση: $m = c^d \bmod n$, όπου (n,d) το ιδιωτικό κλειδί του Β. Η μαθηματική σχέση που έχουν 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 m 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: $s = m^d \bmod n$, όπου d και n

είναι το ιδιωτικό κλειδί του Α. Για να επαληθεύσει την υπογραφή ο Β εκτελεί την πράξη: m = se mod n, όπου e και n το δημόσιο κλειδί του Α.

DSA (Digital Signature Algorithm)

Το National Institute of Standards and Technology (NIST) δημοσιοποίησε το Digital Signature Algorithm (DSA), που είναι μέρος του Capstone Project της κυβέρνησης των Ηνωμένων Πολιτειών, το Μάιο του 1994. Έχει καθιερωθεί ως ο επίσημος αλγόριθμος παραγωγής ψηφιακών υπογραφών της κυβέρνησης των ΗΠΑ.

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 επιβεβαίωση 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 DSA έχει ολοκληρωθεί σε πολλά συστήματα ασφαλείας, αν και έχει λάβει πολλές αρνητικές κριτικές. Κυριότερες αδυναμίες του θεωρούνται η έλλειψη ευελιξίας, η αργή επαλήθευση των υπογραφών, η αδυναμία συνεργασίας με άλλα πρωτόκολλα πιστοποίησης ταυτότητας και τέλος ότι ο αλγόριθμος δεν είχε αποκαλυφθεί.

1.4 Βασικοί μηχανισμοί και διαδικασίες Κρυπτογραφίας

Η παράγραφος αυτή έχει ως στόχο την συνοπτική περιγραφή των βασικών μηχανισμών και διαδικασιών που λαμβάνουν χώρα κατά την διεκπεραίωση κρυπτογραφικών λειτουργιών. Συνήθως η χρήση των μηχανισμών αυτών αποτελεί στοιχειώδες βήμα μιας συνολικότερης κρυπτογραφικής λειτουργίας. Οι μηχανισμοί που περιγράφονται εδώ είναι βασισμένοι σε ευρέως διαδεδομένα πρότυπα.

1.4.1 Συμφωνία κλειδιών

Με τον όρο συμφωνία κλειδιών εννοούμε τη διαδικασία επίλυσης του ακόλουθου προβλήματος: δύο οντότητες θέλουν να συμφωνήσουν στην πληροφορία κρυπτογραφικών κλειδιών μυστικά πάνω από ένα ανοιχτό κατανεμημένο δίκτυο. Προκειμένου να επιτευχθεί η ασφαλής συμφωνία χρησιμοποιούνται πρωτόκολλα συμφωνίας κλειδιών (key agreement protocols) τα οποία είναι θεμιτό να έχουν τα ακόλουθα χαρακτηριστικά:

- **Γνωστά κλειδιά συνόδου**: ένα πρωτόκολλο επιτυγχάνει το στόχο του παρά το γεγονός ότι κάποιος έχει υποκλέψει κάποια από τα κλειδιά προηγούμενων συνόδων.
- **(Τέλεια) πρόσθια μυστικότητα (perfect forward secrecy)**: Εάν κάποιο από τα κρυπτογραφικά μυστικά που χρησιμοποιούνται για μια ή περισσότερες οντότητες υποκλαπούν, η μυστικότητα προηγούμενων κλειδιών συνόδων δεν επηρεάζεται.
- **Άγνωστο μοίρασμα κλειδιού**: η οντότητα Α δεν μπορεί να εξαναγκαστεί να μοιραστεί το κλειδί της με την οντότητα Β χωρίς η Α να το γνωρίζει, για παράδειγμα όταν ο Α πιστεύει ότι μοιράζεται το κλειδί με μια οντότητα Γ που είναι διαφορετική της Β.
- **Απομίμηση με υποκλοπή κλειδιού**: Εάν υποθέσουμε ότι το κρυπτογραφικό μυστικό του i που χρησιμοποιείται στην συμφωνία υποκλέπτεται, τότε ο υποκλοπέας που γνωρίζει την τιμή του μπορεί να υποδυθεί τον i, εφόσον αυτή η τιμή ακριβώς χαρακτηρίζει τον i. Ενδέχεται παρ' όλα αυτά, αυτή η απώλεια να μην επιτρέπει στον υποκλοπέα να υποδυθεί το ρόλο άλλων οντοτήτων πέραν του i.
- **Απώλεια πληροφορίας**: Η υποκλοπή πληροφορίας που δεν θα ήταν υπό κανονικές συνθήκες διαθέσιμη στον υποκλοπέα, δεν επηρεάζει την ασφάλεια του πρωτοκόλλου.
- **Ανεξαρτησία μηνυμάτων**: Ανεξάρτητες ροές ενός πρωτοκόλλου που τρέχουν ανάμεσα σε δύο έντιμες οντότητες δε σχετίζονται μεταξύ τους.

