ΤΕΙ ΗΠΕΙΡΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ Υ/Η – ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

Άρτα Ιανουάριος 2014

Κρυπτογραφία και ψηφιακή υπογραφή

Πτυχιακή εργασία

Ζούζιας Βασίλειος

Υπεύθυνος καθηγητής

Σακκάς Λάμπρος

Άρτα Ιανουάριος 2014

Δήλωση περί μη λογοκλοπής

Η παρούσα πτυχιακή εργασία δεν αποτελεί αντιγραφή ούτε προέρχεται από ανάθεση σε τρίτους. Οι πηγές που χρησιμοποιήθηκαν αναφέρονται σαφώς στη βιβλιογραφία και στο κείμενο ενώ κάθε εξωτερική βοήθεια, αν υπήρξε, αναγνωρίζεται ρητά.

Περιεχόμενα

1.Πρόλογος

Η ανάγκη για ασφαλή αποθήκευση και μετάδοση πληροφορίας είναι αναπόσπαστο κομμάτι της ανθρώπινης ιστορίας. Αυτή η ανάγκη αρχικά δημιουργήθηκε λόγω των διαφορών των ανθρώπων σε επίπεδο κοινωνικών και πολιτικών, πεποιθήσεων. Σήμερα, η ραγδαία ανάπτυξη των επικοινωνιακών συστημάτων προσφέρει, σε ένα μεγάλο ποσοστό ανθρώπων, πρόσβαση σε μία τεράστια ποσότητα πληροφορίας και μία ποικιλία από ηλεκτρονικά μέσα με σκοπό την ανταλλαγή προσωπικών δεδομένων. Για αυτό το λόγο, κάθε πληροφορία που μεταδίδεται χρειάζεται να μετατραπεί σε μία μη αναγνωρίσιμη μορφή έτσι ώστε να διασφαλιστεί η ασφάλειά της.

Μια από τις μεθόδους που χρησιμοποιούνται για την ασφαλή διακίνηση των πληροφοριών στο σύγχρονο περιβάλλον, είναι η κρυπτογραφία. Η κρυπτογραφία αποτέλεσε μια πανάρχαια μέθοδο εξασφάλισης της εμπιστευτικότητας των συναλλαγών, όπως προκύπτει από ιστορικές αναφορές. Εξακολουθεί επίσης, έως και σήμερα να συμβάλλει στον παραπάνω στόχο, καθώς η ίδια αποτελεί μια πολύ βασική τεχνολογία στον τομέα της ασφάλειας του Internet.

Η κρυπτογραφία, αρχικά είχε σαν πεδία εφαρμογής της τον στρατό και την διπλωματία. Στην εποχή μας με την ανάπτυξη της τεχνολογίας η χρησιμότητά της κρίνεται απολύτως αναγκαία. Το πεδίο εφαρμογής ευρύ, περιλαμβάνοντας όλους τους τομείς στους οποίους η ασφαλής μετάδοση παίζει κύριο λόγο. Ψηφιακές συναλλαγές, επικοινωνίες καθώς και πλήθος άλλων εφαρμογών έχουν εισβάλλει στην καθημερινότητά μας οι οποίες πρέπει να διασφαλίσουν την εγκυρότητα τους. Έτσι δημιουργήθηκε η ανάγκη για την κατασκευή σχημάτων ψηφιακών υπογραφών.

Ένα σχήμα ψηφιακής υπογραφής είναι το ανάλογο μιας χειρόγραφης υπογραφής για κάθε είδους ψηφιακή συναλλαγή ή επικοινωνία. Μια έγκυρη ψηφιακή υπογραφή διαβεβαιώνει στον παραλήπτη ενός μηνύματος ποιος είναι ο αποστολέας και αν έχει τροποποιηθεί το μήνυμα κατά την μεταφορά του.

1.1.Ορολογία

Κρυπτολογία **(Cryptology)** είναι η επιστήμη που ασχολείται με τη μελέτη της απόκρυψης της ασφαλούς επικοινωνίας και ανάκτησης πληροφορίας. Διαχωρίζεται σε δύο κλάδους:

Την ***Κρυπτογραφία*** **(Cryptography)**: Ο όρος προέρχεται από τις λέξεις ‘κρυπτός’ και ‘γράφος’. Κυριολεκτικά σημαίνει τη μελέτη της μυστικογραφίας. Γενικότερα αφορά τον επιστημονικό κλάδο που ασχολείται με τη μελέτη, χρήση και ανάπτυξη τεχνικών κρυπτογράφησης και αποκρυπτογράφησης για την απόκρυψη των περιεχομένων των μηνυμάτων (ή των αποθηκευμένων

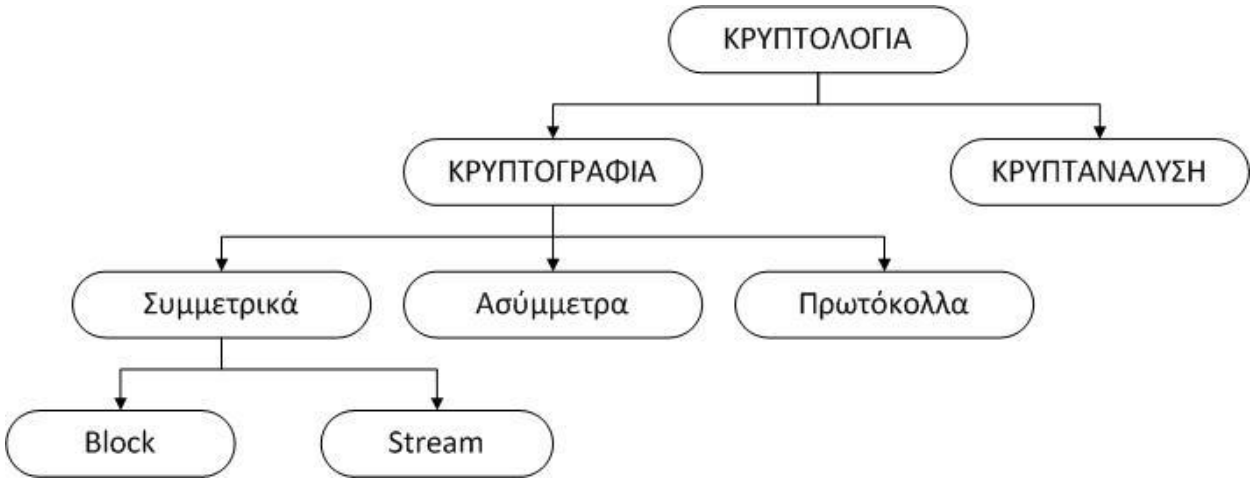
δεδομένων) και τη διευκόλυνση της ανίχνευσης κακόβουλων μετατροπών στα μηνύματα.

Την ***Κρυπτανάλυση*** **(Cryptanalysis)**: Αποτελεί τη διαδικασία της προσπάθειας αποκάλυψης του αρχικού κειμένου ή του κλειδιού από μη εξουσιοδοτημένες οντότητες. Η στρατηγική που χρησιμοποιείται από τον κρυπταναλυτή εξαρτάται από τη φύση της κρυπτογράφησης και από τις πληροφορίες που είναι διαθέσιμες σε αυτόν.

Κρυπτογράφηση **(encryption / encipherment)** είναι η διεργασία μετασχηματισμού ενός μηνύματος σε μια ακατανόητη μορφή με τη χρήση ενός κρυπτογραφικού αλγόριθμου, έτσι ώστε αυτό να μην είναι αναγνώσιμο από τρίτα μέρη (εκτός του νόμιμου παραλήπτη).

Αποκρυπτογράφηση **(decryption / decipherment)** είναι η διεργασία ανάκτησης του αρχικού μηνύματος (αναγνώσιμη μορφή) από μια ακατανόητη έκδοσή του που είχε παραχθεί μέσω μιας διεργασίας κρυπτογράφησης. Η αποκρυπτογράφηση εκτελείται από κάποιο εξουσιοδοτημένο μέρος, σε αντίθεση με την κρυπτανάλυση.

Μία επισκόπιση της *Κρυπτολόγους* φαίνεται στο παρακάτω σχήμα.



Σχήμα 1.1: Επισκόπηση κρυπτολογίας.

Αρχικό κείμενο (plaintext) είναι το μήνυμα το οποίο αποτελεί είσοδο σε μια διαδικασία κρυπτογράφησης, δηλαδή κρυπτογραφείται.

Κρυπτογραφημένο κείμενο (cipher text) είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγορίθμου πάνω στο αρχικό κείμενο. Το κρυπτογραφημένο κείμενο αποκρυπτογραφείται για να ανακτηθεί το αρχικό κείμενο.

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με βάση τη βοήθεια ενός αλγορίθμου κρυπτογράφησης και ενός κλειδιού κρυπτογράφησης.

Κρυπτογραφικός αλγόριθμος (cipher) είναι η μέθοδος (συνήθως μια μαθηματική συνάρτηση) μετασχηματισμού δεδομένων σε μια μορφή που να μην επιτρέπει σε μη εξουσιοδοτημένα μέρη την αποκάλυψη του περιεχομένου τους.

Η δυνατότητα, όμως, της διατήρησης της μυστικότητας των πληροφοριών βασίζεται περισσότερο στο ***κλειδί (key)*** που είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στην συνάρτηση κρυπτογράφησης. Επομένως, η ανθεκτικότητα μιας κρυπτογράφησης εξαρτάται περισσότερο από το μέγεθος των κλειδιών που χρησιμοποιούνται παρά από τους αλγορίθμους. Όσο μεγαλύτερο είναι το μήκος ενός κλειδιού τόσο ανθεκτικότερη είναι η κρυπτογράφηση.

1.2. Έννοιες θεωρίας αριθμών.

Η θεωρία αριθμών και οι αλγεβρικές δομές τα τελευταία χρόνια χρησιμοποιούνται όλο και περισσότερο στην κρυπτολογία. Αριθμο-θεωρητικοί αλγόριθμοι χρησιμοποιούνται σήμερα ευρέως εξαιτίας εν μέρει της ανακάλυψης των κρυπτογραφικών σχημάτων τα οποία στηρίζονται σε μεγάλους πρώτους αριθμούς.

Στη θεωρία αριθμών ασχολούμαστε με το σύνολο Z = {…, –2, – 1, 0, 1, 2, …} των ακεραίων και το σύνολο N = {0, 1, 2, …} των φυσικών αριθμών. Μια από τις κεντρικές έννοιες είναι αυτή της διαιρετότητας. Έστω δύο ακέραιοι a και d. Ο d διαιρεί τον a, συμβολικά d | a, σημαίνει ότι a = kd για κάποιον ακέραιο k. Κάθε ακέραιος διαιρεί το 0. Αν a > 0 και d | a, τότε |d| ≤ a. Αν d | a, τότε λέμε και ότι ο a είναι πολλαπλάσιο του d. Αν τώρα ο d δεν διαιρεί τον a, γράφουμε d ? a.

Αν d | a και d ≥ 0, ο d λέγεται διαιρέτης του a. Αν d | a, τότε a = kd ή ισοδύναμα a = (–k)(–d), που σημαίνει ότι d | a αν και μόνον αν –d | a, οπότε χωρίς βλάβη της γενικότητας μπορούμε να ορίσουμε τους διαιρέτες να είναι μη αρνητικοί, έχοντας κατά νου ότι ο αντίθετος (αρνητικός) οποιουδήποτε διαιρέτη του a διαιρεί επίσης τον a. Αν d είναι ένας διαιρέτης ενός ακέραιου a ≠ 0 τότε ισχύει 1 ≤ d ≤ |a|.

Για παράδειγμα, οι διαιρέτες του 18 είναι 1, 2, 3, 6, 9 και 18. Κάθε ακέραιος a έχει σαν τετριμμένους διαιρέτες τους 1 και a. Οι μη τετριμμένοι διαιρέτες του a λέγονται και παράγοντες του a. Για παράδειγμα, οι παράγοντες του 24 είναι 2, 3, 4, 6, 8 και 12. Ένας ακέραιος a > 1 του οποίου οι μόνοι διαιρέτες είναι οι τετριμμένοι διαιρέτες 1 και a λέγεται ότι είναι πρώτος αριθμός ή απλά πρώτος. Οι πρώτοι παίζουν σημαντικότατο ρόλο στη θεωρία αριθμών επειδή έχουν χαρακτηριστικές ιδιότητες.

Κατά σειρά αύξοντος μεγέθους οι ακέραιοι 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, …, 389, …, 2003 είναι πρώτοι. Αποδεικνύεται ότι υπάρχουν άπειροι πρώτοι. Ένας ακέραιος a > 1 ο οποίος δεν είναι πρώτος λέγεται ότι είναι σύνθετος αριθμός ή απλά σύνθετος. Για παράδειγμα, ο 15 είναι σύνθετος γιατί 3 | 15. Κατά σειρά αύξοντος μεγέθους οι ακέραιοι 4, 6, 8, 9, 10, …, $666 = 2 \cdot 3^2 \cdot 37$, …, $2001 = 3 \cdot 23 \cdot 29$, … είναι σύνθετοι. Ο ακέραιος 1 δεν είναι πρώτος ούτε σύνθετος. Ένας λόγος γι αυτό είναι ότι, όπως θα δούμε παρακάτω, το Θεώρημα 2.5 λέει ότι ένας σύνθετος γράφεται κατά μοναδικό τρόπο ως γινόμενο πρώτων οπότε αν ο 1 ήταν πρώτος η μοναδικότητα θα τινάζονταν στον αέρα. Επίσης να αναφέρουμε ότι ο 1 λέγεται ότι είναι μια μονάδα (unit), γιατί έχει αντίστροφο στο Z. Παρόμοια, ο ακέραιος 0 και όλοι οι αρνητικοί ακέραιοι δεν είναι ούτε πρώτοι ούτε σύνθετοι.

Η έννοια της διαίρεσης είναι στενά συνδεδεμένη με την πρόσθεση και μάλιστα με το πρόβλημα της καλύτερης προσέγγισης ενός φυσικού αριθμού a από τον φυσικό αριθμό n, με n < a. Για τον λόγο αυτό θεωρούμε την ακολουθία a, a – n, a –2n, …, a – qn, … .

Η καλύτερη προσέγγιση επιτυγχάνεται όταν η διαφορά a – qn είναι θετική και γίνει η μικρότερη δυνατή.

Η τιμή του q για την οποία συμβαίνει αυτό είναι το γνωστό μας πηλίκο της διαίρεσης a δια n και ο αριθμός r = a – qn είναι το υπόλοιπο. Έτσι ο φυσικός a γράφεται στη μορφή a = qn + r όπου το υπόλοιπο είναι αυστηρά μικρότερο του n αφού διαφορετικά η διαφορά a – (q + 1)n θα ήταν η καλύτερη προσέγγιση. Τα παραπάνω μας οδηγούν, γενικεύοντας στους ακέραιους, στο γνωστό Θεώρημα της Διαίρεσης.

– Για κάθε ακέραιο a και οποιονδήποτε θετικό ακέραιο n, υπάρχουν μοναδικοί ακέραιοι q και r τέτοιοι ώστε 0 ≤ r < n και a = qn + r.

Η τιμή q, συμβολικά a div n, είναι το πηλίκο της διαίρεσης και είναι $q = \lfloor a/n \rfloor$, όπου $\lfloor x \rfloor$ είναι ο μεγαλύτερος ακέραιος που δεν υπερβαίνει τον αριθμό x. Η τιμή r είναι το υπόλοιπο της διαίρεσης και συμβολίζεται με a mod n:

$$a \bmod n = a - \lfloor a/n \rfloor n$$

Έτσι, για κάθε ακέραιο a και θετικό ακέραιο n μπορούμε πάντα να γράφουμε $a = \lfloor a/n \rfloor n + a \bmod n$ όπου ο a mod n είναι ένας ακέραιος στο διάστημα, 0 ≤ a mod n < n. Έχουμε ότι n | a αν και μόνον αν a mod n = 0. Καλούμε το a mod n ως το μικρότερο μη αρνητικό κατάλοιπο του a, modulo n. Επίσης, λέμε ότι το a mod n είναι το αποτέλεσμα της αναγωγής του a, modulo n.

Για παράδειγμα, αν a = 73, n = 17, τότε q = 4 και r = 5. Έτσι, 73 mod 17 = 5 και 73 div 17 = 4. Επίσης αν a = 34, n = 17, τότε 34 mod 17 = 0 αφού 34 = 2·17.

Γενικεύοντας την (2.1) μπορούμε να ορίσουμε μια συνάρτηση ‘‘mod’’ ως εξής:

$$a \bmod n = \begin{cases} a & , \text{για } n = 0 \\ a - \lfloor a/n \rfloor n & , \text{διαφορετικά} \end{cases}$$

Να σημειώσουμε ότι ο ορισμός αυτός έχει νόημα για όλους τους ακέραιους a και n.

1.3.Κρυπτογραφικό σύστημα

Ένα ***Κρυπτογραφικό Σύστημα*** είναι ένα πλήρες σύστημα που περιλαμβάνει όλους τους ανθρώπους, διαδικασίες, εργαλεία, κρυπτογραφήματα, κλειδιά και κανάλια μετάδοσης που εμπλέκονται σε μια ασφαλή μεταφορά δεδομένων. Σε ένα τυπικό σύστημα κρυπτογράφησης τα δεδομένα κρυπτογραφούνται και το παραγόμενο μήνυμα αποστέλλεται στον παραλήπτη και αποκρυπτογραφείται για

να παραχθεί το αρχικό κείμενο. Αυτοί οι μετασχηματισμοί αναπαρίστανται ως εξής:

Εικόνα 1.2.: Κρυπτογραφικό σύστημα.

1.3.1.Ασφάλεια.

Κάθε σύστημα πρέπει να παρέχει ένα πακέτο ασφάλειας που να μπορεί να εξασφαλίσει τη μυστικότητα του. Έστω ότι δύο άτομα Α και Β επικοινωνούν μεταξύ τους μέσω ενός διαύλου επικοινωνίας. Η επικοινωνία μεταξύ τους είναι ασφαλής, εάν ικανοποιεί τις ακόλουθες ιδιότητες:

Εμπιστευτικότητα (Confidentiality): Αναφέρεται στο πως περισσότεροι άνθρωποι πιστοποιούν ένα ασφαλές σύστημα. Κανείς άλλος, εκτός από τους εξουσιοδοτημένους χρήστες, δεν μπορεί να λάβει γνώση οποιουδήποτε μέρους της πληροφορίας που ανταλλάσσεται μεταξύ τους.

Ακεραιότητα (Integrity): Το περιεχόμενο των δεδομένων που ανταλλάσσονται εξασφαλίζεται πως δεν κινδυνεύει από κανενός τύπου τροποποίηση που μπορεί να συμβεί ανάμεσα στους συναλλασσόμενους (αποστολέας-παραλήπτης). Κανείς άλλος δεν μπορεί να τροποποιήσει τα μηνύματα τους.

Αυθεντικότητα (Authentication): Καθένας από τους Α και Β πρέπει να είναι σίγουρος για την ταυτότητα του μηνύματος που λαμβάνει από τον άλλον. Αυτό σημαίνει πως πριν την αποστολή και λήψη δεδομένων χρησιμοποιώντας το σύστημα, ο αποστολέας και ο παραλήπτης θα πρέπει να έχουν ταυτοποιηθεί.