Ένα από τα πιο γνωστά πρωτόκολλα συμφωνίας κλειδιών είναι αυτό των Diffie-Hellman το οποίο περιγράφεται στο RFC 2631 (Diffie-Hellman Key Agreement Method) [DH] και παρουσιάζεται συνοπτικά στη συνέχεια. Άλλα πρωτόκολλα είναι το Station-To-Station (STS) [STS] (που βασίζεται στο Diffie-Hellman), η αυθεντικοποίηση με τον Κέρβερο (Kerberos) [Kerberos].

Παραδείγματα Αλγορίθμων 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. Όπως έχει ήδη αναφερθεί, 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 δημοσιοποιημένες 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 $g^k = n \bmod p$.

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 $g^a \bmod p$ και του Β είναι $g^b \bmod p$. Στην συνέχεια ανταλλάσσουν τις δημόσιες τιμές τους. Τέλος, ο Α κάνει τον υπολογισμό $g^{ab} = (g^b)^a \bmod p$ και Β κάνει με την σειρά του τον υπολογισμό $g^{ba} = (g^{a)b} \bmod p$. Επειδή $g^{ab} = g^{ba} = k$, ο Α και Β έχουν τώρα ένα κοινό μυστικό κλειδί. Το πρωτόκολλο εξαρτάται από το γεγονός ότι είναι αδύνατον να υπολογιστεί το k από τις δημόσιες τιμές $g^a \bmod p$ και $g^b \bmod p$ χωρίς την 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 Α και Β και όταν ανταλλάσσουν τις δημόσιες τιμές τους τις αντικαθιστά με τις δικές του. Δηλαδή όταν ο Α μεταδίδει την δημόσια τιμή του στον Β, ο C την αντικαθιστά με τη δική του και την στέλνει στον Β και ομοίως όταν ο Β στέλνει τη δημόσια τιμή του στον Α. Σαν συνέπεια, οι C και Α συμφωνούν σε ένα μυστικό κλειδί και οι C και Β συμφωνούν σε ένα άλλο κλειδί. Έτσι ο C μπορεί να διαβάσει τα μηνύματα που μεταδίδουν ο Α στον Β 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 τα ιδιωτικά κλειδιά των Α και Β, ενώ χρησιμοποιούνται και πιστοποιητικά για την απόκτηση των σωστών δημόσιων κλειδιών. Ο C ακόμα και αν είναι σε θέση να παρακολουθεί την επικοινωνία των Α και Β, 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 να χρησιμοποιηθεί και ένα προσυμφωνημένο συμμετρικό κλειδί.

Ας υποθέσουμε ότι ο χρήστης Α θέλει να στείλει μήνυμα στον χρήστη Β. Ο Α επιλέγει ένα συμμετρικό κλειδί και κρυπτογραφεί το μήνυμα με αυτό. Έπειτα κρυπτογραφεί το μυστικό συμμετρικό κλειδί με το δημόσιο κλειδί του Β. Στέλνει στο Β το κρυπτογραφημένο μήνυμα συνοδευόμενο από το κρυπτογραφημένο κλειδί. Όταν ο Β 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.

1.4.2 Συναρτήσεις κατακερματισμού

Μια συνάρτηση κατακερματισμού (hash function) Η είναι ένας μετασχηματισμός που λαμβάνει μια είσοδο μεταβλητού μήκους m και επιστρέφει μια συμβολοακολουθία σταθερού μήκους, που ονομάζεται τιμή της συνάρτησης h, δηλαδή h = H(m). Οι συναρτήσεις κατακερματισμού με αυτή την ιδιότητα βρίσκουν εφαρμογή σε μια πληθώρα περιπτώσεων, αλλά όταν χρησιμοποιούνται στην κρυπτογραφία συνήθως επιλέγονται ώστε να διαθέτουν και επιπλέον ιδιότητες.

Οι βασικές απαιτήσεις από μια κρυπτογραφική συνάρτηση κατακερματισμού είναι οι ακόλουθες:

- Η είσοδος να είναι οποιουδήποτε μήκους.
- Η έξοδος να έχει σταθερό μέγεθος.
- Η H(x) να είναι εύκολο να υπολογιστεί για οποιοδήποτε δεδομένο x.
- Η H(x) είναι μονόδρομη (one-way).
- Η H(x) είναι ανθεκτική σε συγκρούσεις (collision-free).

Μια συνάρτηση κατακερματισμού Η είναι μονόδρομη όταν είναι δύσκολο να αντιστραφεί, όπου ο όρος «δύσκολο» σημαίνει ότι για μια δεδομένη τιμή της συνάρτηση h, είναι υπολογιστικά αδύνατο να βρεθεί κάποια είσοδος x έτσι ώστε H(x)=h.