Αδυναμία αποκήρυξης (Non repudiation): Κανείς από τους δύο να μην μπορεί να αρνηθεί την πατρότητα προηγούμενων μηνυμάτων του.

Αξιοπιστία και Διαθεσιμότητα (Service Reliability and Availability): Τα συστήματα θα πρέπει να παρέχουν μία εγγύηση ποιότητας των υπηρεσιών στους χρήστες τους, αφού ακόμα και ασφαλή συστήματα συχνά δέχονται επιθέσεις από εισβολείς. Αυτό μπορεί να επηρεάσει την διαθεσιμότητα και το είδος των υπηρεσιών που παρέχουν στους χρήστες.

Για να αποφεύγονται οι αποκαλούμενες επιθέσεις εκτενών αναζητήσεων πρέπει το πλήθος των πιθανών διαφορετικών συνδυασμών κλειδιών για έναν κρυπτογραφικό αλγόριθμο να είναι μεγάλο. Αυτό συμβαίνει γιατί σε περίπτωση

που ο κρυπταναλυτής αποκτήσει ένα αντίστοιχο ζεύγος αρχικού και κρυπτογραφημένου κειμένου, μπορεί προσπαθώντας με όλα τα πιθανά κλειδιά να δει ποιο ταιριάζει και κατόπιν να το χρησιμοποιήσει για να αποκρυπτογραφεί κι άλλα κρυπτογραφημένα κείμενα που έχουν κρυπτογραφηθεί με το ίδιο κλειδί. Διαφορετικά, σε περίπτωση που απλά κατάφερε να υποκλέψει ένα κρυπτογραφημένο κείμενο, μπορεί να το αποκρυπτογραφήσει με διαφορετικούς συνδυασμούς κλειδιών μέχρι να βρει ένα αρχικό κείμενο που έχει λογική σημασία, οπότε τότε αποκτά, ουσιαστικά, και το σωστό κλειδί που στη συνέχεια μπορεί να το χρησιμοποιήσει για την αποκρυπτογράφηση και άλλων κρυπτογραφημένων κειμένων.

Τυπικά, τα κλειδιά είναι σειρές από bits και ως εκ τούτου η απαίτηση για μεγάλο πλήθος κλειδιών έχει την έννοια της χρήσης ολοένα και περισσότερων bits. Η χρήση 64 bits αποτελεί ένα τυπικό μήκος κλειδιού το οποίο παρέχει 264 ≅ 1019 διαφορετικά κλειδιά, που σημαίνει ότι αν είχαμε τη δυνατότητα να δοκιμάζαμε ένα κλειδί ανά nanosecond, δηλαδή 1.000.000.000 κλειδιά ανά δευτερόλεπτο, θα χρειαζόμασταν περίπου 300 χρόνια για να δοκιμάσουμε όλους τους δυνατούς συνδυασμούς κλειδιών.

Γενικά, όταν αναλύουμε την *ανθεκτικότητα* ενός κρυπτογραφικού αλγορίθμου, είναι σημαντικό να υποθέτουμε ότι ο κρυπταναλυτής έχει αποκτήσει με διάφορους τρόπους ένα αξιόλογο ποσό πληροφοριών στο οποίο βασίζει την επίθεσή του. Αυτό σημαίνει ότι όταν αναλύουμε την ασφάλεια ενός συστήματος είναι βασικό να κάνουμε υποθέσεις για την χειρότερη περίπτωση (worst case). Πιο συγκεκριμένα αποτελεί κοινή πρακτική ότι ο κρυπταναλυτής διαθέτει :

- Πλήρη γνώση του κρυπτογραφικού αλγορίθμου,
- Μερικά κρυπτογραφημένα μηνύματα που όλα έχουν προκύψει με τη χρήση του ίδιου μυστικού κλειδιού,
- Μερικά “γνωστά μηνύματα”, π.χ. μέρος ή το σύνολο από αρχικά μηνύματα που αντιστοιχούν σε γνωστά κρυπτογραφημένα μηνύματα.

Μια επιπρόσθετη πιθανή υπόθεση είναι ότι ο κρυπταναλυτής διαθέτει το κρυπτογραφημένο κείμενο που αντιστοιχεί σε ένα επιλεγμένο από τον ίδιο αρχικό κείμενο. Αυτού του είδους η επίθεση ονομάζεται *επίθεση επιλεγμένου αρχικού κειμένου* (chosen plaintext attack). Στην πράξη, αυτό θα απαιτούσε από τον κρυπταναλυτή το να μπορεί να εισάγει στο σύστημα μηνύματα της επιλογής του, κάτι που είναι αρκετά δύσκολο να γίνει.

Με βάση τις υποθέσεις για την χειρότερη περίπτωση, πρέπει να ακολουθούν δοκιμές με σκοπό να βρεθούν τρόποι κρυπτογραφικής ανάλυσης του κρυπτογραφικού αλγορίθμου, δηλαδή της εύρεσης του μυστικού κλειδιού. Σε αυτή την περίπτωση, ο σχεδιαστής του κρυπτογραφικού αλγορίθμου ή ο χρήστης που πρόκειται να χρησιμοποιήσει ένα προϊόν κρυπτογράφησης πρέπει να παίξει το ρόλο του κρυπτογραφικός αναλυτής και να δοκιμάσει να σπάσει τον αλγόριθμο. Με αυτόν τον τρόπο μόνο μπορεί κανείς να διαπιστώσει την ανθεκτικότητα ενός κρυπτογραφικού αλγορίθμου.

Στις περισσότερες περιπτώσεις οι κρυπτογραφικοί αλγόριθμοι θεωρείται ότι είναι ισχυροί εφόσον οι προσπάθειες των εξειδικευμένων κρυπταναλυτών δεν είναι αρκετές για να μπορούν να τους σπάσουν με συμβατικά μέσα και σε λογικούς χρόνους. Κατά τ' άλλα, δεν υπάρχουν φορμαλιστικές μέθοδοι που να αποδεικνύουν την ασφάλεια που παρέχουν οι περισσότεροι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται στην πράξη.

Όμως η κρυπτογραφία αποτελεί μια ραγδαία αναπτυσσόμενη περιοχή έρευνας και νέοι κρυπτογραφικοί αλγόριθμοι σχεδιάζονται και "σπάνε", αν και μερικοί αντέχουν καλά στις παρατεταμένες προσπάθειες κρυπτανάλυσης που γίνονται.

Αξιολόγηση ασφάλειας

Η ασφάλεια ενός κρυπτοσυστήματος είναι ένα αντικείμενο το οποίο μπορεί να εξεταστεί από πολλές πλευρές. Η ανάγκη καθορισμού αντικειμενικών μέτρων για την μέτρηση της ασφάλειας είχε ως αποτέλεσμα τη δημιουργία διαφόρων μαθηματικών μοντέλων.

- Ασφάλεια άνευ όρων (unconditionally secure) . Ένα κρυπτοσύστημα είναι άνευ όρων ασφαλές όταν το κρυπτοκείμενο δεν δίνει καμιά πληροφορία στον αντίπαλο σχετικά με το απλό κείμενο. Η υπόθεση απαιτεί ότι ο αντίπαλος έχει πλήρη υπολογιστική ισχύ στη διάθεσή του. Το μοντέλο αυτό διατυπώθηκε από το Shannon ,όπου η ασφάλεια εξετάζεται κάτω από το πρίσμα της θεωρίας της πληροφορίας. Σύμφωνα με τη θεωρία της πληροφορίας ένα κρυπτοσύστημα είναι άνευ όρων ασφαλές όταν η πιθανότητα που έχει ο αντίπαλος για να σπάσει το κρυπτοκείμενο είναι η ίδια με την πιθανότητα που θα έχει εάν του δοθεί λύση για ένα τμήμα του κρυπτοκειμένου.
- Υπολογιστική ασφάλεια (computationally secure).Σε αυτό το μοντέλο εισάγεται η παράμετρος της δυνατότητας χρήσης υπολογιστικής ισχύος του αντιπάλου. Ένα κρυπτοκείμενο είναι υπολογιστικά ασφαλές όταν προκειμένου να το σπάσει ο αντίπαλος απαιτείται υπολογιστική ισχύς πέραν των δυνατοτήτων του. Ο υπολογισμός γίνεται με βάση τον καλύτερο αλγόριθμο που γνωρίζει ο αντίπαλος προκειμένου να σπάσει το κρυπτοσύστημα. Ο προφανής αλγόριθμος που έχει για να σπάσει ένα κρυπτοσύστημα είναι αυτός της εξαντλητικής αναζήτησης (exhaustive search) όπου ο αντίπαλος δοκιμάζει ένα-ένα τα κλειδιά έως ότου ανακαλύψει το σωστό. Ο αναμενόμενος χρόνος ανακάλυψης του σωστού κλειδιού είναι ανάλογος του μισού του συνολικού αριθμού των κλειδιών. Σε ορισμένα κρυπτοσυστήματα έχουν ανακαλυφθεί και πιο «έξυπνοι» αλγόριθμοι αναζήτησης κλειδιών, που φτάνουν στο επιθυμητό αποτέλεσμα πιο γρήγορα από την εξαντλητική αναζήτηση. Συνεπώς, η

υπολογιστική ασφάλεια δεν εγγυάται την ασφάλεια ενός κρυπτο συστήματος, επειδή στο μέλλον μπορεί να ανακαλυφθεί αλγόριθμος κρυπτ ανάλυσης ο οποίος να μπορεί να εκτελεσθεί εντός των υπολογιστικών δυνατοτήτων του αντιπάλου.

- Ασφάλεια θεωρητικής πολυπλοκότητας (complexity theoretic). Θεωρείται ότι ο αντίπαλος μπορεί να πραγματοποιήσει επίθεση στο κρυπτοσύστημα η οποία απαιτεί πολυωνυμική υπολογιστική ισχύ. Δηλαδή, οι παράμετροι ασφάλειας του κρυπτοσυστήματος μπορούν να εκφραστούν πολυωνυμικά ως προς το χώρο και το χρόνο. Η ανάλυση με βάση το μοντέλο ασφάλειας θεωρητικής πολυπλοκότητας εξετάζει ασυμπτωτικά την αντοχή του κρυπτοσυστήματος σε κρυπταναλυτικές επιθέσεις και δεν έχει πρακτική αξία. Ωστόσο μια τέτοια ανάλυση μπορεί να οδηγήσει στη διαπίστωση θεμελιωδών εννοιών και αρχών ασφάλειας των κρυπτοσυστημάτων.
- Αποδείξιμη ασφάλεια (provable security). Ένα κρυπτοσύστημα είναι αποδείξιμα ασφαλές όταν μπορούμε να αποδείξουμε ότι η ασφάλειά του είναι ισοδύναμη κάποιου γνωστού και καλά μελετημένου προβλήματος που θεωρείται «δύσκολο». Παραδείγματα τέτοιων προβλημάτων βρίσκουμε στη θεωρία αριθμών, όπως η παραγοντοποίηση ενός μεγάλου σύνθετου αριθμού στους πρώτους παράγοντές του και ο υπολογισμός του διακριτού λογάριθμου ενός αριθμού. Τα κρυπτοσυστήματα που είναι αποδείξιμα ασφαλή ανήκουν σε υποσύνολο των συστημάτων που είναι υπολογιστικά ασφαλή, αλλά ένα κρυπτοσύστημα αποδείξιμης ασφάλειας έχει πολύ καλές προοπτικές να είναι ασφαλές, αφού το υποκείμενο «δύσκολο» πρόβλημα έχει υποστεί εκτενείς μελέτες και είναι γενικώς αποδεκτό ως «δύσκολο».

1.3.2. Διάκριση κρυπτογραφικών συστημάτων.

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

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

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

Τον αριθμό των κλειδιών που χρησιμοποιούνται:
Εάν ο πομπός και ο δέκτης χρησιμοποιούν το ίδιο κλειδί, τότε το σύστημα αναφέρεται ως ***συμμετρικό*** ή μοναδικού κλειδιού ή μυστικού κλειδιού ή συμβατικής κρυπτογραφίας. Εάν, όμως, ο πομπός και ο δέκτης χρησιμοποιούν διαφορετικά κλειδιά, τότε το σύστημα αναφέρεται ως ***ασύμμετρο***, ή σύστημα ζεύγους κλειδιών, ή κρυπτογραφίας δημοσίου κλειδιού.

Τον τρόπο με τον οποίο επεξεργάζεται το αρχικό κείμενο:

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

1.4.Ιστορική αναδρομή.

Ο όρος κρυπτογραφία συνδυάζει δύο ελληνικές λέξεις, τη λέξη κρυπτό που σημαίνει μυστικό και τη λέξη γράφος προκειμένου να προσδιοριστεί με ακρίβεια η λειτουργία της.
Η κρυπτογραφία έχει μια πάρα πολύ μεγάλη ιστορία, της οποίας η αρχή εντοπίζεται σύμφωνα με το βιβλίο του πριν από 4000 χρόνια περίπου και συνδέεται με τους Αιγύπτιους. Η ιστορία της μπορεί να χωριστεί σε τρείς περιόδους με σκοπό την καλύτερη κατανόηση της.
Έτσι η πρώτη περίοδος εκτείνεται από την πρώτη εμφάνιση της κρυπτογραφίας μέχρι και τον 19^{ο} αιώνα. Η επόμενη περίοδος ξεκινά από τις αρχές του 20^{ο} αιώνα και φτάνει μέχρι τη δεκαετία του 1950 από όπου και αρχίζει η τελευταία περίοδος της κρυπτογραφίας, η οποία συνεχίζεται στις μέρες μας.

1.4.1 Πρώτη περίοδος κρυπτογραφίας (1900 π.χ. – 1900 μ.Χ.)

Κατά τη διάρκεια αυτής της περιόδου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, που βασίζονταν κυρίως σε απλές αντικαταστάσεις γραμμάτων. Όλες αυτές δεν απαιτούσαν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές, αλλά στηρίζονταν στην ευφυΐα και την ευρηματικότητα των δημιουργών τους. Όλα αυτά τα συστήματα έχουν στις μέρες μας κρυπταναλυθεί και έχει αποδειχθεί ότι, εάν είναι γνωστό ένα μεγάλο κομμάτι του κρυπτογραφημένου μηνύματος, τότε το αρχικό κείμενο μπορεί σχετικά εύκολα να επανακτηθεί.

Όπως προκύπτει από μία μικρή σφηνοειδή επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, οι πολιτισμοί που αναπτύχθηκαν στη Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία ήδη από το 1500 π.Χ. Επίσης, ως το αρχαιότερο βιβλίο κρυπτοκωδικών στον κόσμο, θεωρείται μία σφηνοειδής επιγραφή στα Σούσα της Περσίας, η οποία περιλαμβάνει τους αριθμούς 1 έως 8 και από το 32 έως το 35, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καθένα σφηνοειδή σύμβολα.

Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Γύρω στον 5ο π.Χ. αιώνα εφηύραν την «σκυτάλη», την πρώτη κρυπτογραφική στην οποία χρησιμοποίησαν για την κρυπτογράφηση τη μέθοδο της αντικατάστασης.

Εικόνα 1.3.: Σπαρτιατική σκυτάλη

Στην αρχαιότητα χρησιμοποιήθηκαν κυρίως συστήματα, τα οποία βασίζονταν στη στεγανογραφία και όχι τόσο στην κρυπτογραφία. Οι Έλληνες συγγραφείς δεν αναφέρουν αν και πότε χρησιμοποιήθηκαν συστήματα γραπτής αντικατάστασης γραμμάτων, αλλά τα βρίσκουμε στους Ρωμαίους, κυρίως την εποχή του Ιουλίου Καίσαρα. Ο Ιούλιος Καίσαρας έγραφε στον Κικέρωνα και σε άλλους φίλους του, αντικαθιστώντας τα γράμματα του κειμένου, με γράμματα, που βρίσκονται 3 θέσεις μετά, στο Λατινικό Αλφάβητο.

Έτσι, σήμερα, το σύστημα κρυπτογράφησης που στηρίζεται στην αντικατάσταση των γραμμάτων του αλφαβήτου με άλλα που βρίσκονται σε καθορισμένο αριθμό θέσης πριν ή μετά, λέγεται κρυπτοσύστημα αντικατάστασης του Καίσαρα. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες.

1.4.2.Δεύτερη περίοδος κρυπτογραφίας (1900μ.χ-1950μ.χ)

Η δεύτερη περίοδος κρυπτογραφίας τοποθετείται στις αρχές του 20^{ου} αιώνα και φτάνει μέχρι το 1950. Επομένως καλύπτει τους δυο παγκοσμίους πολέμους,

εξαιτίας των οποίων η κρυπτογραφία αναπτύχθηκε τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια.
Τα κρυπτογραφικά συστήματα της περιόδου αυτής αρχίζουν να γίνονται πιο πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομαγνητικές συσκευές οι οποίες ονομάζονται κρυπτομηχανές.
Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά την διάρκεια της περιόδου αυτής η κρυπτανάλυση τους είναι συνήθως επιτυχημένη.
Οι Γερμανοί έκαναν εκτενή χρήση (σε διάφορες παραλλαγές) ενός συστήματος γνωστού ως **Enigma.**

Εικόνα 1.4.: Η μηχανή enigma.

Η μηχανή Enigma χρησιμοποιήθηκε ευρέως στη Γερμανία. Ο Marian Rejewski στην Πολωνία, προσπάθησε και τελικά παραβίασε την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma (που χρησιμοποιούσε μια ηλεκτρομηχανική κρυπτογραφική συσκευή) χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ήταν η μεγαλύτερη σημαντική ανακάλυψη στην κρυπτολογική ανάλυση της εποχής. Οι Πολωνοί συνέχισαν να αποκρυπτογραφούν τα μηνύματα που βασίζονταν στην κρυπτογράφηση με το Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε ορισμένες σημαντικές αλλαγές και οι Πολωνοί δεν μπόρεσαν να τις παρακολουθήσουν, επειδή η αποκρυπτογράφηση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν.
Έτσι, εκείνο το καλοκαίρι μεταβίβασαν τη γνώση τους, μαζί με μερικές μηχανές που είχαν κατασκευάσει στους Βρετανούς και τους Γάλλους. Ακόμη ο Rejewski με μαθηματικούς και κρυπτογράφους, όπως ο Biuro Szyfrow, κατέληξαν σε συνεργασία με τους Βρετανούς και τους Γάλλους μετά από αυτή την εξέλιξη. Η συνεργασία αυτή συνεχίστηκε από τον Άλαν Τούρινγκ (Alan Turing), τον Γκόρντον Ουέλτσμαν (Gordon Welchman) και από πολλούς άλλους στο Μπλέτσλεϊ Παρκ (Bletchley Park), κέντρο της Βρετανικής Υπηρεσίας κρυπτογράφησης-αποκρυπτογράφησης και οδήγησε σε συνεχείς αποκρυπτογραφήσεις των διαφόρων παραλλαγών του Enigma. Αυτό έγινε με τη

βοήθεια και ενός υπολογιστή, που κατασκεύασαν οι Βρετανοί επιστήμονες, ο οποίος ονομάστηκε Colossus και δυστυχώς καταστράφηκε με το τέλος του Πολέμου.

Οι κρυπτογράφοι του αμερικανικού ναυτικού (σε συνεργασία με Βρετανούς και Ολλανδούς κρυπτογράφους μετά από το 1940 έσπασαν αρκετά κρυπτο συστήματα του Ιαπωνικού ναυτικού. Το σπάσιμο ενός από αυτά του JN-25 οδήγησε στην αμερικανική νίκη, στη Ναυμαχία της Μιντγουέι, καθώς και στην εξόντωση του Αρχηγού του Ιαπωνικού Στόλου Ιζορόκου Γιαμαμότο.

Το Ιαπωνικό Υπουργείο Εξωτερικών χρησιμοποίησε ένα τοπικά αναπτυγμένο κρυπτοσύστημα, (που καλείται Purple), και χρησιμοποίησε, επίσης, διάφορες παρόμοιες μηχανές για τις συνδέσεις μερικών ιαπωνικών πρεσβειών. Μία από αυτές αποκλήθηκε "Μηχανή-Μ" από τις ΗΠΑ, ενώ μια άλλη αναφέρθηκε ως «Red» (Κόκκινη). Μια ομάδα του αμερικανικού στρατού, η αποκαλούμενη SIS, κατάφερε να σπάσει το ασφαλέστερο ιαπωνικό διπλωματικό σύστημα κρυπτογράφησης (μια ηλεκτρομηχανική συσκευή, η οποία αποκλήθηκε "Purple" από τους Αμερικανούς) πριν καν ακόμη αρχίσει ο Β΄ Παγκόσμιος Πόλεμος. Οι Αμερικανοί αναφέρονται στο αποτέλεσμα της κρυπτανάλυσης, ειδικότερα της μηχανής Purple, αποκαλώντας το ως Magic (Μαγεία).

Οι συμμαχικές κρυπτομηχανές που χρησιμοποιήθηκαν στον δεύτερο παγκόσμιο πόλεμο περιλάμβαναν το βρετανικό Type X και το αμερικανικό SIGABA. Και τα δύο ήταν ηλεκτρομηχανικά σχέδια παρόμοια στο πνεύμα με το Enigma, με σημαντικές βελτιώσεις. Κανένα δεν έγινε γνωστό ότι παραβιάστηκε κατά τη διάρκεια του πολέμου. Τα στρατεύματα στο πεδίο μάχης χρησιμοποίησαν το M-209 και τη λιγότερη ασφαλή οικογένεια κρυπτομηχανών M-94. Οι Βρετανοί πράκτορες της Υπηρεσίας "SOE" χρησιμοποίησαν αρχικά ένα τύπο κρυπτογραφίας που βασιζόταν σε ποιήματα (τα απομνημονευμένα ποιήματα ήταν τα κλειδιά). Οι Γερμανοί, ώρες πριν την Απόβαση της Νορμανδίας συνέλαβαν ένα μήνυμα - ποίημα του Πολ Βερλέν, για το οποίο, χωρίς να το έχουν αποκρυπτογραφήσει, ήταν βέβαιοι πως προανήγγειλε την απόβαση. Η Γερμανική ηγεσία δεν έλαβε υπόψη της αυτή την προειδοποίηση.

Οι Πολωνοί είχαν προετοιμαστεί για την εμπόλεμη περίοδο κατασκευάζοντας την κρυπτομηχανή LCD Lacida, η οποία κρατήθηκε μυστική ακόμη και από τον Rejewski. Όταν τον Ιούλιο του 1941 ελέγχθηκε από τον Rejewski η ασφάλειά της, του χρειάστηκαν μερικές μόνον ώρες για να την "σπάσει" και έτσι αναγκάστηκαν να την αλλάξουν βιαστικά.

Τα μηνύματα που εστάλησαν με Lacida τελικά δεν ήταν συγκρίσιμα με αυτά του Enigma, αλλά η παρεμπόδιση θα μπορούσε να έχει σημάνει το τέλος της κρίσιμης κρυπταναλυτικής Πολωνικής προσπάθειας.

1.4.3 Τρίτη περίοδος κρυπτογραφίας (1950 μ.χ.- Σήμερα)

Αυτή η περίοδος χαρακτηρίζεται από την έξαρση της ανάπτυξης στους επιστημονικούς κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει ουσιαστικά με τον Claude Shannon, ο οποίος θεωρείται αναμφισβήτητα ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας. Το 1949 δημοσίευσε το έγγραφο «Θεωρία επικοινωνίας των συστημάτων μυστικότητας» (Communication Theory of Secrecy Systems) στο τεχνικό περιοδικό Bell System και λίγο αργότερα στο βιβλίο του, «Μαθηματική Θεωρία της Επικοινωνίας» (Mathematical Theory of Communication), μαζί με τον Warren Weaver.Εκτός από τις άλλες εργασίες του επάνω στη θεωρία δεδομένων και επικοινωνίας καθιέρωσε μια στερεά θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση. Εκείνη την εποχή η κρυπτογραφία εξαφανίζεται και φυλάσσεται από τις μυστικές υπηρεσίες κυβερνητικών επικοινωνιών όπως η NSA.Πολύ λίγες εξελίξεις δημοσιοποιήθηκαν ξανά μέχρι τα μέσα της δεκαετίας του '70, όταν όλα άλλαξαν.

Στα μέσα της δεκαετίας του '70 έγιναν δύο σημαντικές δημόσιες (δηλ. μη-μυστικές) πρόοδοι. Πρώτα ήταν η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES (Data Encryption Standard) στον ομοσπονδιακό κατάλογο της Αμερικής στις 17 Μαρτίου 1975. Το προτεινόμενο DES υποβλήθηκε από την IBM, στην πρόσκληση του Εθνικού Γραφείου των Προτύπων (τώρα γνωστό ως NIST), σε μια προσπάθεια να αναπτυχθούν ασφαλείς ηλεκτρονικές εγκαταστάσεις επικοινωνίας για επιχειρήσεις όπως τράπεζες και άλλες μεγάλες οικονομικές οργανώσεις. Μετά από τις συμβουλές και την τροποποίηση από την NSA, αυτό το πρότυπο υιοθετήθηκε και δημοσιεύθηκε ως ένα ομοσπονδιακό τυποποιημένο πρότυπο επεξεργασίας πληροφοριών το 1977 (αυτήν την περίοδο αναφέρεται σαν FIPS 46-3). Ο DES ήταν ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης που εγκρίνεται από μια εθνική αντιπροσωπεία όπως η NSA. Η απελευθέρωση της προδιαγραφής της από την NBS υποκίνησε μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας.

Ο DES αντικαταστάθηκε επίσημα από τον AES το 2001 όταν ανήγγειλε ο NIST το FIPS 197. Μετά από έναν ανοικτό διαγωνισμό, ο NIST επέλεξε τον αλγόριθμο Rijndael, που υποβλήθηκε από δύο Φλαμανδούς κρυπτογράφους, για να είναι το AES. Ο DES και οι ασφαλέστερες παραλλαγές του όπως ο 3DES ή TDES χρησιμοποιούνται ακόμα σήμερα, ενσωματωμένος σε πολλά εθνικά και οργανωτικά πρότυπα. Το βασικό μέγεθος των 56-bit έχει αποδειχθεί ότι είναι ανεπαρκές να αντισταθεί στις επιθέσεις ωμής βίας (μια τέτοια επίθεση πέτυχε να σπάσει τον DES σε 56 ώρες ενώ το άρθρο που αναφέρεται ως το σπάσιμο του DES δημοσιεύτηκε από τον O'Reilly and Associates). Κατά συνέπεια, η χρήση

απλής κρυπτογράφησης με τον DES είναι επισφαλής για χρήση στα νέα σχέδια των κρυπτογραφικών συστημάτων και μηνύματα που προστατεύονται από τα παλαιότερα κρυπτογραφικά συστήματα που χρησιμοποιούν DES. Όλα τα μηνύματα που έχουν αποσταλεί από το 1976 με τη χρήση DES, διατρέχουν επίσης σοβαρό κίνδυνο αποκρυπτογράφησης. Ανεξάρτητα από την έμφυτη ποιότητά του, το βασικό μέγεθος του DES (56-bit) ήταν πιθανά πάρα πολύ μικρό ακόμη και το 1976, πράγμα που είχε επισημάνει ο Whitfield Diffie. Υπήρξε επίσης η υποψία ότι κυβερνητικές οργανώσεις είχαν ακόμα και τότε ικανοποιητική υπολογιστική δύναμη ώστε να σπάσουν μηνύματα που είχαν κρυπτογραφηθεί με τον DES.

1.5.Βασικές αρχές σχεδιασμού κρυπτογραφημάτων ομάδας.

1.5.1.Τα μέτρα του Shannon.

Ο Shannon, ο θεμελιωτής της θεωρίας της πληροφορίας διατύπωσε το 1949 ένα σύνολο από μέτρα τα οποία χαρακτηρίζουν ένα ορθά σχεδιασμένο αλγόριθμο κρυπτογράφησης.

1. Μήκος του κλειδιού. Η ευκολία χειρισμού του κλειδιού εξαρτάται από το μήκος του.

2. Βαθμός απαιτούμενης κρυπτογραφικής ασφάλειας. Το μέτρο αυτό αφορά το κέρδος του αντιπάλου σε πληροφορία, όταν παρατηρεί το κρυπτοκείμενο.

3. Πρακτική εκτέλεση της κρυπτογράφησης και της αποκρυπτογράφησης. Η προσπάθεια που απαιτείται για την κρυπτογράφηση και την αποκρυπτογράφηση σε χρόνο ή λειτουργίες.

4. Διόγκωση του κρυπτοκειμένου. Είναι επιθυμητό το κρυπτοκείμενο να έχει το ίδιο μήκος με το απλό κείμενο.

5. Διάδοση των σφαλμάτων κρυπτογράφησης. Είναι επιθυμητό ένα σφάλμα κατά την κρυπτογράφηση να επηρεάζει σε όσο το δυνατό μικρότερο βαθμό την αποκρυπτογράφηση.

Η ύπαρξη των μέτρων σε ένα κρυπτοσύστημα είναι υποχρεωτική, αλλά συγχρόνως και αντιφατική, με αποτέλεσμα να μην υπάρχει στην πραγματικότητα κρυπτοσύστημα το οποίο να ικανοποιεί όλα τα μέτρα στο μέγιστό τους. Για παράδειγμα, πλήρης έλλειψη του μέτρου 2 σημαίνει ότι ο αντίπαλος μπορεί να ανακτήσει πλήρως το απλό κείμενο, ή ακόμη καλύτερα, το απλό κείμενο να είναι αποδεκτό κρυπτοκείμενο. Η πλήρης έλλειψη των μέτρων 3 και 4 επιτρέπει κρυπτοσυστήματα που μπορούν να μεγιστοποιούν όλα τα άλλα μέτρα. Η πλήρης έλλειψη του μέτρου 5 δέχεται την ύπαρξη κρυπτοσυστήματος που μεγιστοποιεί όλα τα άλλα μέτρα, αλλά σε περίπτωση σφάλματος κατά την κρυπτογράφηση, η

ανάκτηση του απλού κειμένου θα ήταν αδύνατη, ακόμη και για κάποιο τμήμα αυτού.

1.5.2.Σύγχυση και διάχυση.

Δυο ιδιότητες που χρησιμοποιούνται στην αξιολόγηση της κρυπτογραφικής δύναμης είναι η σύγχυση και η διάχυση.

Έστω ένα απλό κείμενο το οποίο αντιστοιχεί σε ένα κρυπτοκείμενο μέσω ενός κρυπταλγορίθμου. Εάν αντικαταστήσουμε ένα σύμβολο του απλού κειμένου και κρυπτογραφήσουμε το νέο απλό κείμενο, τότε για ένα αλγόριθμο με υψηλή διάχυση, ο αντίπαλος δεν θα μπορεί να προβλέψει ποια σύμβολα του κρυπτο κειμένου θα μεταβληθούν ή γενικότερα θα επηρεαστούν.

Σύγχυση είναι η ικανότητα του αλγορίθμου κρυπτογράφησης όπου ο αντίπαλος δεν είναι σε θέση να προβλέψει ποιες μεταβολές θα συμβούν στο κρυπτο κείμενο, δεδομένης μια μεταβολής στο απλό κείμενο.

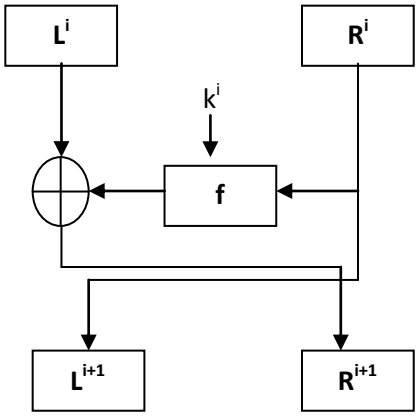
Δηλαδή ένας αλγόριθμος έχει υψηλή σύγχυση όταν οι σχέσεις μεταξύ του απλού κειμένου και του κρυπτοκειμένου είναι αρκετά πολύπλοκες, ώστε να χρειάζεται ο αντίπαλος να ξοδέψει σημαντικό χρόνο προκειμένου να τις προσδιορίσει.

Διάχυση είναι η ικανότητα του αλγορίθμου κρυπτογράφησης όπου ένα τμήμα του απλού κειμένου να έχει την ευκαιρία να επηρεάσει όσο το δυνατόν περισσότερα τμήματα του κρυπτοκειμένου.

Ένας αλγόριθμος έχει υψηλή διάχυση όταν ένα στοιχειώδες τμήμα του απλού κειμένου έχει την δυνατότητα να επηρεάσει όλα τα τμήματα του κρυπτοκειμένου, ανεξαρτήτως της τοποθεσίας του τμήματος αυτού του απλού κειμένου.

1.5.3.Δίκτυα Feistel.

Η κρυπτογραφική πράξη τύπου Feistel είναι της μορφής του σχήματος 1.5, η οποία αποτελεί και έναν γύρο σε κρυπτοσύστημα γινομένου. Το βασικό χαρακτηριστικό ενός δικτύου Feistel είναι η πλήρης ελευθερία στην επιλογή της συνάρτησης γύρου f. Η δομή του δικτύου Feistel είναι τέτοια ώστε η αντίστροφη σχέση ορίζεται πάντοτε, ακόμα και αν η συνάρτηση f δεν είναι ενριπτική. Επιπλέον, σε ορισμένες περιπτώσεις ένα δίκτυο Feistel μπορεί να είναι αποδείξιμα ασφαλές, όπως θα δείξουμε παρακάτω



Σχήμα 1.5. : Ένας γύρος Feistel

Σε κάθε γύρο η είσοδος χωρίζεται στο αριστερό και στο δεξιό τμήμα. Τα δύο τμήματα της εισόδου του i-οστού γύρου συμβολίζονται με L_{i-1}και R_{i-1}, ενώ οι έξοδοι συμβολίζονται με L_i και R_i. Στον πρώτο γύρο τα τμήματα L_0 και R_0 αντιστοιχούν στο απλό κείμενο, ενώ στον τελικό γύρο, τα τμήματα L_r και R_r αντιστοιχούν στο κρυπτοκείμενο. Κατά τον γύρο i, η συνάρτηση γύρου f δέχεται ως είσοδο το δεξιό τμήμα της εισόδου και το κλειδί k_i το οποίο προέρχεται από το πρόγραμμα κλειδιού. Η έξοδος της συνάρτησης συνδυάζεται με το αριστερό τμήμα της εισόδου με αποκλειστική διάζευξη και το αποτέλεσμα της πράξης αντιστοιχίζεται στο δεξιό τμήμα της εξόδου, ενώ το δεξιό τμήμα της εισόδου αντιστοιχίζεται στο αριστερό τμήμα της εξόδου. Η ανταλλαγή του αριστερού τμήματος με το δεξί έχει ως αποτέλεσμα ο επόμενος γύρος να εφαρμόσει το αποτέλεσμα της συνάρτησης σε εκείνο το τμήμα της εισόδου το οποίο μεταφέρθηκε ατόφιο από την είσοδο στην έξοδο. Είναι φανερό ότι σε κρυπτο σύστημα με έναν και μόνο γύρο, το δεξιό τμήμα του κρυπτοκειμένου θα είναι ίσο με το αριστερό τμήμα του απλού κειμένου. Αυτό είναι ένα χαρακτηριστικό της κρυπτογραφικής πράξης τύπου Feistel και θεωρητικά ένα δίκτυο όπου τα δύο τμήματα εισόδου έχουν το ίδιο μέγεθος, θα πρέπει να περιλαμβάνει τουλάχιστον τρεις γύρους προκειμένου το κρυπτοσύστημα να έχει τη δυνατότητα να αποκρύψει πλήρως το απλό κείμενο. Στην πράξη όμως απαιτούνται πολύ περισσότεροι γύροι για να είναι ένα κρυπτοσύστημα τύπου Feistel ασφαλές. Ο αριθμός των γύρων καθώς και η κρυπτογραφική δύναμη του κρυπτοσυστήματος εξαρτάται από τη συνάρτηση f.

Έστω nL και nR το μέγεθος σε bits του αριστερού και δεξιού τμήματος αντίστοιχα, με συνολικό μήκος εισόδου n = nL + nR. Η συνάρτηση γύρου θα ορίζει την αντιστοιχία F: $\{0,1\}^n{}_R$ $\{0,1\}^n{}_L$. Αν n = nR=n/2, το δίκτυο Feistel ονομάζεται ισορροπημένο. Η πράξη κρυπτογράφησης ορίζεται από την επανάληψη της κρυπτογραφικής πράξης:

$$e^i{}_{ki}\,(L^i, R^i) = L^{i-1} \,||\, (F\,(R^{i-1} \oplus, K^i) \qquad L^{i-1}, \quad \text{για } 0 < i < r$$

όπου a||b το δυαδικό τμήμα το οποίο αποτελείται από την αλληλουχία των τμημάτων a και b. Για το απλό κείμενο θα είναι p = L0||R0, ενώ για το κρυπτο κείμενο θα είναι c = Lr||Rr. Το κλειδί επιλέγεται σε κάθε γύρο από το πρόγραμμα κλειδιού{k1,k2,…,kr}. Κατά την αποκρυπτογράφηση εφαρμόζεται η ίδια πράξη, με τη διαφορά ότι το πρόγραμμα κλειδιού ακολουθεί την αντίστροφη σειρά, {kr,kr-1,…,k1}.

Το τμήμα της εισόδου το οποίο τροφοδοτείται στη συνάρτηση γύρου ονομάζεται προέλευση, ενώ το τμήμα της εισόδου στο οποίο εφαρμόζεται το αποτέλεσμα της συνάρτησης με αποκλειστική διάζευξη ονομάζεται στόχος. Αν το μέγεθος της πηγής είναι μεγαλύτερο από το μέγεθος του στόχου, τότε το δίκτυο ονομάζεται δίκτυο Feistel σημαίνουσας προέλευσης, ενώ στην περίπτωση που το μέγεθος του στόχου είναι μεγαλύτερο, το δίκτυο ονομάζεται δίκτυο Feistel σημαίνοντος στόχου. Αν το άθροισμα του μεγέθους της πηγής και του στόχου είναι ίσο με το μέγεθος της εισόδου, τότε το δίκτυο ονομάζεται τέλειο, ενώ στην περίπτωση που το άθροισμα της πηγής και του στόχου είναι μικρότερο, το δίκτυο ονομάζεται ατελές.