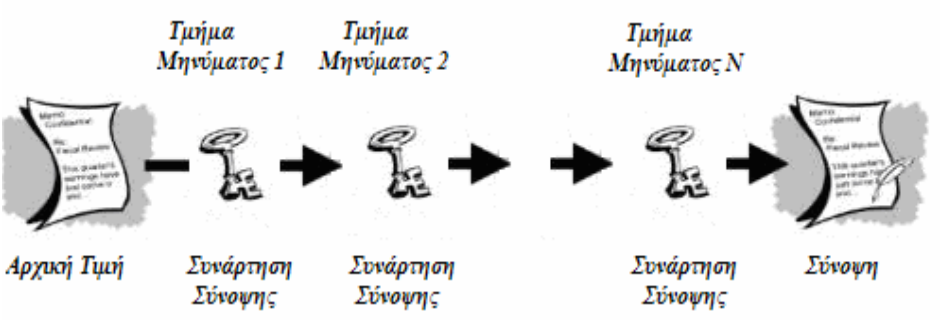
Εάν για ένα δεδομένο μήνυμα x, είναι υπολογιστικά αδύνατο να βρεθεί ένα μήνυμα y το οποίο είναι διαφορετικό από το x έτσι ώστε H(x) = H(y), τότε η H χαρακτηρίζεται ως μια συνάρτηση κατακερματισμού ασθενώς ανθεκτική στις συγκρούσεις (weakly collision-free).

Μια ισχυρά ανθεκτική στις συγκρούσεις (strongly collision-free) συνάρτηση κατακερματισμού H χαρακτηρίζεται αυτή για την οποία είναι υπολογιστικά αδύνατο να βρεθούν οποιαδήποτε δύο μηνύματα x και y για τα οποία H(x)=H(y).

Η τιμή της συνάρτησης κατακερματισμού αναπαριστά με συνέπεια το μήνυμα ή έγγραφο από το οποίο υπολογίστηκε. Πρακτικά παρουσιάζει συνοπτικά το μεγαλύτερο μήνυμα ή έγγραφο, για αυτό καλείται και σύνοψη μηνύματος (message digest ή hash). Κάποιος θα μπορούσε να θεωρήσει την τιμή αυτή ως ένα «ψηφιακό δακτυλικό αποτύπωμα» του εγγράφου ("digital fingerprint"). Παραδείγματα των πλέον διαδεδομένων συναρτήσεων κατακερματισμού είναι οι MD2 [MD2], MD5 [MD5] και SHA1 [SHA1], κάποιες συνοπτικές πληροφορίες για τις οποίες παρουσιάζονται στην επόμενη παράγραφο.

Σχήμα 3: *Συνάρτηση Κατακερματισμού (hash function)*

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 μιας συνάρτησης κατακερματισμού, μια συνάρτηση συμπίεσης μπορεί να πραγματοποιηθεί με την επανειλημμένη εφαρμογή της συναρτήσεων σύνοψης έως ότου ολόκληρο το μήνυμα έχει υποστεί επεξεργασία. Πιο αναλυτικά, το μήνυμα τεμαχίζεται σε τμήματα (blocks), των οποίων το μέγεθος εξαρτάται από την συνάρτηση σύνοψης, και συμπληρώνεται (padded) για λόγους ασφαλείας, ώστε το μήκος του μηνύματος να είναι πολλαπλάσιο του μήκους του block. Το παρακάτω σχήμα επιδεικνύει την λογική της διαδικασίας.



Σχήμα 4: *Συνάρτηση Συμπίεσης*

Μια βασική χρήση των κρυπτογραφικών συναρτήσεων κατακερματισμού επιτελείται στην παροχή ψηφιακών υπογραφών όπως περιγράφεται στη συνέχεια στην παράγραφο 1.4.5, όπου συνδυάζονται με κρυπτογραφία δημοσίου κλειδιού. Επιπλέον η τιμή μιας συνάρτησης μπορεί να δημοσιευθεί χωρίς να αποκαλύπτονται τα περιεχόμενα του εγγράφου από το οποίο προκύπτει. Αυτό βρίσκει εφαρμογή στην ψηφιακή χρονοσφράγιση (digital timestamping), όπου χρησιμοποιώντας συναρτήσεις κατακερματισμού, κάποιος μπορεί να λάβει ένα χρονοσφραγισμένο έγγραφο χωρίς να αποκαλύπτει τα περιεχόμενα του εγγράφου στην υπηρεσία χρονοσφράγισης.

Παραδείγματα Συναρτήσεων 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)

Και οι τρεις 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 κατα-

σκευή 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 υπόκειται επεξεργασία με τη συνάρτηση σύνοψης. Τα τμήματα που διαχειρίζεται η συνάρτηση σύνοψης έχουν μήκος 512 bits και κάθε τμήμα υπόκειται πλήρη επεξεργασία 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.

1.4.3 Αλγόριθμοι κρυπτογράφησης τμημάτων

Οι αλγόριθμοι κρυπτογράφησης τμημάτων (block ciphers) είναι ένας τύπος αλγορίθμων συμμετρικής κρυπτογράφησης που μετατρέπει ένα τμήμα μη κρυπτογραφημένου κειμένου, καθορισμένου μεγέθους (plaintext), σε ίδιου μεγέθους τμήμα κρυπτογραφημένου κειμένου (ciphertext). Αυτός ο μετασχηματισμός πραγματοποιείται με τη βοήθεια ενός μυστικού κλειδιού που παρέχεται από το χρήστη. Η αποκρυπτογράφηση γίνεται με την εφαρμογή του αντίστροφου μετασχηματισμού στο κρυπτογραφημένο κείμενο χρησιμοποιώντας το ίδιο μυστικό κλειδί. Το καθορισμένο μήκος καλείται *μέγεθος τμήματος (block size)*.