Σε ένα ατελές δίκτυο υπάρχει τμήμα της εισόδου το οποίο εμφανίζεται ατόφιο στη έξοδο και επιπλέον δεν συμπεριλαμβάνεται στην πράξη της συνάρτησης γύρου. Το τμήμα αυτό ονομάζεται μηδενικό.

Στη βιβλιογραφία το συντριπτικό ποσοστό στην έρευνα των δικτύων Feistel αποδίδεται σε ισορροπημένα δίκτυα Feistel, δηλαδή το αριστερό τμήμα της εισόδου είναι ο στόχος και είναι ίσο με το δεξιό τμήμα της εισόδου που είναι η προέλευση. Ο βασικός λόγος εκτενούς μελέτης των ισορροπημένων δικτύων Feistel είναι επειδή τα πιο διαδεδομένα κρυπτοσυστήματα τα οποία βασίζονται σε δίκτυα Feistel είναι ισορροπημένα, όπως το κρυπτοσύστημα DES που μελετάμε στο επόμενο κεφάλαιο. Ωστόσο, η ασύμμετρη κατανομή των τμημάτων της εισόδου σε δίκτυα Feistel σημαίνουσας προέλευσης και σημαίνοντος στόχου δημιουργεί υποψίες ότι ένα μη ισορροπημένο δίκτυο Feistel μπορεί να είναι κρυπτογραφικά αδύναμο. Στην περίπτωση του δικτύου Feistel σημαίνοντος στόχου θα υπάρχουν σε κάθε γύρο γραμμικές σχέσεις μεταξύ ορισμένων bits εισόδου με ορισμένα bits εξόδου. Στην περίπτωση δικτύου Feistel σημαίνουσας προέλευσης θα απαιτούνται περισσότεροι γύροι για να εμφανισθεί κάθε bit στο τμήμα του στόχου.

1.5.4.Ασφάλεια δικτύων Feistel.

Η μελέτη και τεκμηρίωση της ασφάλειας των δικτύων feistel είναι μια από τις πιο χαρακτηριστικές περιπτώσεις της σύγχρονης κρυπτογραφίας. Η προσέγγιση σε ένα αποδείξιμα ασφαλές κρυπτογραφικό σύστημα ακολουθεί τα εξής βασικά στάδια:

1.Αναγνώριση του προβλήματος, όπου ξεχωρίζουμε ένα πρόβλημα κρυπτογραφίας. Ένα από τα κλασικά προβλήματα, για παράδειγμα είναι: η είναι μονόδρομη συνάρτηση;

2.Καθορισμός του προβλήματος. Αυτό είναι ίσως το πιο βασικό στάδιο στο οποίο περιγράφουμε μαθηματικά το πρόβλημα.

3.Ανάπτυξη του πρωτοκόλλου το οποίο καθορίζει τα βήματα τα οποία θα ακολουθήσουμε για να αποδείξουμε την ασφάλεια του προβλήματος.

4.Καθορισμός της υποθέσεως η οποία αναφέρεται στις δυνατότητες του αντιπάλου.

5.Απόδειξη. Με βάση την υπόθεση, εκτελούμε το πρωτόκολλο για να προσδιορίσουμε αν το πρόβλημα το οποίο έχουμε καθορίσει οδηγεί σε ασφαλή κατασκευή.

1.6.Είδη κρυπτογράφησης.

Οι μέθοδοι οι οποίες χρησιμοποιούνται χωρίζονται σε δύο κατηγορίες: τη συμμετρική και την ασύμμετρη.

Η συμμετρική κρυπτογραφία, ή αλλιώς κρυπτογραφία ιδιωτικού κλειδιού βασίζεται στην ύπαρξη ενός μοναδικού κλειδιού, το οποίο χρησιμοποιείται, τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση δεδομένων. Στην πραγματικότητα το κλειδί αυτό είναι ένα σύνολο χαρακτήρων, με βάση το οποίο τα προγράμματα κρυπτογράφησης, με τη χρήση ειδικών αλγορίθμων, μετατρέπουν το κείμενο σε μη αναγνώσιμη μορφή. Στη συνέχεια το κείμενο αποστέλλεται στον παραλήπτη, ο οποίος για να το επαναφέρει στην αρχική του μορφή θα πρέπει να γνωρίζει το κλειδί αλλά και τους αλγορίθμους οι οποίοι χρησιμοποιήθηκαν για την κρυπτογράφηση του.

Αλγόριθμοι συμμετρικής κρυπτογράφησης υπάρχουν πολλοί, με πιο γνωστό τον αλγόριθμο des ο οποίος αναπτύχθηκε το 1977 από την εταιρία IMB και χρησιμοποιήθηκε από την κυβέρνηση των ΗΠΑ ως επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών.

Το σύστημα συμμετρικής κρυπτογραφίας δεν μπορεί να χρησιμοποιηθεί ευρέως, διότι ο παραλήπτης του μηνύματος θα πρέπει να γνωρίζει το κλειδί της κρυπτογράφησης κάτι που προϋποθέτει ότι θα πρέπει να σταλεί στον παραλήπτη μέσω ενός ασφαλούς διαύλου. Αν και έχουν αναπτυχθεί συστήματα τα οποία επιτρέπουν την ασφαλή ανταλλαγή κλειδιών μέσα από δημόσια δίκτυα, η κάλυψη των απαιτήσεων μεγάλου αριθμού χρηστών κάθε άλλο παρά εύκολη είναι, ενώ απαιτούνται και πρόσθετες διαδικασίες ασφαλείας σε ένα κεντρικό ασφαλή εξυπηρετητή (server).

Η αδυναμία αυτή της συμμετρικής κρυπτογράφησης οδήγησε στην καθιέρωση της ασύμμετρης κρυπτογράφησης ή κρυπτογράφησης δημόσιου κλειδιού ως του μοναδικού τρόπου που μπορεί να εγγυηθεί την ασφαλή μεταφορά δεδομένων. Οι αλγόριθμοι ασύμμετρης κρυπτογράφησης χρησιμοποιούν για τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης, δυο ξεχωριστά κλειδιά ένα δημόσιο και ένα ιδιωτικό τα οποία σχετίζονται μεταξύ τους. Τα κλειδιά που ανήκουν στο ζεύγος αυτό έχουν τη σημαντική ιδιότητα ότι είναι πρακτικά αδύνατος ο υπολογισμός του ενός κλειδιού γνωρίζοντας το άλλο.

Η φιλοσοφία των συστημάτων αυτών βασίζεται στη δυνατότητα δημοσίευσης των δημόσιων κλειδιών. Καθώς όπως αναφέραμε είναι πρακτικά αδύνατη η εύρεση του αντίστοιχου ιδιωτικού κλειδιού. Το δημόσιο κλειδί λοιπόν κοινοποιείται από κάθε χρήστη συνήθως μέσω ειδικών καταλόγων ή απευθείας από τον ένα χρήστη στον άλλο. Ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα, εξασφαλίζοντας με αυτό τον τρόπο ότι μόνο ο παραλήπτης που θα διαθέτει το σχετιζόμενο ιδιωτικό κλειδί μπορεί να το αποκρυπτογραφήσει. Επειδή όμως η μέθοδος αυτή έχει τον ίδιο δείκτη ασφαλείας με τη συμμετρική, απαιτεί περίπου χίλιες φορές περισσότερο χρόνο και δέκα φορές περισσότερα κλειδιά για να εκτελέσει τη διαδικασία κρυπτογράφησης- αποκρυπτογράφησης. Για το λόγο αυτό έχει επικρατήσει μια μέθοδος που συνδυάζει και τις δύο. Έτσι για την κωδικοποίηση ενός μηνύματος χρησιμοποιείται ένα προσωρινό τυχαίο κλειδί, το οποίο στη συνέχεια με τη βοήθεια του δημόσιου κλειδιού του παραλήπτη, κρυπτογραφείται και αποστέλλεται μαζί με το κωδικοποιημένο κείμενο. Στη συνέχεια ο παραλήπτης κάνοντας χρήση του ιδιωτικού κλειδιού του, αποκρυπτογραφεί το κλειδί και στη συνέχεια στέλνει το μήνυμα. Με τη διαδικασία αυτή επιτυγχάνεται η κρυπτογράφηση αρχείων με ασφάλεια που είναι υψηλότερη όσο μεγαλώνει το μέγεθος των χρησιμοποιούμενων κλειδιών.

Η κρυπτογράφηση δημόσιου κλειδιού είναι μια μορφή κρυπτογραφίας που γενικά επιτρέπει στους χρήστες να επικοινωνήσουν με ασφάλεια, χωρίς την κατοχή προγενέστερης πρόσβασης σε ένα κοινό μυστικό κλειδί, με τη χρησιμοποίηση ενός ζευγαριού κρυπτογραφικών κλειδιών, που ονομάζεται δημόσιο και ιδιωτικό κλειδί και συσχετίζονται μαθηματικά.

Στο πανεπιστήμιο Stanford, οι Diffie και Hellman το 1976 πρότειναν ένα διαφορετικό είδος κρυπτογραφικού συστήματος, στο οποίο τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης ήταν διαφορετικά.

Η μέθοδος αυτή της εκθετικής ανταλλαγής κλειδιών, είναι γνωστή ως ανταλλαγή Diffie - Hellman. Ήταν η πρώτη δημοσιευμένη πρακτική μέθοδος για ένα κοινό μυστικό κλειδί μεταδιδόμενο από ένα μη προστατευμένο κανάλι επικοινωνιών χωρίς χρησιμοποίηση προγενέστερου κοινού μυστικού.

Οι αλγόριθμοι δημόσιου κλειδιού είναι συνήθως βασισμένοι σε πολύπλοκα μαθηματικά προβλήματα. Ο RSA για παράδειγμα βασίζεται στη δυσκολία παραγοντοποίησης. Για λόγους αποδοτικότητας, χρησιμοποιούνται στην πράξη τα υβριδικά συστήματα κρυπτογράφησης όπου ένα ανταλλάσσεται χρησιμοποιώντας κρυπτογράφηση δημόσιου κλειδιού και το υπόλοιπο περιεχόμενο της επικοινωνίας κρυπτογραφείται χρησιμοποιώντας κρυπτογράφηση ιδιωτικού κλειδιού.

Η κρυπτογράφηση δημόσιου κλειδιού παρέχει επίσης μηχανισμούς για τη δημιουργία ψηφιακών υπογραφών, οι οποίες είναι ένας τρόπος να εξασφαλιστεί υψηλό επίπεδο εμπιστευτικότητας ότι το λαμβανόμενο μήνυμα εστάλη από τον σωστό αποστολέα. Οι υπογραφές συχνά θεωρούνται από τη νομοθεσία ως ψηφιακό ισοδύναμο των ψηφιακών υπογραφών. Υπό μια τεχνική έννοια, δεν είναι δεδομένο ότι δεν υπάρχει καμία φυσική επαφή μεταξύ του υπογράφοντος και του υπογεγραμμένου. Χρησιμοποιώντας τα κατάλληλα σχέδια και εφαρμογές υψηλής ποιότητας είναι δυνατό να επιτευχθεί ένας πολύ υψηλός βαθμός διαβεβαίωσης της υπογραφής.

1.7.Σύγκριση συμμετρικής και ασύμμετρης κρυπτογραφίας.

Η συμμετρική κρυπτογράφηση κλειδιού έχει ένα σημαντικό μειονέκτημα. Δύο άνθρωποι που επιθυμούν να ανταλλάξουν εμπιστευτικά μηνύματα πρέπει να μοιραστούν ένα μυστικό κλειδί. Η ανταλλαγή του κλειδιού πρέπει να γίνει με ένα ασφαλή τρόπο και όχι με τα μέσα που θα επικοινωνούσαν κανονικά. Αυτό είναι συνήθως το πιο δύσκολο σημείο και το σύστημα κρυπτογραφίας δημόσιων κλειδιών παρέχει μια εναλλακτική λύση.

Γενικά οι τεχνικές δημόσιου κλειδιού είναι πολύ ισχυρότερες υπολογιστικά από τους καθαρά συμμετρικούς αλγορίθμους, αλλά η σωστή χρήση αυτών των τεχνικών επιτρέπει μια ευρεία ποικιλία εφαρμογών τους.

Όσον αφορά την ασφάλεια δεν υπάρχει τίποτα που να καθιστά ασφαλέστερους τους αλγορίθμους δημόσιου κλειδιού σε σύγκριση με τους συμμετρικούς αλγορίθμους κλειδιών. Υπάρχουν δημοφιλείς και μη δημοφιλείς αλγόριθμοι. Υπάρχουν αυτοί που έχουν παραβιαστεί και αυτοί που δεν έχουν ακόμα τουλάχιστον σπάσει. Δυστυχώς όμως η δημοτικότητα δεν είναι αξιόπιστος δείκτης ασφάλειας. Πολλές αποδείξεις υποστηρίζουν ότι το σπάσιμο ενός αλγορίθμου, όσον αφορά κάποιους καθορισμένους με σαφήνεια στόχους ασφάλειας είναι ισοδύναμο με την επίλυση ενός από τα δημοφιλέστερα μαθηματικά προβλήματα που θεωρούνται να είναι ισοδύναμα με τη κατασκευή ενός διακεκριμένου λογάριθμου.

Γενικά, κανένας από τους αλγόριθμους δεν έχει αποδειχθεί να είναι απόλυτα ασφαλής. Όμως με όλους τους κρυπτογραφικούς αλγορίθμους, αυτοί οι αλγόριθμοι πρέπει να επιλεχθούν και να χρησιμοποιηθούν με εξαιρετική προσοχή.

1.8. Καταστάσεις λειτουργίας συμμετρικών κρυπταλγορίθμων.

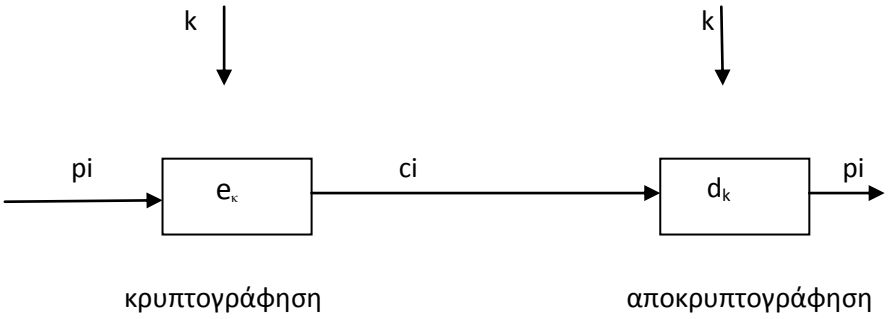
Οι τρόποι λειτουργίας είναι τρόποι διασύνδεσης κρυπταλγορίθμων τμήματος, με στόχο την περαιτέρω αύξηση της κρυπτογραφικής δύναμης και την αποτελεσματική απόκρυψη πιθανών υπολειμμάτων πληροφορίας του απλού κειμένου που μπορεί να υπάρχει στο κρυπτοκείμενο.

Υπάρχουν 4 τυποποιημένοι μέθοδοι-τύποι λειτουργίας σύμφωνα με το πρότυπο fips 81 και αρκετοί μη τυποποιημένοι τρόποι λειτουργίας. Οι τέσσερεις τρόποι λειτουργίας είναι:

1. ηλεκτρονικό κωδικοβιβλίο (electronic codebook, ECB)
2. κρυπτοαλγόριθμος αλυσιδωτού τμήματος (cipher block chaining, CBC)
3. ανάδραση κρυπταλγόριθμου (cipher feedback, CFB)
4. ανάδραση εξόδου (output feedback, OFB)

1.8.1.Ηλεκτρονικό κωδικοβιβλίο, ECB.

Ο τρόπος λειτουργίας ECB αποτελεί την ευθεία συνδεσμολογία όπου το απλό κείμενο τροφοδοτείται στον κρυπταλγόριθμο και το κρυπτοκείμενο προκύπτει από την έξοδο, όπως φαίνεται στο σχήμα 1.6. Η ονομασία του τρόπου αυτού προέρχεται από την αναπαράσταση του κρυπτοσυστήματος ως ένα μεγάλο βιβλίο το οποίο περιέχει όλα τα ζεύγη απλού κειμένου και κρυπτογραφικού κειμένου για κάθε κλειδί. Έτσι για έναν κρυπτογραφικό αλγόριθμο τμήματος με μέγεθος απλού κειμένου και κρυπτογραφικού κειμένου n bits και μέγεθος κλειδιού k bits, μπορούμε να φανταστούμε ότι το βιβλίο περιέχει 2 κεφάλαια. Ένα κεφάλαιο για το κάθε κλειδί, και το περιεχόμενο του κάθε κεφαλαίου θα αποτελούνταν από 2×2k καταχωρήσεις, οι μισές ταξινομημένες ως προς το απλό κείμενο, και οι υπόλοιπες ταξινομημένες ως προς το κρυπτοκείμενο.



Σχήμα 1.6.: Τρόπος λειτουργίας ECB

Το απλό κείμενο χωρίζεται σε τμήματα P = [p1p2…pl], όπου το κάθε τμήμα μεγέθους n bits τροφοδοτείται στον αλγόριθμο κρυπτογράφησης:

$$Ci= ek (pi)$$

Η αναγκαία κατάτμηση του απλού κειμένου είναι και το μειονέκτημα της ECB λειτουργίας. Για όμοια τμήματα του απλού κειμένου, τα αντίστοιχα κρυπτο κείμενα που προκύπτουν είναι επίσης όμοια. Αυτό καθιστά την ECB ακατάλληλη για τις εφαρμογές στις οποίες υπάρχουν επαναλαμβανόμενα μοτίβα δεδομένων. Για παράδειγμα, στα δίκτυα ηλεκτρονικών υπολογιστών, τα δεδομένα που ανταλλάσσονται μεταξύ των υπολογιστών βασίζονται σε πρωτόκολλα επικοινωνίας τα οποία χρησιμοποιούν τυποποιημένα μηνύματα. Έτσι ο αντίπαλος είναι σε θέση να αναγνωρίζει τα επαναλαμβανόμενα τμήματα του απλού κειμένου, καθώς και τις στιγμές κατά τις οποίες γίνεται η αλλαγή του κλειδιού κρυπτογράφησης. Αυτή η διαρροή της πληροφορίας για τις περισσότερες εφαρμογές δεν είναι επιτρεπτή.

Καταλήγουμε λοιπόν στο συμπέρασμα ότι, η αναγκαία κατάτμηση σε συνδυασμό με το γεγονός ότι το κάθε τμήμα κρυπτογραφείται ανεξάρτητα από τα υπόλοιπα τμήματα του απλού κειμένου δίνει το πλεονέκτημα στον αντίπαλο να αναγνωρίσει με αφαιρετικό τρόπο το περιεχόμενο του απλού κειμένου.

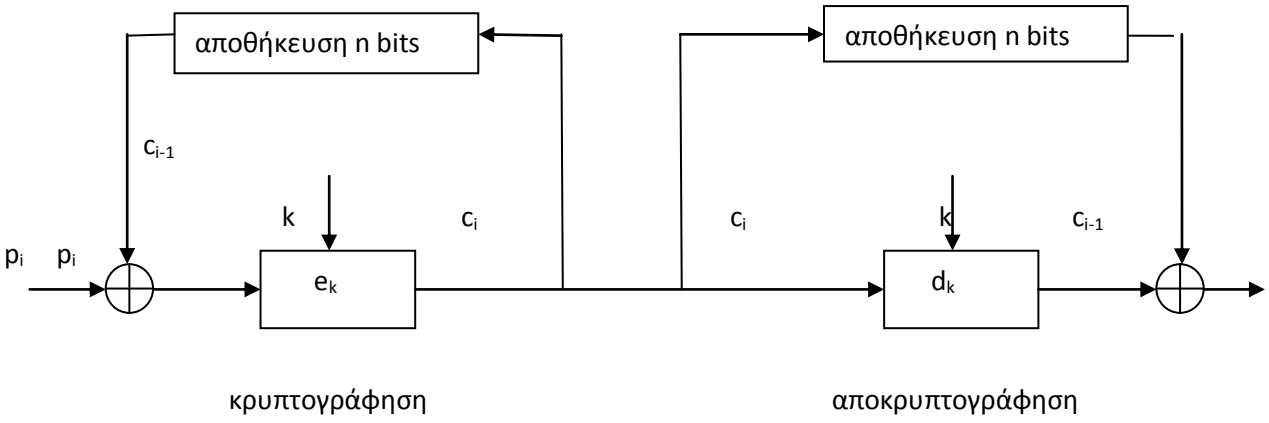
1.8.2.Κρυπταλγόριθμος αλυσιδωτού τμήματος CBC.

Η κρυπτογράφηση ενός τμήματος του απλού κειμένου p_i εξαρτάται και από το προηγούμενο τμήμα p_{i-1} με την ακόλουθη σχέση κρυπτογράφησης:

$$c_i=e_k(c_{i-1} \oplus p_i),$$

ενώ η αποκρυπτογράφηση ορίζεται από την σχέση:

$$p_i=d_k(c_i) \oplus c_{i-1}$$



Σχήμα 1.7. : Τρόπος λειτουργίας CBC

Η ορθότητα της σχέσης κρυπτογράφησης/αποκρυπτογράφησης είναι φανερή από:

$$p_i = d_k (c_i) \oplus c_{i-1} = c_{i-1} \oplus p_i \oplus c_{i-1} = (c_{i-1} \oplus c_{i-1}) \oplus p_i = p_i$$

Μπορούμε να παρατηρήσουμε ότι η ποσότητα του κρυπτοκειμένου που εφαρμόζεται στην αποκλειστική διάζευξη είναι η ίδια τόσο στην πλευρά της κρυπτογράφησης, όσο και στην πλευρά της αποκρυπτογράφησης, και είναι αυτή που προκύπτει από την προηγούμενη κρυπτογράφηση.

Για να καθορισθεί πλήρως η κρυπτογράφηση της λειτουργίας CBC, θα πρέπει να ορισθούν η αρχική τιμή c_0, καθώς και το τελικό τμήμα του απλού κειμένου, στην περίπτωση που το μέγεθος του απλού κειμένου δεν είναι πολλαπλάσιο του n. Στην περίπτωση της κρυπτογράφησης του πρώτου τμήματος p_1 είναι:

$$c_1 = e_k (c_0 \oplus p_i),$$

που σημαίνει ότι απαιτείται η ποσότητα c_0.

Αυτή η ποσότητα είναι το διάνυσμα αρχικοποίησης το οποίο θα πρέπει να είναι γνωστό τόσο κατά τη διαδικασία της κρυπτογράφησης, όσο και κατά τη διαδικασία της αποκρυπτογράφησης. Αν και η εμπιστευτικότητα δεν είναι υποχρεωτική, αποτελεί κοινή πρακτική να στέλνεται στον αποδέκτη κρυπτογραφημένο με ECB.

Ένας δεύτερος λόγος που προτιμάται η κρυπτογραφημένη αποστολή του διανύσματος αρχικοποίησης, είναι η προστασία της ακεραιότητάς του, η οποία είναι σημαντικότερη από την εμπιστευτικότητα του διανύσματος. Η προστασία της ακεραιότητας πραγματοποιείται με τη χρήση συνάρτησης ακεραιότητας σε συνδυασμό με την κρυπτογράφηση ECB. Το διάνυσμα αρχικοποίησης διαιρείται σε δύο τμήματα, το πρώτο μήκους n-a bits και το δεύτερο μήκους a bits. Στο πρώτο τμήμα εφαρμόζεται κάποια μονόδρομη συνάρτηση hash, και τα πρώτα a

bits του αποτελέσματος απαρτίζουν το δεύτερο τμήμα του διανύσματος. Με αυτόν τον τρόπο το δεύτερο τμήμα του διανύσματος αποτελεί τη σύνοψη του πρώτου τμήματος.

Στη συνέχεια το διάνυσμα κρυπτογραφείται και αποστέλλεται στον αποδέκτη. Ο αποδέκτης με τη σειρά του το αποκρυπτογραφεί και ελέγχει αν το δεύτερο τμήμα του διανύσματος είναι η σύνοψη του πρώτου. Στην περίπτωση που ο αντίπαλος προσβάλλει την ακεραιότητα του διανύσματος, αυτό θα γίνει αντιληπτό από τον αποδέκτη.

Όσον αφορά το τελευταίο τμήμα του απλού κειμένου, υπάρχει το ενδεχόμενο το τμήμα αυτό να είναι μικρότερο του n. Αυτό συμβαίνει όταν το μέγεθος του κρυπτο κειμένου δεν είναι πολλαπλάσιο του n. Στην περίπτωση αυτή προστίθενται μηδενικά στο τέλος, έως ότου το τμήμα έχει μέγεθος ίσο με n bits. Στις εφαρμογές στις οποίες τα δεδομένα ακολουθούν αυστηρή τυποποίηση και δεν είναι επιτρεπτό να συμπεριλαμβάνονται τα επιπλέον μηδενικά, τα τελευταία bits του τμήματος χρησιμοποιούνται για την καταγραφή του πλήθους των επιπρόσθετων μηδενικών. Για z μηδενικά, απαιτούνται log2(z) δυαδικές θέσεις.

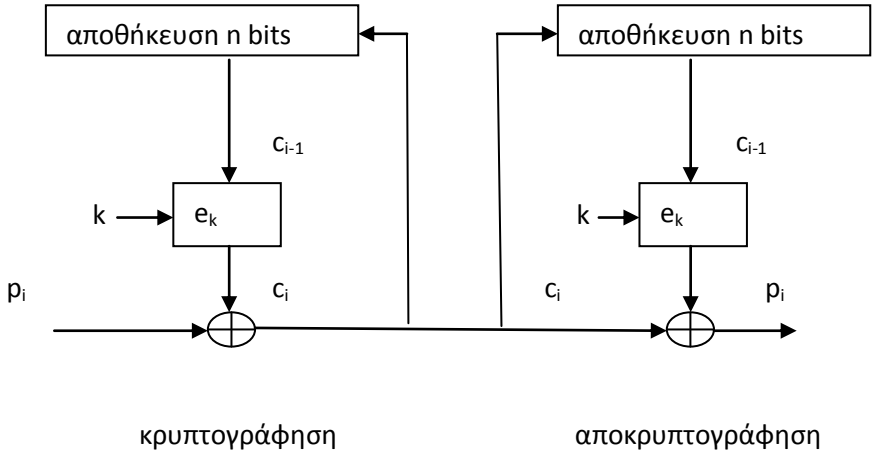
1.8.3.Ανάδραση κρυπτογραφικού αλγόριθμου CFB.

Το κρυπτογραφημένο κείμενο προκύπτει από την επανακρυπτογράφηση του προηγούμενου κρυπτοκειμένου, συνδυασμένο με αποκλειστική διάζευξη με το απλό κείμενο. Έτσι η κρυπτογράφηση ορίζεται ως:

$$c_i = e_k (c_{i-1}) \oplus p_i$$

ενώ κατά την αποκρυπτογράφηση ισχύει:

$$p_i = e_k (c_{i-1}) \oplus c_i$$



Σχήμα 1.8. : Τρόπος λειτουργίας CFB

Η λειτουργία CFB μπορεί να θεωρηθεί ως κρυπταλγόριθμος ροής, όπου τα σύμβολα του απλού κειμένου είναι οι δυαδικές λέξεις μεγέθους n bits, που σημαίνει ότι το αλφάβητο του απλού κειμένου και του κρυπτοκειμένου αποτελείται από 2n σύμβολα. Ο κρυπταλγόριθμος τμήματος λειτουργεί ως γεννήτρια κλειδοροής.

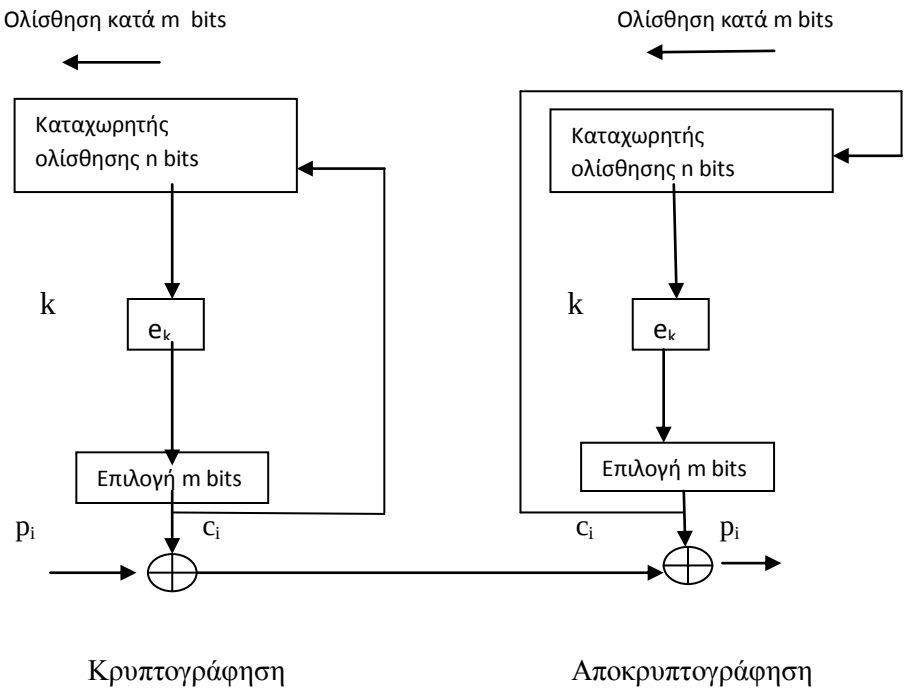
Επίσης σε έναν κρυπταλγόριθμο ροής, οι γεννήτριες της κλειδοροής του αποστολέα και του αποδέκτη θα πρέπει να παράγουν την ίδια ακολουθία. Αυτό φαίνεται και από την πράξη αποκρυπτογράφησης, όπου ο κρυπτογραφικός αλγόριθμος τμήματος εφαρμόζεται σε λειτουργία κρυπτογράφησης και όχι αποκρυπτογράφησης.

Παρόμοια με τη λειτουργία CBC, για την πλήρη εκτέλεση της CFB απαιτείται διάνυσμα αρχικοποίησης. Το διάνυσμα αυτό αποθηκεύεται στον καταχωρητή αποθήκευσης που τροφοδοτεί τον κρυπταλγόριθμο τμήματος. Η μετάδοση του διανύσματος αρχικοποίησης δεν απαιτεί εμπιστευτικότητα. Αντίθετα, μπορεί να προηγηθεί του μηνύματος και να σταλεί κρυπτογραφημένο με το ίδιο το κρυπτο σύστημα της CFB. Οι δύο καταχωρητές αποθήκευσης μπορούν να έχουν μηδενικές τιμές κατά τη μετάδοση του διανύσματος αρχικοποίησης.

1.8.4.Ανάδραση εξόδου OFB.

Η λειτουργία OFB είναι μια προσέγγιση του κρυπτογραφικού αλγόριθμου Vernam και ισοδυναμεί με τον κρυπταλγόριθμο ροής. Η κρυπτογράφηση πραγματοποιείται με την αποκλειστική διάζευξη του απλού κειμένου με την ακολουθία της κλειδοροής. Αντίστοιχα, η αποκρυπτογράφηση πετυχαίνεται με την αποκλειστική διάζευξη του κρυπτοκειμένου με την ακολουθία της κλειδοροής.

Η διαδικασία δημιουργίας της κλειδοροής είναι ανεξάρτητη από το απλό κείμενο και το κρυπτοκείμενο.



Σχήμα 1.9.: Τρόπος λειτουργίας OFB

Θα μπορούσαμε να υποστηρίξουμε ότι η ασφάλεια της OFB είναι μικρότερη από την ασφάλεια των υπολοίπων τριών τρόπων λειτουργίας και αυτό γιατί ο μόνος τρόπος διασύνδεσης του απλού κειμένου και του κρυπτοκειμένου είναι η πράξη της αποκλειστικής διάζευξης. Εφόσον η γεννήτρια της κλειδοροής είναι μηχανή πεπερασμένων καταστάσεων, η κλειδοροή που παράγει θα είναι περιοδική. Επομένως υπάρχει κάποια χρονική στιγμή όπου η κλειδοροή εμφανίζει τα ίδια κλειδιά.

Αν ο αντίπαλος εντοπίσει την αρχή της περιόδου, τότε μπορεί να απομακρύνει την πληροφορία της κλειδοροής από το κρυπτοκείμενο με τον ακόλουθο τρόπο.

Έστω τα τμήματα του κρυπτοκειμένου c_i και c_i τα οποία προκύπτουν από την εφαρμογή ιδίων τμημάτων της κλειδοροής. Αν συνδυάσουμε τα κρυπτοκείμενα με αποκλειστική διάζευξη προκύπτει ότι:

$$c_i \oplus c_j = (p_i \oplus k_i) \oplus (p_j \oplus k_i) = p_i \oplus p_j$$

δηλαδή η κλειδοροή έχει εξαλειφθεί. Αν το απλό κείμενο είναι κάποια φυσική γλώσσα με υψηλή περίσσεια, τότε ο αντίπαλος μπορεί να εντοπίσει την περίοδο με στατιστικές μεθόδους. Στη συνέχεια, μπορεί να συνδυάζει με αποκλειστική διάζευξη απλά κείμενα της γλώσσας στο παραπάνω άθροισμα για να ξεχωρίσει τα p_i και p_j.

Επομένως στην περίπτωση της λειτουργίας OFB δεν υπάρχει η ίδια ελευθερία επιλογής κρυπταλγόριθμου τμήματος που υπάρχει στους υπόλοιπους τρόπους λειτουργίας. Ο κρυπτοαλγόριθμος τμήματος θα πρέπει από τη μια να έχει μεγάλη περίοδο, ενώ από την άλλη θα πρέπει να αλλάζει το κλειδί προτού ξεπεραστεί αυτή η περίοδος. Η αλλαγή του κλειδιού του κρυπταλγόριθμου τμήματος θα έχει ως αποτέλεσμα η γεννήτρια κλειδοροής να μεταπίπτει σε άλλη ακολουθία κλειδοροής.

1.9. Κρυπτανάλυση.

Με τον όρο κρυπτανάλυση εννοούμε τη μελέτη των τεχνικών μαθηματικών, οι οποίες επιχειρούν την ανέραιση των τεχνικών της κρυπτογραφίας και γενικότερα της ασφαλούς μετάδοσης των πληροφοριών.

Η κρυπτανάλυση βασίζεται πέραν των μαθηματικών και στο εμπειρικό γεγονός ότι στην πράξη, ο κρυπταναλυτής έχει στη διάθεσή του πάρα πολύ μεγάλο αριθμό κρυπτογραφημένων κειμένων, τα οποία κρυπτογραφήθηκαν με τον ίδιο τρόπο. Επίσης θεωρούμε σαν δεδομένο ότι ο κρυπταναλυτής γνωρίζει πλήρως τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης που χρησιμοποιήθηκε. Οι διαδικασίες κρυπτανάλυσης ονομάζονται επιθέσεις.

Σκοπός του κρυπταναλυτή είναι να αποκτήσει:

1.ενα μέρος από κάποιο αρχικό καθαρό κείμενο ή ολόκληρο.

2.ενα μέρος από κάποιο κρυπτογραφημένο κείμενο ή ολόκληρο.

3.συνδυασμό των προηγούμενων.

4.συνδυασμό των προηγούμενων από διαφορετικά μηνύματα

5.γνώση παραγωγής ή απόκτησης των κλειδιών κρυπτογράφησης.

2.Αλγόριθμοι κρυπτογράφησης.

2.1.Αλγόριθμοι αντικατάστασης.

Οι αλγόριθμοι κρυπτογράφησης αποτελούν το μέσο για το μετασχηματισμό μηνυμάτων σε κρυπτογραφημένα κείμενα. Μια διαδικασία κρυπτογράφησης συμβολίζεται ως : $c= e_k (m)$, όπου m είναι το αρχικό κείμενο, e είναι ο αλγόριθμος κρυπτογράφησης, k είναι το μυστικό κλειδί και c είναι το

κρυπτογραφημένο κείμενο. Αντίστοιχα, η διαδικασία της αποκρυπτογράφησης συμβολίζεται ως : $m = d_k (c)$.

Αντίστοιχα με τα κρυπτογραφικά συστήματα και οι αλγόριθμοι γενικά ταξινομούνται σε κατηγορίες ανάλογα με τα κλειδιά και τον τρόπο κρυπτογράφησης των μηνυμάτων. Με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων ταξινομούνται σε αλγόριθμους αντικατάστασης και μετατόπισης. Στην κατηγορία αυτή ανήκουν ο αλγόριθμος του Καίσαρα και ο αλγόριθμος Vigenere.

2.1.1.Αλγόριθμος του Καίσαρα.

Ο Ιούλιος Καίσαρας επινόησε έναν απλό κρυπτογραφικό αλγόριθμο για να επικοινωνεί με τους επιτελείς του, με μηνύματα που δεν θα ήταν δυνατόν να τα διαβάσουν οι εχθροί του. Ο αλγόριθμος βασιζόταν στην αντικατάσταση κάθε γράμματος του αλφαβήτου με κάποιο άλλο, όχι όμως τυχαία επιλεγμένο.
Ο αλγόριθμος κρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα δεξιά. Κάθε γράμμα αντικαθίσταται από κάποιο άλλο με κάποιο κλειδί π.χ. 3. Δηλαδή, η κρυπτογράφηση ενός μηνύματος γίνεται με αντικατάσταση κάθε γράμματος από το γράμμα που βρίσκεται 3 θέσεις δεξιότερά του στο αλφάβητο. Θα μπορούσε το κλειδί να ήταν ο αριθμός 6, οπότε το κρυπτογραφημένο κείμενο που θα προέκυπτε θα ήταν διαφορετικό. Έτσι, διατηρώντας τον ίδιο αλγόριθμο κρυπτογράφησης και επιλέγοντας διαφορετικό κλειδί παράγονται διαφορετικά κρυπτογραφημένα μηνύματα.
Ο πίνακας αντιστοίχισης των γραμμάτων, έχοντας ως κλειδί το 3, φαίνεται παρακάτω:

Το γράμμα	a	b	c	d	e	f	g	h	i	j	k	v	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Αντικαθίσταται από το γράμμα	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

Αν, για παράδειγμα, το απλό κείμενο είναι η λέξη secret, θα προκύψει το κρυπτογράφημα wigvix. Για να το αποκρυπτογραφήσει κάποιος θα πρέπει να αντιστρέψει τη διαδικασία κρυπτογράφησης, με άλλα λόγια να αντικαταστήσει κάθε γράμμα με αυτό που βρίσκεται 3 θέσεις αριστερότερά του στο αλφάβητο. Προφανώς, δεν αρκεί να ξέρει ότι ο κατάλληλος αλγόριθμος αποκρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα αριστερά, αλλά πρέπει να γνωρίζει και πόσες θέσεις χρειάζεται να τα ολισθήσει. Πρέπει δηλαδή να γνωρίζει το κλειδί, που σε αυτήν την περίπτωση είναι ο αριθμός 3.