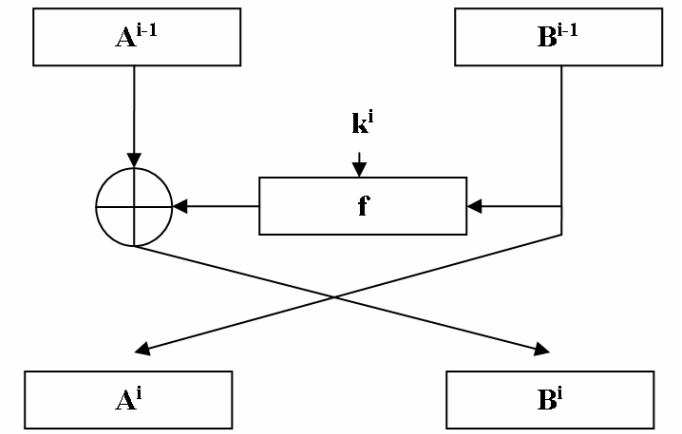
Οι αλγόριθμοι τμημάτων λειτουργούν επαναληπτικά, κρυπτογραφώντας ένα τμήμα διαδοχικά αρκετές φορές. Σε κάθε γύρο, ο ίδιος μετασχηματισμός εφαρμόζεται στα δεδομένα χρησιμοποιώντας ένα υπό-κλειδί. Το σύνολο των υπό-κλειδιών προέρχεται από το μυστικό κλειδί που χορήγησε ο χρήστης, με ειδική συνάρτηση. Το σύνολο των υπό-κλειδιών καλείται πρόγραμμα κλειδιών.

Ο αριθμός των επαναλήψεων του επαναληπτικού αλγορίθμου εξαρτάται από το επιθυμητό επίπεδο ασφάλειας και την απόδοση του συστήματος. Στις περισσότερες περιπτώσεις, ο αυξημένος αριθμός επαναλήψεων βελτιώνει την προσφερόμενη ασφάλεια, αλλά για μερικούς αλγόριθμους ο αριθμός των επαναλήψεων που απαιτούνται για να επιτευχθεί ικανοποιητική ασφάλεια είναι πολύ μεγάλος για να πραγματοποιηθεί.

Οι αλγόριθμοι Feistel [Feistel] είναι ειδικές περιπτώσεις επαναληπτικών αλγορίθμων όπου το κρυπτογραφημένο κείμενο υπολογίζεται ως εξής:

1. το κείμενο χωρίζεται στο μισό.
2. η συνάρτηση f εφαρμόζεται στο ένα μισό με χρήση ενός υπό-κλειδιού και η έξοδος της f περνάει από λογική πράξη X-OR με το άλλο μισό.
3. το αποτέλεσμα της λογικής πράξης γίνεται είσοδος της f (με νέο υπόκλειδί) και το προηγούμενο μισό το οποίο μετασχηματίστηκε γίνεται μία από τις εισόδους της επόμενης X-OR.
4. ο αλγόριθμος συνεχίζεται με τον ίδιο τρόπο και στο τέλος της τελευταίας επανάληψης, τα δύο κρυπτογραφημένα μισά συνενώνονται.

Σχηματικά η παραπάνω διαδικασία φαίνεται στο Σχήμα 5 όπου τα τμήματα εισόδου του i-στου γύρου επανάληψης συμβολίζονται με $\mathbf{A}^{i-1}$ και $\mathbf{B}^{i-1}$ και οι έξοδοι που τροφοδοτούνται στην επόμενη επανάληψη με $\mathbf{A}^{i}$ και $\mathbf{B}^{i}$. Το κλειδί κάθε επανάληψης συμβολίζεται με $\mathbf{k}^{i}$.



Σχήμα 5: *Αλγόριθμος Feistel*

Ένα σημαντικό χαρακτηριστικό του Feistel είναι ότι η αποκρυπτογράφηση είναι δομικά ταυτόσημη με την κρυπτογράφηση. Τα υπό-κλειδιά χρησιμοποιούνται σε αντίστροφη σειρά στην αποκρυπτογράφηση. Οι αλγόριθμοι Feistel κα-

λούνται και DES-like ciphers. Άλλοι γνωστοί αλγόριθμοι τμημάτων είναι ο DES [DES] και ο AES [AES].

1.4.4 Αλγόριθμοι κρυπτογράφησης ροών

Ένας αλγόριθμος κρυπτογράφησης ροών (Stream cipher) είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης. Είναι εξαιρετικά ταχείς αλγόριθμοι, κατά πολύ ταχύτεροι από τους αλγόριθμους τμημάτων. Σε αντίθεση με τους αλγόριθμους τμημάτων που λειτουργούν με μεγάλα τμήματα δεδομένων, οι αλγόριθμοι ροών τυπικά λειτουργούν με μικρότερες μονάδες απλού κειμένου, συνήθως με bits. Η κρυπτογράφηση ενός συγκεκριμένου κειμένου με έναν αλγόριθμο τμήματος θα καταλήγει πάντα στο ίδιο αποτέλεσμα όταν χρησιμοποιείται το ίδιο κλειδί. Με έναν αλγόριθμο ροών όμως, ο μετασχηματισμός των μικρότερων αυτών μονάδων θα ποικίλει, ανάλογα με το πότε λαμβάνονται κατά τη διάρκεια της κρυπτογράφησης.

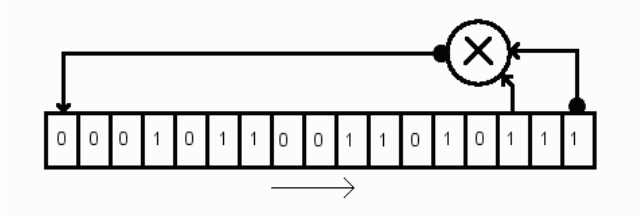
Ένας αλγόριθμος ροών παράγει μια ακολουθία από bits που χρησιμοποιείται σαν κλειδί και καλείται κλειδοροή (keystream). Η κρυπτογράφηση επιτυγχάνεται με το συνδυασμό της κλειδοροής με το plaintext, συνήθως μέσω πράξης X-OR. Η παραγωγή της κλειδοροής μπορεί να είναι ανεξάρτητη του plaintext και του ciphertext (οπότε μιλάμε για σύγχρονο αλγόριθμο – synchronous stream cipher) ή μπορεί να εξαρτάται από αυτά (οπότε μιλάμε για αυτοσυγχρονιζόμενο αλγόριθμο - self-synchronizing stream cipher). Οι περισσότεροι αλγόριθμοι ροών είναι σύγχρονοι.

Οι αλγόριθμοι ροών βασίζονται στις θεωρητικές ιδιότητες ενός one-time pad. One-time pads (καμιά φορά καλούνται και Vernam ciphers) είναι αλγόριθμοι που χρησιμοποιούν μια ακολουθία bits (η κλειδοροή που αναφέρθηκε παραπάνω) που παράγεται τελείως στην τύχη. Η κλειδοροή έχει το ίδιο μέγεθος με το μη κρυπτογραφημένο κείμενο και συνδυάζεται μέσω μιας πράξης X-OR με αυτό για την παραγωγή του ciphertext. Επειδή η κλειδοροή είναι τελείως τυχαία και έχει το ίδιο μέγεθος με το plaintext, η εύρεση του κειμένου είναι αδύνατη ακόμα και με τη διάθεση τεράστιας υπολογιστικής ισχύος. Ένας τέτοιος αλγόριθμος προσφέρει τέλεια μυστικότητα και ασφάλεια και έχει χρησιμοποιηθεί σε μεγάλη κλίμακα σε καιρό πολέμου για την διασφάλιση διπλωματικών καναλιών. Το γεγονός, όμως, ότι το μυστικό κλειδί (δηλαδή η κλειδοροή), που χρησιμοποιείται μόνο μία φορά, έχει το ίδιο μέγεθος με το μήνυμα, εισάγει σημαντικό πρόβλημα στην διαχείριση του κλειδιού. Παρ' όλη την ασφάλεια που προσφέρει, ο one-time pad δεν μπορεί να εφαρμοστεί στην πράξη.

Οι αλγόριθμοι ροών αναπτύχθηκαν σαν μια προσέγγιση της λειτουργίας ενός one-time pad. Βέβαια δεν είναι σε θέση παρέχουν τη θεωρητική ασφάλεια ενός time-pad αλλά είναι εφαρμόσιμοι και πρακτικοί. Ο πιο ευρέως χρησιμοποιούμενος αλγόριθμος ροών είναι ο RC4 [RC4]. Ενδιαφέρον παρουσιάζει το γεγονός ότι συγκεκριμένοι τρόποι λειτουργίας ενός αλγόριθμου τμημάτων (όπως

π.χ. του DES) προσομοιάζουν έναν αλγόριθμο ροών. Ακόμα και έτσι, οι αυθεντικοί αλγόριθμοι ροών είναι αρκετά ταχύτεροι.