2.1.2.Ο αλγόριθμος Vigenere

Ένας άλλος παρόμοιος κρυπτογραφικός αλγόριθμος είναι ο αλγόριθμος Vigenere. Σε αυτόν τα γράμματα αντιστοιχίζονται πάλι με τους αριθμούς από το 0

ως το 25, όπως ακριβώς και με τον κρυπτογραφικό αλγόριθμο του Καίσαρα. Όμως το μυστικό κλειδί, τώρα, δεν είναι ένας αριθμός αλλά μια μικρή ακολουθία γραμμάτων, όπως για παράδειγμα μια λέξη.
Κατά την κρυπτογράφηση προστίθεται το αριθμητικό ισοδύναμο κάθε γράμματος του αρχικού κειμένου με το αριθμητικό ισοδύναμο ενός γράμματος του κλειδιού. Επειδή συνήθως το μήκος του αρχικού κειμένου είναι μεγαλύτερο από το μήκος του κλειδιού, τα γράμματα του κλειδιού ανακυκλώνονται και επαναλαμβάνεται η χρήση τους όσο χρειάζεται.
Αξίζει να σημειώσουμε ότι ο κρυπτογραφικός αλγόριθμος του Καίσαρα είναι μια ειδική περίπτωση του κρυπτογραφικού αλγορίθμου Vigenere για την περίπτωση που το μήκος της λέξης του κλειδιού είναι ίσο με 1.
Αυτός ο αλγόριθμος ανήκει στην κατηγορία των αποκαλούμενων *Κρυπτογραφικών Αλγορίθμων Πολυαλφαβητικής Αντικατάστασης* (polyalphabetic substitution ciphers). Ο κρυπτογραφικός αλγόριθμος Vigenere είναι και αυτός μια ειδική μορφή κρυπταλγορίθμου ροής. Ακριβώς όπως με τον κρυπτογραφικό αλγόριθμο του Καίσαρα, χρησιμοποιεί πρόσθεση με υπολογισμό του modulo 26 αντί για πρόσθεση με υπολογισμό του modulo 2 για να συνδυάσει το αρχικό κείμενο με το κλειδί. Είναι απλά η λέξη-κλειδί, η οποία επαναλαμβάνεται όσο χρειάζεται. Φυσικά ο κρυπτογραφικός αλγόριθμος Vigenere σπάζει εύκολα.

2.1.3.Σημειοματάριο μιας χρήσης.

Ο κρυπτογραφικός αλγόριθμος του σημειωματάριου μιας χρήσης (The one-time pad cipher) ή αλγόριθμος του Vernam είναι μια ειδική παραλλαγή κρυπτογραφικού αλγορίθμου ροής. Το ψευδοτυχαίο κλειδί αντικαθίσταται από μια τυχαία (μη επαναλαμβανόμενη) ακολουθία δυαδικών ψηφίων (bits) η οποία χρησιμοποιείται μόνο μια φορά (από αυτό προκύπτει και ο χαρακτηρισμός «μιας χρήσης»). Αν χρησιμοποιηθεί σωστά, ο αλγόριθμος αυτός αποδεδειγμένα δεν είναι δυνατόν να σπάσει (unbreakable).
Το μοναδικό πρόβλημα αφόρα τη διαχείριση των κλειδιών. Πριν να καταστεί δυνατή η κρυπτογραφημένη επικοινωνία, τα δυο μέρη (αποστολέας και παραλήπτης) πρέπει να συμφωνήσουν σε τόσο υλικό τυχαίων κλειδιών όσα και τα δεδομένα που θα μεταδοθούν.

2.2.Συμμετρικοί και ασύμμετροι αλγόριθμοι κρυπτογράφησης.

Υπάρχουν διάφορες τεχνικές αλγορίθμων στις οποίες βασίζονται οι αντίστοιχοι κώδικες κρυπτογραφίας. Στη συνέχεια θα αναφέρω τις δυο βασικότερες κατηγορίες τεχνικών αλγορίθμων οι οποίες είναι: 1) Συμμετρικοί αλγόριθμοι 2) Ασύμμετροι αλγόριθμοι. Στους συμμετρικούς αλγόριθμους συγκαταλέγονται οι DES και Blowfish ενώ στους ασύμμετρους ο RSA.

Το ασύμμετρο σύστημα κρυπτογράφησης δημοσίου κλειδιού δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Χαρακτηριστικό του είναι ότι έχει δυο είδη κλειδιών, ένα ιδιωτικό και

ένα δημόσιο. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό. Η βασική σχέση μεταξύ τους είναι : ότι κρυπτογραφεί το ένα, μπορεί να το αποκρυπτογραφήσει μόνο το άλλο.

2.2.1.Ο αλγόριθμος κρυπτογράφησης DES

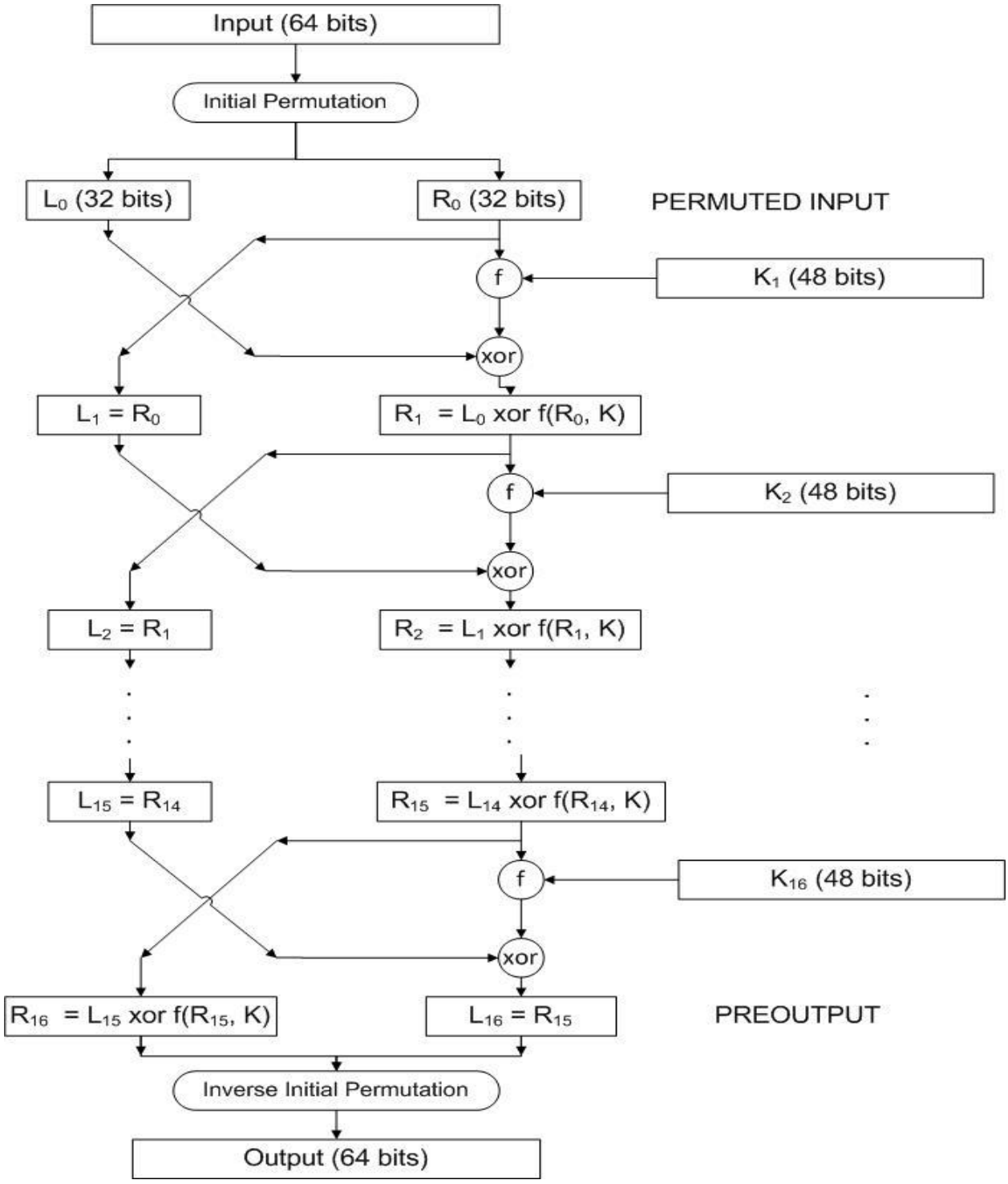
Ο DES αποτελεί τον Data Encryption Standard, έναν αλγόριθμο της κυβέρνησης των Ηνωμένων Πολιτειών για κρυπτογράφηση και αποκρυπτογράφηση αταξινόμητων δεδομένων. Περιγράφεται από τα Federal Information Processing Standards (FIPS) 46, όπου η πιο πρόσφατη έκδοση του είναι FIPS 46-3. Βασίζεται στο κρυπτογράφημα Lucifer της IBM. Η κρυπτογράφηση των δεδομένων τα μετατρέπει σε μία μορφή ακατανόητη το κρυπτογράφημα (*cipher*). Η αποκρυπτογράφηση μετατρέπει το κρυπτογράφημα στα αρχικά δεδομένα – αρχικό κείμενο (*plaintext*). Οι αλγόριθμοι που περιγράφονται σε αυτό το πρότυπο καθορίζουν τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης που βασίζονται στον δυαδικό αριθμό-κλειδί (*key*).
Το κλειδί αποτελείται από 64 δυαδικά ψηφία από τα οποία τα 56 χρησιμοποιούνται άμεσα στον αλγόριθμο. Τα υπόλοιπα 8, που δεν χρησιμοποιούνται στον αλγόριθμο χρησιμοποιούνται για ανίχνευση λαθών (error detection). Αυτά τα 8 bits τοποθετούνται ώστε να αποτελούν bit περιττής ισοτιμίας για κάθε 8-bit byte του κλειδιού.

Ο DES δουλεύει με bits. Κάθε τετράδα bits αποτελεί έναν δεκαεξαδικό αριθμό. Το δυαδικό 0001 αντιστοιχεί στο δεκαεξαδικό 1, το δυαδικό 1000 στο δεκαεξαδικό 8 και το δυαδικό 1111 στο δεκαεξαδικό F. Για παράδειγμα, αν θεωρήσουμε το μη κρυπτογραφημένο κείμενο 8787878787878787 και το κρυπτογραφήσουμε με το κλειδί 0E329232EA6D0D73 θα λάβουμε το κρυπτογραφημένο μήνυμα 0000000000000000. Αν αποκρυπτογραφήσουμε το κρυπτογραφημένο αυτό μήνυμα με το μυστικό κλειδί 0E329232EA6D0D73 το αποτέλεσμα που θα λάβουμε θα είναι το αρχικό μη κρυπτογραφημένο μήνυμα 8787878787878787. Αυτό το παράδειγμα είναι επιδέξια κατασκευασμένο και μεθοδικό γιατί το μη κρυπτογραφημένο μήνυμα έχει μήκος ακριβώς 64 bits.

Το ίδιο θα συνέβαινε και αν το αρχικό μήνυμα είχε μήκος πολλαπλάσιο των 64 bits, συνθήκη, όμως, που δεν ικανοποιείται από τα περισσότερα μηνύματα που πρόκειται να κρυπτογραφηθούν.

Ένα τμήμα – block για να κρυπτογραφηθεί πρέπει να περάσει από μία αρχική μετάθεση (Initial Permutation - **IP**), μετά από ένα πολύπλοκο υπολογισμό που εξαρτάται από το κλειδί, και τελικά από μία τελική μετάθεση (Final Permutation – **IP-1**) που είναι αντίστροφη της αρχικής. Ο ενδιάμεσος υπολογισμός χρησιμοποιεί

μία συνάρτηση f , που ονομάζεται cipher function, και τη συνάρτηση δημιουργίας κλειδιού (Key Schedule - **KS**). Εν συνεχεία παρουσιάζεται το σχήμα 2.1 απεικονίζει τη διαδικασία κρυπτογράφησης (encryption) του DES.



Σχήμα 2.1.:Διαδικασία κρυπτογράφησης des.

Στην αριστερή πλευρά της εικόνας παρουσιάζονται τα τρία στάδια της επεξεργασίας του αρχικού κειμένου. Στην αρχή, το κείμενο των 64-bit ακολουθεί την αρχική μετάθεση (**IP**) στα πλαίσια του οποίου τα bits αναδιατάσσονται για να παραχθεί η μετασχηματισμένη είσοδος. Γίνεται αντιμετάθεση σύμφωνα με τον παρακάτω πίνακα, όπου οι είσοδοι στον πίνακα δείχνουν την νέα αναδιάταξη των bits από την αρχική. Το 58ο bit της εισόδου γίνεται το 1ο του IP, το 50^{ο} γίνεται 2ο κτλ.

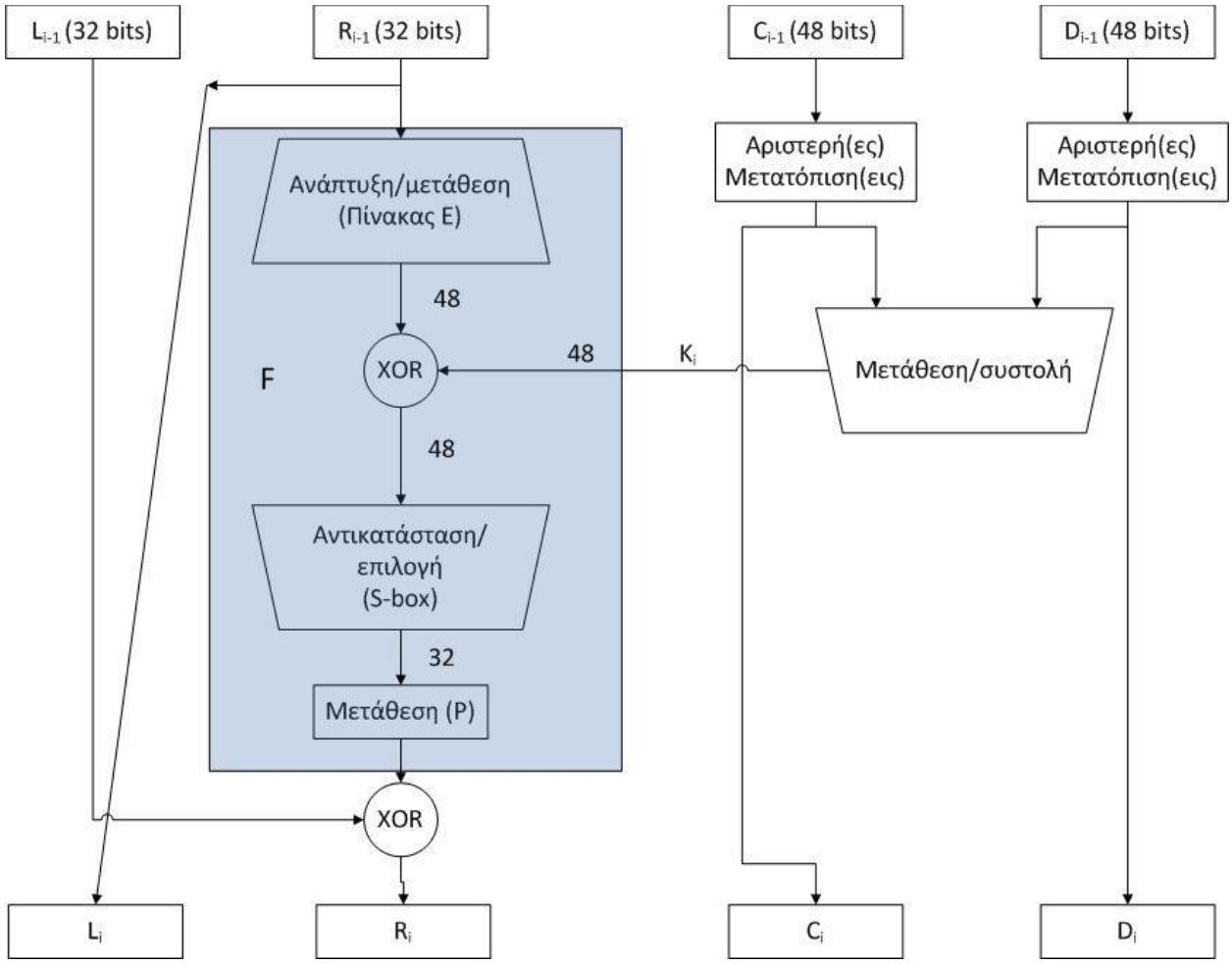
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Πίνακας 2.2.: πίνακας αρχικής αντιμετάθεσης IP.

Η μετασχηματισμένη είσοδος των 64-bit συμμετέχει σε 16 επαναλήψεις, παράγοντας μία ενδιάμεση τιμή των 64-bit στο τέλος κάθε επανάληψης. Το αριστερό μισό τμήμα σε συνδυασμό με το δεξί μισό τμήμα οποιασδήποτε ενδιάμεσης τιμής 64-bit αντιμετωπίζονται ως ξεχωριστές ποσότητες 32-bit, οι οποίες περιγράφονται ως L (Left - Αριστερή) και R (Right - Δεξιά).