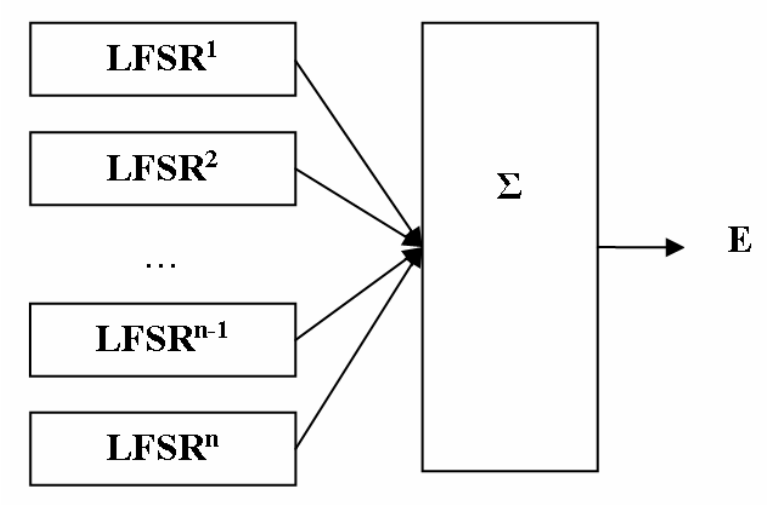
Ένας μηχανισμός για την παραγωγή της κλειδοροής είναι ο Καταχωρητής Γραμμικής Ολίσθησης με Ανάδραση (Linear Feedback Shift Register – LFSR) (βλ. Σχήμα 6).



Σχήμα 6: *Ένα 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. Η κλειδοροή δεν αποτελεί πλέον το μυστικό κλειδί (όπως στους one-time pads) λόγω του μεγέθους της. Η συμπεριφορά του καταχωρητή ρυθμίζεται από ένα ρολόι και σε κάθε χρονική στιγμή τα bits μετακινούνται μία θέση δεξιά, τη στιγμή που το X-OR 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 όσο και υπό μορφή υλικού, ενώ η λειτουργία τους είναι ταχύτατη. Οι ακολουθίες bit, όμως, που δημιουργούνται από ένα και μοναδικό LFSR δεν είναι ασφαλής καθ' ότι τον τελευταίο καιρό έχει αναπτυχθεί μια δυνατή μαθηματική φόρμουλα που επιτρέπει την ανάλυση του μηχανισμού και εύρεση της κλειδοροής. Απαιτείται, λοιπόν, η συνδυασμένη χρήση πολλών LFSR όπως φαίνεται στο ακόλουθο σχήμα.



Σχήμα 7: *Παράλληλη σύνδεση από n LFSR με τις εξόδους τους να συνδυάζονται από την Σ*

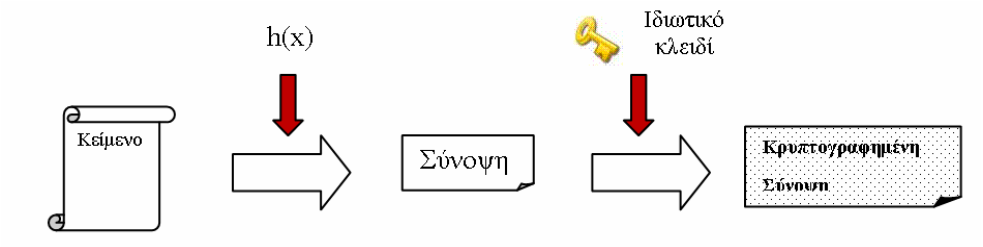
Ένας συνδυασμός LFSR είναι ο Shift Register Cascade [Gollman]. Αποτελείται από ενά σύνολο από LFSR που συνδέονται μεταξύ τους με τέτοιο τρόπο ώστε η συμπεριφορά του ενός να εξαρτάται από την συμπεριφορά του άλλου. Αυτό επιτυγχάνεται συνήθως με την χρήση του ενός LFSR να ελέγχει το ρολόι του άλλου. Άλλο παράδειγμα τέτοιου συνδυασμού είναι ο Shrinking Generator [Coppersmith] που αναπτύχθηκε από τους Coppersmith, Krawczyk και Mansour. Βασίζεται στην αλληλεπίδραση των εξόδων δύο LFSR. Τα bits της μιας εξόδου χρησιμοποιούνται για να καθορίσουν, μέσω κατάλληλης τεχνικής, εάν τα bits της δεύτερης εξόδου θα συμπεριληφθούν στην κλειδοροή. Είναι απλός και έχει καλά χαρακτηριστικά ασφάλειας. Άλλοι γνωστοί αλγόριθμοι ροών είναι οι A5/1 [A5/1], A5/2 [A5/2] (χρησιμοποιούμενοι στην τηλεφωνία) και ο ISAAC [ISAAC].

1.4.5 Ψηφιακές υπογραφές

Το γεγονός ότι στην ασύμμετρη κρυπτογραφία το ιδιωτικό κλειδί το έχει μόνο ο ιδιοκτήτης του, σημαίνει ότι το αποτέλεσμα οποιασδήποτε συνάρτησης χρησιμοποιεί το κλειδί αυτό, μπορεί να θεωρηθεί ότι έχει επιτελεστεί από το συγκεκριμένο ιδιοκτήτη και κανέναν άλλο. Μια ψηφιακή υπογραφή δημιουργείται από την χρήση του ιδιωτικού κλειδιού προκειμένου να «υπογραφούν» ηλεκτρονικά δεδομένα, με τέτοιο τρόπο που να μην μπορεί να πλαστογραφηθεί.

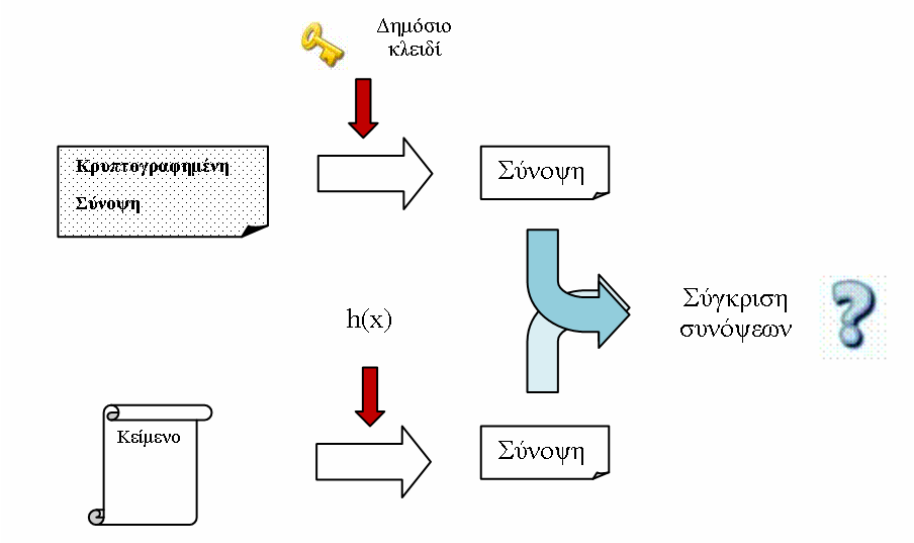
Στο ακόλουθο σχήμα παρουσιάζεται η τυπική διαδικασία δημιουργίας μιας ψηφιακής υπογραφής. Αρχικά εφαρμόζεται μια συνάρτηση κατακερματισμού h(x) στο κείμενο που θα υπογραφεί. Στη συνέχεια η σύνοψη που προκύπτει κρυπτογραφείται με το ιδιωτικό κλειδί του υπογράφοντος σύμφωνα με ένα συ-

γκεκριμένο αλγόριθμο και έτσι προκύπτει μια κρυπτογραφημένη σύνοψη. Αυτή ακριβώς η κρυπτογραφημένη σύνοψη αποτελεί την «ψηφιακή υπογραφή» και αποστέλλεται μαζί με το κείμενο στον παραλήπτη, συνοδευμένη από το δημόσιο κλειδί του αποστολέα.



Σχήμα 8: *Παραγωγή ψηφιακών υπογραφών με κρυπτογραφία δημοσίου κλειδιού*

Η επαλήθευση της ψηφιακής υπογραφής ακολουθεί μια παρόμοια διαδικασία που αποτελείται από δύο υποεργασίες. Στην πρώτη υποεργασία χρησιμοποιείται ο ίδιος αλγόριθμος μαζί με το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφηθεί η σύνοψη. Στη δεύτερη υποεργασία, χρησιμοποιείται η ίδια συνάρτηση κατακερματισμού h(x) που εφαρμόστηκε και κατά την δημιουργία της υπογραφής για να ληφθεί και πάλι η σύνοψη του κειμένου. Στο τελευταίο βήμα συγκρίνονται οι δύο συνόψεις που έχουν προκύψει. Εάν είναι εντελώς όμοιες, τότε η ψηφιακή υπογραφή είναι έγκυρη και άρα είναι όντως υπογεγραμμένη από το συγκεκριμένο αποστολέα και δεν έχει αλλοιωθεί κατά την αποστολή. Εάν οι συνόψεις διαφέρουν τότε η υπογραφή είναι άκυρη.



Σχήμα 9: *Επαλήθευση ψηφιακής υπογραφής*

Όπως θα δούμε στο επόμενο κεφάλαιο, η κρίσιμη παράμετρος για την επιτυχία των ψηφιακών υπογραφών είναι το κατά πόσο είναι εύκολο ο παραλήπτης ενός μηνύματος να έχει πρόσβαση στο δημόσιο κλειδί του αποστολέα προκειμένου να μπορεί πάντα να επαληθεύσει μια υπογραφή. Αυτό αποτελεί βασικό ζήτημα των Υποδομών Δημοσίου Κλειδιού (βλ. παράγραφο 2.2).

Οι ψηφιακές υπογραφές είναι ισχυρότερες από τις γραπτές διότι η υπογραφή είναι μαθηματικά δεμένη με τα υπογεγραμμένα δεδομένα. Η ψηφιακή υπογραφή δεν μπορεί να μεταφερθεί από ένα κείμενο σε άλλο και οποιαδήποτε αλλαγή στα υπογεγραμμένα δεδομένα, ακυρώνει την υπογραφή.