Συνοπτικά, η επεξεργασία κάθε επανάληψης μπορεί να περιγραφεί με τους παρακάτω τύπους:

$L_i = R_{i-1}$ $R_i = L_{i-1}$ XOR F (R_{i-1}, K1)

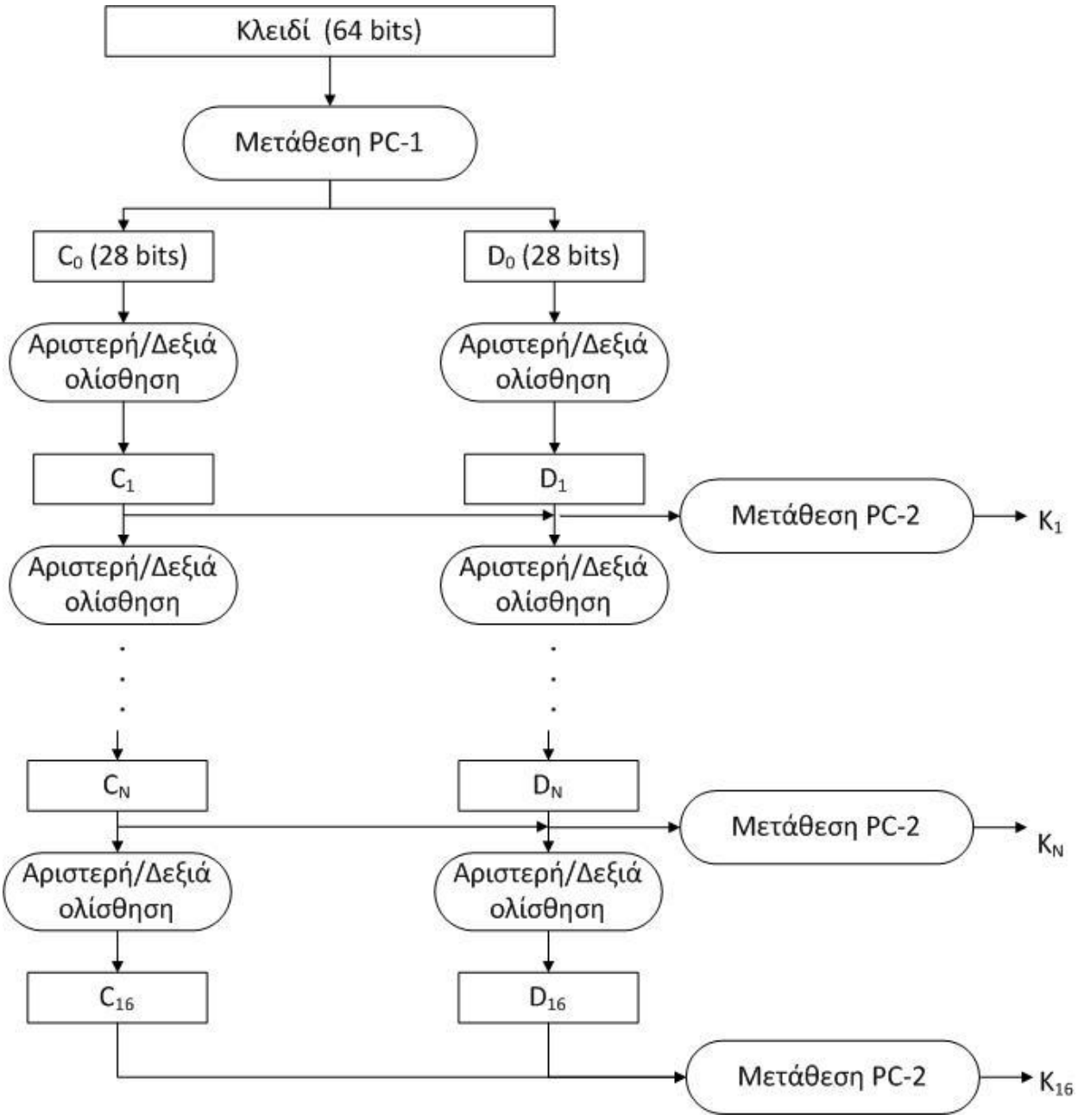


Σχήμα 2.3.: Ένας κύκλος αλγορίθμου Des.

Η αριστερή έξοδος μιας επανάληψης L_i είναι ίση με τη δεξιά είσοδο της επανάληψης R_{i-1}. Η δεξιά έξοδος R_i είναι το αποτέλεσμα της εφαρμογής του XOR μεταξύ του L_{i-1} και μιας σύνθετης συνάρτησης F των R_{i-1} και K_i. Η σύνθετη συνάρτηση περιλαμβάνει διαδικασίες μετάθεσης (permutation) και αντικατάστασης (substitution). Η λειτουργία αντικατάστασης γνωστή ως “S-box”, απλώς απεικονίζει κάθε συνδυασμό 48 εισαγόμενων bit σε ένα συγκεκριμένο τύπο των 32-bit εξόδου.

Το κλειδί των 56-bit αντιμετωπίζεται ύστερα από μία μετάθεση ως δύο ποσότητες των 28-bit, αναφερόμενες ως C_0 και D_0. Σε κάθε επανάληψη, τα C και D υποβάλλονται χωριστά σε μία αριστερή κυκλική ολίσθηση, ή περιστροφή 1 ή 2 bit. Οι τιμές που έχουν υποστεί μετατοπίσεις χρησιμοποιούνται ως είσοδοι στην επόμενη επανάληψη. Επιπλέον χρησιμοποιούνται ως είσοδοι σε μία άλλη συνάρτηση μετασχηματισμού, που παράγει έξοδο 48-bit, η οποία ακολούθως λειτουργεί ως είσοδος στη συνάρτηση $F(R_{i-1}, K_i)$.

Η διαδικασία της αποκρυπτογράφησης με τον αλγόριθμο DES είναι ουσιαστικά ίδια με τη διαδικασία κρυπτογράφησης, αφού ο κανόνας που ακολουθείται είναι: Το κρυπτογράφημα χρησιμοποιείται ως είσοδος στον αλγόριθμο DES, αλλά τα κλειδιά K_i τοποθετούνται σε αντίστροφη σειρά. Ουσιαστικά, το K16 χρησιμοποιείται στην πρώτη επανάληψη, το K15 στη δεύτερη επανάληψη, κοκ., έως ότου χρησιμοποιηθεί το K1 στη δέκατη έκτη και τελευταία επανάληψη.

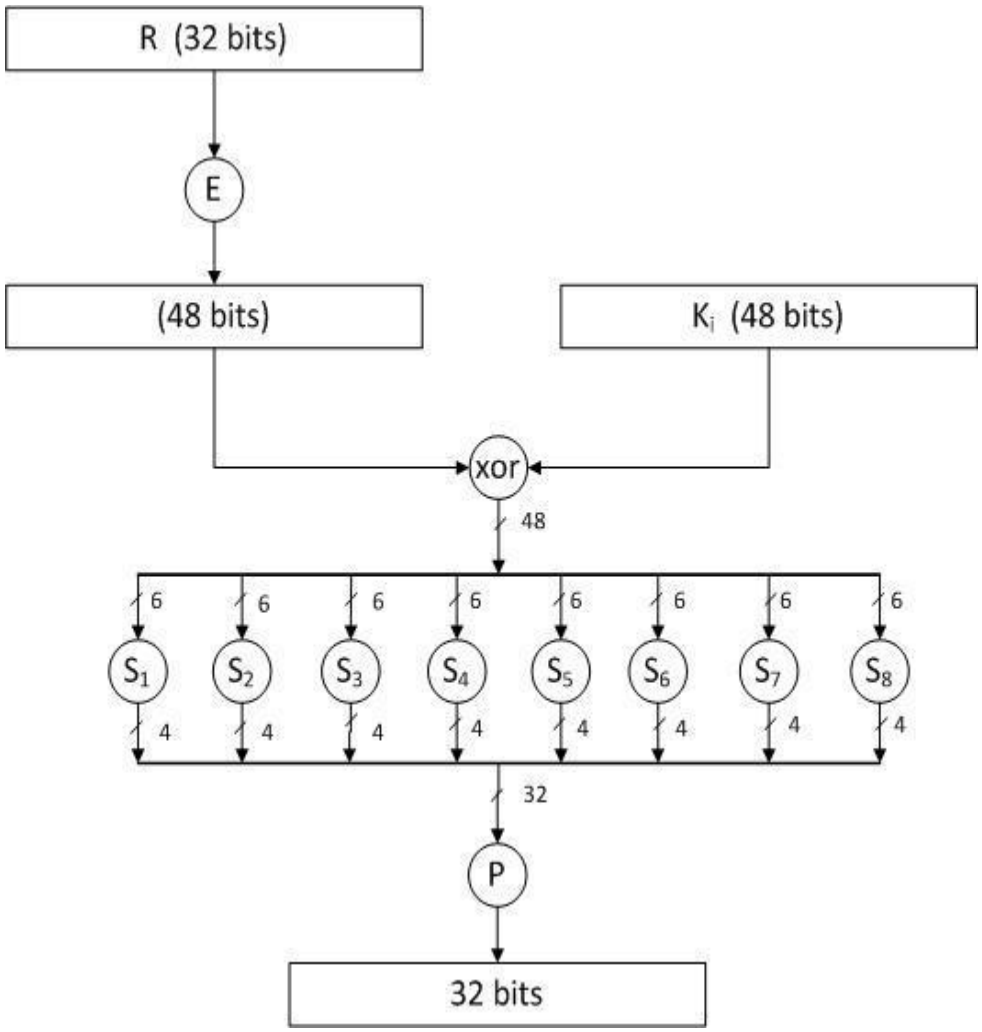


Σχήμα 2.4.: Δημιουργία υποκλειδιών του Des.

Ύστερα από την αρχική μετάθεση σειρά έχουν οι δεκαέξι επαναλήψεις, για 1 ≤ n ≤ 16 , χρησιμοποιώντας τη συνάρτηση F η οποία επεμβαίνει σε τμήματα, ένα τμήμα δεδομένων μήκους 32 bits και το υπό-κλειδί K_n μήκους 48 bits και παράγει ένα νέο, μήκους 32 bits. Με αυτόν τον τρόπο προκύπτει ένα τελικό μήνυμα για n=16, το L16R16.

Αυτό συμβαίνει σε κάθε γύρο, δηλαδή τα 32 δεξιά bits του προηγούμενου αποτελέσματος γίνονται τα 32 αριστερά bits του τρέχοντος βήματος. Για τα 32 δεξιά bits του τρέχοντος βήματος τα 32 αριστερά bits του προηγούμενου βήματος εφαρμόζεται XOR με τα αποτελέσματα της συνάρτησης F:

$$R_1 = L_1 \text{ XOR } F(R_0, K_1)$$



Εικόνα 2.5.: Υπολογισμός της συνάρτησης F.

Για να υπολογίσουμε την F επεκτείνουμε το τμήμα R_{n-1} από 32 σε 48 bits. Για να επιτευχθεί αυτό, χρησιμοποιείται ένας πίνακας με βάση τον οποίο επιλέγονται κάποια στοιχεία του πίνακα R_{n-1} και επαναλαμβάνονται.

Ονομάζουμε τη χρήση αυτού του πίνακα επιλογής **E** . Έτσι η λειτουργία $E(R_{n-1})$ έχει είσοδο ένα τμήμα 32 bits και έξοδο τμήμα μήκους 48 bits. Ο πίνακας **E** φαίνεται παρακάτω:

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Πίνακας 2.6.: Πίνακας επέκτασης E.

Έπειτα, χρησιμοποιούμε την πράξη XOR για το υποκλειδί K_n και το $E(R_{n-1})$:

$$K_n \text{ XOR } E\ R_{n-1}$$

Ο υπολογισμός της συνάρτησης F δεν έχει ολοκληρωθεί. Ως εδώ έχουμε ένα τμήμα μήκους 48 bits τα οποία ομαδοποιούμε σε οκτώ ομάδες των έξι bits. Κάθε μια ομάδα από bits θα χρησιμοποιηθεί σαν διεύθυνση σε κάποιους πίνακες που ονομάζονται “S-Boxes”. Κάθε ομάδα αποτελούμενη από έξι bits μας δίνει μια διεύθυνση σε κάθε πίνακα S. Σε κάθε διεύθυνση είναι αποθηκευμένος ένας αριθμός μήκους τεσσάρων bits ο οποίος και αντικαθιστά τα αρχικά έξι bits. Έτσι το τελικό τμήμα που προκύπτει από αυτή την διαδικασία είναι μήκους 32 bits.

$$K_n \text{ XOR } E\ (R_{n-1}) = B_1B_2B_3B_4B_5B_6B_7B_8$$

Όπου Bi είναι μια ομάδα από bits. Στη συνέχεια υπολογίζουμε το νέο τμήμα :

$$S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$$

Όπου η ποσότητα Si(Bi) αντιστοιχεί στο αποτέλεσμα που προκύπτει για την i-οστή εξάδα στον i-οστό πίνακα S. Πριν παραθέσουμε τους πίνακες Si ας εξηγήσουμε πως λειτουργούν.

S_1

Row No.	Column Number															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Αν θεωρήσουμε S1 την συνάρτηση που περιγράφεται στον παραπάνω πίνακα και Β μια δέσμη από έξι bit η λειτουργία S1(B) περιγράφεται ακολούθως : Το πρώτο και το τελευταίο bit του Β παριστάνουν έναν δεκαδικό αριθμό από το 0 ως το 3 (ή έναν δυαδικό από το 00 ως το 11). Θέτουμε αυτόν τον αριθμό ίσο με i . Τα υπόλοιπα, μεσαία, bit παριστάνουν έναν δεκαδικό αριθμό από το 0 ως το 15 (ή έναν δυαδικό από το 0000 ως το 1111) τον οποίο και θέτουμε ίσο με j . Έπειτα αναζητούμε στον πίνακα S-box1 τον αριθμό που βρίσκεται στην i -οστή γραμμή και στην j -οστή στήλη. Ο αριθμός που προκύπτει απ' αυτή την αναζήτηση είναι ένας δεκαδικός αριθμός από το 0 ως το 15 ο οποίος αναπαρίσταται μοναδικά, όπως γνωρίζουμε, από τέσσερα δυαδικά ψηφία. Αυτός ο αριθμός είναι και το αποτέλεσμα που προκύπτει από την πράξη S1(B). Για παράδειγμα αν B=011011, το πρώτο ψηφίο είναι 0 και το τελευταίο 1, άρα επιλέγουμε την 1η γραμμή. Τα μεσαία 4 ψηφία είναι 1101, το οποίο είναι το δυαδικό ισοδύναμο του δεκαδικού αριθμού 13, επομένως η στήλη που επιλέγεται είναι η 13η. Στην 1η γραμμή και την 13η στήλη εμφανίζεται ο αριθμός 5 (σε δυαδικό σύστημα το 0101), το οποίο είναι και το αποτέλεσμα. Επομένως έχουμε ότι S1(011011)=0101.

Παρακάτω παρατίθενται οι πίνακες-συναρτήσεις S_1 ως S_8:

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Πίνακας 2.7: Πίνακες αντικατάστασης S_1 εως S_8

Το τελευταίο στάδιο του υπολογισμού της συνάρτησης F περιλαμβάνει μια αντιμετάθεση των στοιχείων της δέσμης που προκύπτει από τον υπολογισμό $S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$. Έτσι λοιπόν, υπολογίζεται η τιμή της F :

$$F=P\ (S_1(B_1)S_2(B_2)S_3(B_3)\ldots\ldots S_8(B_8)$$

Η πράξη της αντιμετάθεσης P περιγράφεται από τον πίνακα που παρατίθεται παρακάτω:

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Πίνακας 2.8.: Πίνακας αντιμετάθεσης P.

Παρατηρούμε ότι σε αυτήν την πράξη δεν μεταβάλλεται το μήκος της δέσμης καθώς εμφανίζονται και τα 32 στοιχεία του πίνακα.

Δημιουργία υποκλειδιών

Τα bit του αρχικού κλειδιού αντιμετατίθενται σύμφωνα με τον παρακάτω πίνακα **PC-1**. Όπως φαίνεται από τον πίνακα, από τη στιγμή που η πρώτη τιμή του είναι το νούμερο 57, σημαίνει ότι το 57ο bit του αρχικού κλειδιού K μετατίθεται σε πρώτο bit για το κλειδί K+ (επόμενο κλειδί). Ομοίως το 49ο bit του αρχικού κλειδιού μετατίθεται σε δεύτερο και το 4ο του αρχικού σε τελευταίο για το K+. Πρέπει να παρατηρήσουμε ότι μόνο 56 από τα 64 bits του αρχικού κλειδιού εμφανίζονται στον πίνακα αντιμετάθεσης.

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Πίνακας 2.9.:Πίνακας αντιμεταθέσεων PC-1.

Έπειτα, χωρίζουμε αυτό το κλειδί σε δύο κομμάτια C_0 και D_0 (αριστερό και δεξί αντίστοιχα) τα οποία έχουν μήκος 28 bits το καθένα. Έχοντας προσδιορίσει το C0 και D0, δημιουργούμε δεκαέξι τμήματα C_n και D_n ($1 \leq n \leq 16$). Κάθε ζεύγος C_n και D_n δημιουργείται από το προηγούμενο ζεύγος C_{n-1} και D_{n-1}, αντίστοιχα, για n = 1, 2, …, 16, χρησιμοποιώντας τον παρακάτω πίνακα για αριστερές ολισθήσεις

του προηγούμενου τμήματος. Για να πραγματοποιηθεί μια ολίσθηση προς τα αριστερά μετακινείται κάθε bit μια θέση αριστερά με εξαίρεση το πρώτο, το οποίο πηγαίνει τελευταίο.

Αριθμός Επαναλήψεων	**Αριθμός Αριστερών Ολισθήσεων**
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Πίνακας 2.10.: Πίνακας ολισθήσεων.

Στη συνέχεια σχηματίζουμε τα κλειδιά K_n, με $1 \leq n \leq 16$, χρησιμοποιώντας τον παρακάτω πίνακα αντιμεταθέσεων **PC-2** σε κάθε ζεύγος C_n ,D_n.

Κάθε ζεύγος έχει 56 bits αλλά στον πίνακα αντιμεταθέσεων χρησιμοποιούνται μόνο τα 48. Έτσι λοιπόν το 1ο bit του κλειδιού K_n είναι το 14ο του C_n D_n κτλ:

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

πίνακας 2.11.: Πίνακας αντιμεταθέσεων PC-2.

Ο Αλγόριθμος 3DES Η TRIPLE DES.

Ο αλγόριθμος triple-DES είναι απλά ο DES στον οποίο χρησιμοποιούνται τρία κλειδιά μήκους 56 bits το καθένα. Δίνοντας το αρχικό μηνύματος προς κρυπτογράφηση, το πρώτο κλειδί χρησιμοποιείται από τον DES για την κρυπτογράφηση του μηνύματος. Το δεύτερο κλειδί χρησιμοποιείται για να αποκρυπτογραφήσει το κρυπτογραφημένο με το πρώτο κλειδί μήνυμα. Επειδή όμως το δεύτερο κλειδί δεν είναι το σωστό κλειδί για την αποκρυπτογράφηση του μηνύματος, το μόνο που επιτυγχάνεται με αυτή τη διαδικασία είναι να μπερδεύεται ακόμα περισσότερο το ήδη κρυπτογραφημένο μήνυμα. Τελικά το μήνυμα κρυπτογραφείται ξανά με το τρίτο κλειδί και έτσι προκύπτει το τελικό κρυπτογραφημένο μήνυμα. Αυτή λοιπόν η διαδικασία τριών βημάτων αποκαλείται triple-DES (TDES ή TDEA).

Ο TDEA είναι απλά η εφαρμογή του DES τρεις φορές με τρία κλειδιά τα οποία χρησιμοποιούνται με συγκεκριμένη σειρά. Ο triple-DES μπορεί να εφαρμοστεί και με δύο διαφορετικά κλειδιά αντί για τρία. Στην γενική περίπτωση, το συνολικό εύρος του κλειδιού είναι 2112.