Οι ψηφιακές υπογραφές χρησιμοποιούνται σε έναν αριθμό υπηρεσιών ασφάλειας. Προσδίδουν έλεγχο αυθεντικότητας ή αυθεντικοποίηση σε ένα μήνυμα, εξασφαλίζοντας ότι αυτό έχει προέλθει από έναν συγκεκριμένο χρήστη, ο οποίος είναι ο μοναδικός κάτοχος του ιδιωτικού κλειδιού. Η ψηφιακή υπογραφή προστατεύει το μήνυμα από μη εξουσιοδοτημένη παραποίηση προσδίνοντας έναν έλεγχο ακεραιότητας. Παρόλο που από μόνη της η υπογραφή δεν είναι αρκετή για να επιτύχει την υπηρεσία μη-άρνησης συμμετοχής (non-repudiation) (ή διαφορετικά μη αποδοχής ευθύνης), μια ψηφιακή υπογραφή κατασκευασμένη σε συνδυασμό με κατάλληλα δεδομένα μπορεί να παρέχει ένα μέρος της υπηρεσίας μη-άρνησης (βλ. και παράγραφο 2.5.3 Προηγμένες Ηλεκτρονικές Υπογραφές).

Τα πιο γνωστά συστήματα ασύμμετρης κρυπτογραφίας με τα οποία δημιουργούνται ψηφιακές υπογραφές είναι των Fiege-Fiat-Shamir (FFS) [FFS], το ElGamal [ElGamal], το DSS [DSS] και συστήματα βασισμένα στον RSA [RSA].

1.4.6 Κώδικες Αυθεντικοποίησης Μηνυμάτων

Ένας Κώδικας Αυθεντικοποίησης Μηνύματος ΚΑΜ (Message Authentication Code – MAC) αποτελεί ένα κομμάτι πληροφορίας που χρησιμοποιείται για την αυθεντικοποίηση ενός μηνύματος. Ένας αλγόριθμος ΚΑΜ δέχεται ως είσοδο ένα μυστικό κλειδί και ένα μήνυμα τυχαίου μεγέθους (το οποίο θέλουμε να αυθεντικοποιήσουμε) και έχει ως έξοδο το ΜΑΚ (ή όπως αλλιώς αναφέρεται ετικέτα – tag).

Οι συναρτήσεις που παράγουν ΜΑΚ είναι παρόμοιες με τις συναρτήσεις κατακερματισμού, αλλά έχουν διαφορετικές απαιτήσεις ασφάλειας. Για να θεωρείται ασφαλής, ένας ΜΑΚ πρέπει να ανθίσταται σε πλαστογραφία κατόπιν επιθέσεως. Αυτό σημαίνει ότι ακόμη και αν κάποιος επιτιθέμενος έχει πρόσβαση σε ένα «μαντείο» που κατέχει το μυστικό κλειδί και μπορεί να δημιουργεί ΜΑΚ για μηνύματα, δεν θα μπορεί ποτέ να μαντέψει το ΜΑΚ ενός μηνύματος για το οποίο δεν έχει ρωτήσει ακόμη το «μαντείο» (δηλαδή θα είναι υπολογιστικά αδύνατο).

Επίσης διαφέρουν από τις ψηφιακές υπογραφές στο ότι οι ΚΑΜ υπολογίζονται και επαληθεύονται με το ίδιο κλειδί, οπότε μπορούν να επαληθευτούν μόνο από τον παραλήπτη που το έχει (οι ψηφιακές υπογραφές μπορούν να επαληθευτούν από οποιονδήποτε).

Οι ΚΑΜ μπορούν να κατηγοριοποιηθούν ως:

- Ασφαλείς χωρίς συνθήκες
- Βασισμένοι σε συναρτήσεις κατακερματισμού
- Βασισμένοι σε αλγορίθμους ροών (stream ciphers)
- Βασισμένοι σε αλγορίθμους τμημάτων (block ciphers)

Οι Simmons και Stinson πρότειναν έναν ασφαλή χωρίς συνθήκες ΚΑΜ που βασίζεται σε κρυπτογράφηση με χρήση ενός one-time pad [Kahn]. Το ciphertext του μηνύματος αυθεντικοποιεί τον εαυτό του εφόσον κανένας άλλος δεν έχει πρόσβαση στο one-time pad. Παρ' όλα αυτά, θα πρέπει να υπάρχει πλεονασμός πληροφορίας στο μήνυμα. Ένας ασφαλής ΚΑΜ χωρίς συνθήκες μπορεί να ληφθεί επίσης με την χρήση ενός μυστικού κλειδιού μιας χρήσης (one-time secret key).

Οι ΚΑΜ βασισμένοι σε συναρτήσεις κατακερματισμού χρησιμοποιούν ένα ή περισσότερα κλειδιά σε συνδυασμό με μια συνάρτηση κατακερματισμού για να παράγουν ένα άθροισμα ελέγχου που προστίθεται στο μήνυμα. Ένα παράδειγμα είναι ο αλγόριθμος keyed-MD5.