Ο αλγόριθμος ακολουθεί τη διαδοχή: κρυπτογράφηση, αποκρυπτογράφηση, κρυπτογράφηση (EDE – encryption – decryption - encryption) :

$$C=EK_3[\,DK_2[EK_1[P]]]$$

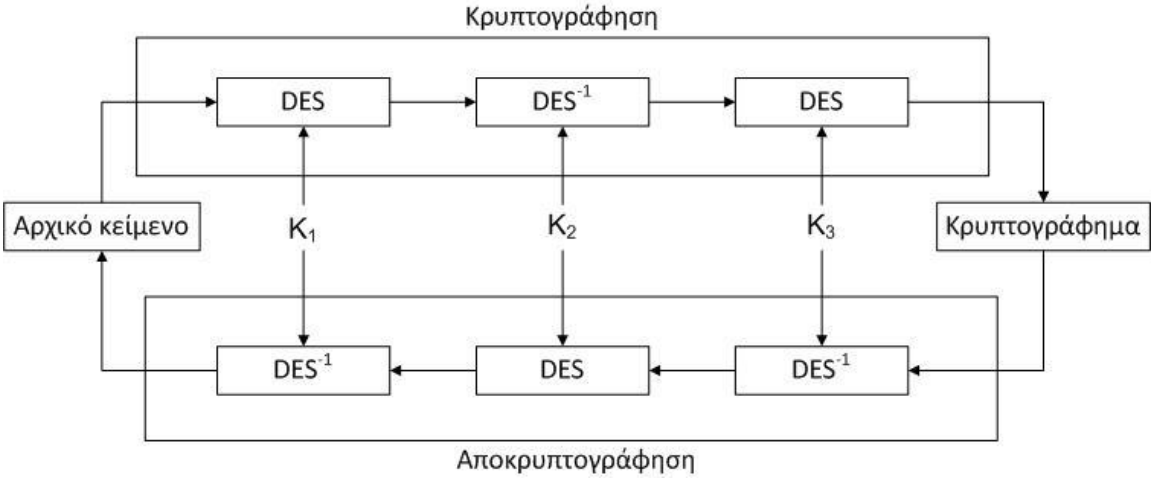
όπου:

C = κρυπτογράφημα

P = αρχικό κείμενο

EK[X] = κρυπτογράφηση του X με χρήση του κλειδιού K

DK[Y] = αποκρυπτογράφηση του X με χρήση του κλειδιού K



Σχήμα 2.12: Αλγόριθμος T-DES

Η αποκρυπτογράφηση ακολουθεί ακριβώς την ίδια διαδικασία με τα κλειδιά σε αντίστροφη χρήση:

$$P=DK_1 [EK_2 [DK_3[C]]]$$

Το πρότυπο καθορίζει τις ακόλουθες επιλογές για το κλειδί για τη δέσμη (K1, K2, K3):

- K1, K2 και K3 ανεξάρτητα κλειδιά.
- K1 και K2 ανεξάρτητα κλειδιά και K3 = K1.
- K1 = K2 = K3

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

$$C=EK_1 [DK_1 [EK_1 [P]]]$$

2.2.2.Ο Αλγόριθμος BLOWFISH

Ο αλγόριθμος Blowfish είναι ένα συμμετρικό μπλοκ κρυπτογράφησης που μπορεί να χρησιμοποιηθεί αποτελεσματικά για την κρυπτογράφηση και διαφύλαξη των δεδομένων. Παίρνει ένα μεταβλητού μήκους κλειδί, από 32 bits έως 448 bits, καθιστώντας ιδανικό για την ασφάλεια των δεδομένων.

Ο Blowfish σχεδιάστηκε το 1993 από τον Bruce Schneier ως μια γρήγορη, εναλλακτική λύση στους απέναντι στους υπάρχοντες αλγόριθμους κρυπτογράφησης.

Ο Blowfish αλγόριθμος είναι μια Feistel Network επανάληψη, μια απλή λειτουργία κρυπτογράφησης 16 φορές.

Όλες οι διαδικασίες είναι προσθήκες XORs με τριανταδυάμπιτες λέξεις. Οι μόνες πρόσθετες διαδικασίες είναι τέσσερις συνταγμένες αναζητήσεις στοιχείων σειράς ανά κύκλο.

Όπως αναφέραμε παραπάνω ο αλγόριθμος Blowfish χρησιμοποιεί έναν μεγάλο αριθμό subkeys. Αυτά τα κλειδιά πρέπει να είναι υπολογισμένα πριν από οποιαδήποτε δεδομένα κρυπτογραφηθούν ή αποκρυπτογραφηθούν.

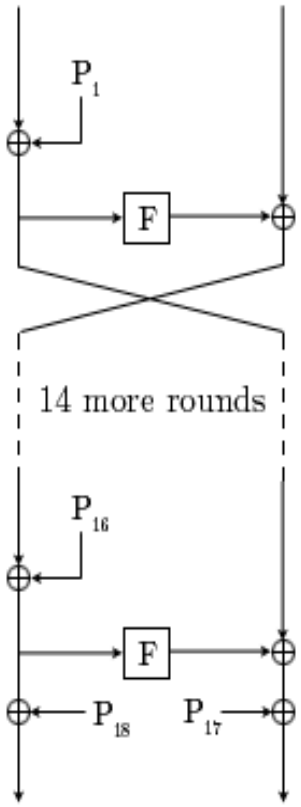
Η P-σειρά αποτελείται από 18 32-bit δευτερεύοντα κλειδιά:

P1, P2, ..., P18.

Υπάρχουν τέσσερα 32-bit S-κουτιά με 256 συμμετοχές το καθένα:

S1, 0, S1, 1,. ..., S1, 255
S2, 0, S2, 1, ..., S2, 255
S3, 0, S3, 1, ..., S3, 255
S4, 0, S4, 1, .., S4, 255.

Το παρακάτω διάγραμμα δείχνει τη δράση του Blowfish



Σχήμα 2.13: Λειτουργία του αλγορίθμου Blowfish

Η Feistel δομή του Blowfish

Η κρυπτογράφηση των δεδομένων γίνεται μέσω ενός δικτύου Feistel που αποτελείται από 16 κύκλους και πραγματοποιείται με την εξής διαδικασία:

Η είσοδος είναι ένα 64-bit στοιχείο δεδομένων, x.
Διαιρεί το x σε δύο 32-bit μισά: XL, XP.
Στη συνέχεια, για i = 1 έως 16:

xL = xL XOR Pi

xR = F (XL) XOR xR

Εναλλαγή XL και xR

Μετά το δέκατο έκτο γύρο, swap XL και xR ξανά για να αναιρέσετε την τελευταία swap.
Στη συνέχεια, XP = xR XOR P17 και XL = xL XOR P18.

Τέλος, επανασυνδέονται XL και xR για να πάρει το κρυπτογράφημα. Η αποκρυπτογράφηση είναι ακριβώς η ίδια όπως η κρυπτογράφηση, εκτός από το ότι P1, P2, ..., P18 χρησιμοποιούνται στην αντίστροφη σειρά.
Εφαρμογές της Blowfish που απαιτούν τις πιο γρήγορες ταχύτητες πρέπει να ξεδιπλώνουν το βρόχο και εξασφαλίζουν ότι όλα τα δευτερεύοντα κλειδιά αποθηκεύονται στη μνήμη cache.
Τα δευτερεύοντα κλειδιά υπολογίζονται με βάση τον αλγόριθμο Blowfish:
α. μονογράψτε πρώτα την P-σειρά και έπειτα τέσσερα S-boxes, στη σειρά, σε ένα συγκεκριμένο string. Αυτή η σειρά αποτελείται από τα δεκαεξαδικά ψηφία του p.
β. XOR P1 με τα πρώτα 32 μπιτ του κλειδιού, XOR το P2 με τα δεύτερα 32 μπιτ του κλειδιού και τα υπόλοιπα για όλα τα κομμάτια του κλειδιού (μέχρι το P18). Ο κύκλος θα επαναλαμβάνεται στα bits των κλειδιών μέχρι ολόκληρη η P-σειρά να γίνει XORed με τα κλειδιά των bits.
γ. κρυπτογραφήστε την all-zero string με τον αλγόριθμο Blowfish, χρησιμοποιώντας τα subkeys που περιγράφονται στα βήματα α και β.
Αντικαταστήστε το P1 και P2 με το αποτέλεσμα του βήματος γ
δ. κρυπτογραφήστε το αποτέλεσμα του βήματος γ χρησιμοποιώντας τον αλγόριθμο Blowfish με τροποποιημένα subkeys.
ε. αντικαταστήστε P3 και P4 με το αποτέλεσμα του βήματος ε.
στ. συνεχίστε τη διαδικασία, αντικαθιστώντας όλα τα στοιχεία της P-σειράς, και έπειτα
ζ. τα τέσσερα S-boxes στην σειρά , με τα αποτελέσματα του συνεχώς μεταβαλλόμενου αλγορίθμου Blowfish.

Συνολικά απαιτούνται 521 εκτελέσεις του αλγορίθμου κρυπτογράφησης Blowfish για την παραγωγή των υποκλειδιών. Ο Blowfish δεν είναι κατάλληλος για εφαρμογές στις οποίες το μυστικό κλειδί αλλάζει συχνά. Αποτελεί όμως τον πιο γρήγορο αλγόριθμο κρυπτογράφησης όταν υλοποιείται σε 32-bit μικροεπεξεργαστές με μεγάλη κρυφή μνήμη δεδομένων.

Ασφάλεια του αλγορίθμου Blowfish

Η ασφάλεια αλγόριθμος Blowfish εξετάστηκε από τον Serge Vaudenay με τα γνωστά s-boxes και τις ρουτίνες r. Μια διαφορική επίθεση μπορεί να ανακτήσει την P-σειρά με 2^{8r+1} με επιλεγμένα plaintexts.
Για ορισμένα αδύνατα κλειδιά που παράγουν κακά S-boxes (οι πιθανότητες να πάρουν αυτά τυχαία είναι 1 στις 2^{14}),η ίδια επίθεση απαιτεί μόνο 2^{4r+1} επιλεγμένα plaintexts να ανακτήσει την P- σειρά. Με τα άγνωστα S-boxes αυτή η επίθεση μπορεί να ανιχνεύσει εάν ένα αδύνατο κλειδί χρησιμοποιείται, αλλά δεν μπορεί

να καθορίσει τι είναι (ούτε τα S-boxes ούτε η P-σειρά). Αυτή η επίθεση λειτουργεί μόνο ενάντια στις μειωμένες-στρογγυλές μεταβλητές είναι απολύτως αναποτελεσματικό ενάντια στους 16 κύκλους εργασίας του Blowfish.
Φυσικά, η ανακάλυψη των αδύνατων κλειδιών είναι σημαντική, ακόμα κι αν φαίνονται αδύνατο να εκμεταλλευτούν. Ένα αδύνατο κλειδί είναι ένα στο οποίο δύο από τις καταχωρήσεις για το S-box είναι ίδιες. Δεν υπάρχει κανένας τρόπος να ελέγξει για τα αδύνατα κλειδιά πριν ελέγξει το κυρίως κλειδί. Για να είστε ασφαλής, μην εφαρμόσετε στον Blowfish έναν μειωμένο αριθμό κύκλων.

2.2.3.Ο αλγόριθμος idea.

Ο Διεθνής αλγόριθμος κρυπτογράφησης δεδομένων (IDEA) είναι ένας αλγόριθμος κρυπτογράφησης μπλοκ σχεδιάστηκε από Xuejia Lai και James L. Massey του ETH Zürich - και περιγράφηκε για πρώτη φορά το 1991. Ο αρχικός αλγόριθμος υπέστη μερικές τροποποιήσεις και τελικά ονομάστηκε ως Διεθνής αλγόριθμο κρυπτογράφησης δεδομένων (IDEA) . Ο προαναφερθέν αλγόριθμος λειτουργεί σε 64 -bit απλό κείμενο και το κρυπτογραφημένο μπλοκ κειμένου (σε ένα χρόνο). Το μήκος του κλειδιού που χρησιμοποιείται για την κρυπτογράφηση είναι 128 bits.

Τώρα , ας δούμε , ποιες είναι οι βασικές λειτουργίες που απαιτούνται σε όλη τη διαδικασία .

Εργασίες που απαιτούνται κατά τους πρώτους 8 γύρους -

1. Πολλαπλασιασμός modulo 216 +1 .

2 . Προσθήκη modulo 216.

3 . Bitwise XOR .

Για την κρυπτογράφηση, η 64-bit απλό κείμενο χωρίζεται σε τέσσερα υπό-block των 16 bits. Στη συζήτησή μας, ορίζουμε αυτά τα τέσσερα μπλοκ, όπως X1 (16 bits), X2 (16 bits), X3 (16 bits) και X4 (16 bits). Κάθε ένα από αυτά τα τμήματα περνά μέσα από 8 γύρους και μία φάση ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ ΕΞΟΔΟΥ. Σε κάθε κύκλο, η ακολουθία γεγονότων είναι η ακόλουθη:

1. Πολλαπλασιάστε X1 και το πρώτο subkey
2. Προσθέστε X2 και το δεύτερο subkey.
3. Προσθέστε X3 και το τρίτο subkey.
4. Πολλαπλασιάστε X4 και το τέταρτο subkey.
5. XOR τα αποτελέσματα των βημάτων (1) και (3).
6. XOR τα αποτελέσματα των βημάτων (2) και (4).
7. Πολλαπλασιάστε τα αποτελέσματα του βήματος (5) με το πέμπτο subkey.
8. Προσθέστε τα αποτελέσματα των βημάτων (6) και (7).

9. Πολλαπλασιάστε τα αποτελέσματα του βήματος (8) με το έκτο subkey.
10. Προσθέστε τα αποτελέσματα των βημάτων (7) και (9).
11. XOR τα αποτελέσματα των βημάτων (1) και (9).
12. XOR τα αποτελέσματα των βημάτων (3) και (9).
13. XOR τα αποτελέσματα των βημάτων (2) και (10).
14. XOR τα αποτελέσματα των βημάτων (4) και (10).

Σε κάθε ένα από αυτούς τους οκτώ γύρους , εκτελούνται ορισμένες (αριθμητικές και λογικές) πράξεις. Κατά τη διάρκεια των οκτώ γύρων, επαναλαμβάνονται οι ίδιες ακολουθίες πράξεων. Στην τελευταία φάση, δηλαδή, τη φάση ΜΕΤΑΤΡΟΠΗ ΕΞΟΔΟΥ, θα εκτελεί μόνο αριθμητικές πράξεις .

1. Πολλαπλασιάστε X1 και το πρώτο subkey.
2. Προσθέστε X2 και το δεύτερο subkey.
3. Προσθέστε το X, και το τρίτο subkey.
4. Πολλαπλασιάστε το X, και το τέταρτο subkey.

Τέλος, τα τέσσερα υπό-block προσαρτούνται για να παραγάγουν το κρυπτογράφημα.

Η δημιουργία των subkeys είναι επίσης εύκολη. Ο αλγόριθμος χρησιμοποιεί 52 τους έξι για κάθε έναν από τους οκτώ κύκλους και τέσσερα ακόμα για το μετασχηματισμό παραγωγής. Κατ' αρχάς, το εκατονεικοσαοκτάμπιτο κλειδί διαιρείται σε οκτώ δεκαεξάμπιτα subkeys. Αυτά είναι τα πρώτα οκτώ subkeys του αλγόριθμου (Τα έξι για τον πρώτο κύκλο, και πρώτα δύο για το δεύτερο κύκλο). Κατόπιν, το κλειδί περιστρέφεται 25 bit στο αριστερά και διαιρείται πάλι σε οκτώ subkeys. Τα τέσσερα πρώτα χρησιμοποιούνται στην 2^{η} περιστροφή τελευταία τα τέσσερα χρησιμοποιούνται στην 3^{η} . Το κλειδί περιστρέφεται άλλα 2.5bit στα αριστερά για τα επόμενα οκτώ subkeys, και τα λοιπά μέχρι το τέλος του αλγορίθμου. Η αποκρυπτογράφηση είναι ακριβώς η ίδια, εκτός από το ότι τα subkeys αντιστρέφονται και ελαφρώς διαφορετικά. Η αποκρυπτογράφηση των subkeys είναι είτε τα πρόσθετα είτε πολλαπλασιαστικά αντίστροφα της κρυπτογράφησης των subkeys.(Για τους σκοπούς του IDEA, το όλο μηδενικά sub-block θεωρείται ότι αντιπροσωπεύει το 2^{16} = -1 για πολλαπλασιασμό του modulo 2^{16}+1 κατά συνέπεια το πολλαπλασιαστικό αντίστροφο 0 είναι 0.) Υπολογίζοντας αυτές παίρνει λίγο χρόνο, αλλά εμείς πρέπει μόνο να το κάνουμε μια φορά για κάθε κλειδί αποκρυπτογράφησης.

2.2.4. Ο αλγόριθμος RC5

Το RC5 είναι ένα block cipher με ποικίλες παραμέτρους: μέγεθος block, μέγεθος κλειδιού, και αριθμός κύκλων. Εφευρέθηκε από Ron Rivest και αναλύθηκε από τα εργαστήρια RSA [1324.1325].
Υπάρχουν τρεις διαδικασίες XOR, η προσθήκη, και οι περιστροφές. Οι περιστροφές είναι συνεχόμενες διαδικασίες στους περισσότερους επεξεργαστές και οι μεταβλητές περιστροφές είναι μια μη γραμμική λειτουργία. Αυτές οι περιστροφές, που εξαρτώνται και από το κλειδί και από τα στοιχεία, είναι η ενδιαφέρουσα λειτουργία.
Ο RC5 έχει ένα block μεταβλητού-μήκους, αλλά αυτό το παράδειγμα θα εστιαστεί σε ένα εξηντατετράμπιτο block δεδομένων. Η κρυπτογράφηση χρησιμοποιεί ένα κλειδί 2r + 2 εξαρτώμενης τριανταδυάμπιτης λέξης όπου r είναι ο αριθμός των κύκλων. Για να κρυπτογραφήσει, διαιρεί αρχικά το block plaintext σε δύο τριανταδυάμπιτες λέξεις: A και B. (Το RC5 κάνει μια μικρή αλλαγή , τα bytes σε λέξεις: Η πρώτη ψηφιολέξη πηγαίνει στα loworder bits της καταχώρισης A, κ.λπ.)
Έτσι :

$$A = A + S_0$$
$$B = B + S_1$$
For $i = 1$ to r:
$$A = ((A \oplus B) <<< B) + S_{2i}$$
$$B = ((B \oplus A) <<< A) + S_{2i+1}$$

Το αποτέλεσμα είναι στους καταχωριστές A και B.
Η αποκρυπτογράφηση είναι εξίσου εύκολη. Διαιρέστε το block plaintext σε δύο λέξεις, A και B, και έπειτα:

For $i = r$ down to 1:
$$B = ((B - S_{2i+1}) >>> A) \oplus A$$
$$A = ((A - S_{2i}) >>> B) \oplus B$$
$$B = B - S_1$$
$$A = A - S_0$$

Το σύμβολο «>>>» είναι μια σωστή κυκλική μετατόπιση. Φυσικά, όλες οι προσθήκες και οι αφαιρέσεις είναι mod 2^{32}.
Η δημιουργία της σειράς κλειδιών είναι πιο περίπλοκη, αλλά και απλή. Κατ' αρχάς, αντιγράψτε τις bytes του κλειδιού σε μια σειρά, L, των τριανταδυάμπιτων λέξεων c , γεμίζοντας την τελική λέξη με τα μηδενικά εάν είναι απαραίτητο. Κατόπιν, μονογράψτε μια σειρά, S, χρησιμοποιώντας μια γραμμική γεννήτρια mod 2^{32}

$$S_0 = P$$
$$\text{for } i = 1 \text{ to } 2(r+1) - 1:$$
$$S_i = (S_{i-1} + Q) \bmod 2^{32}$$

Τα P = Oxb7e15163 και Q = Ox9e3779b9 είναι ι σταθερές που είναι βασισμένες στη δυαδική αντιπροσώπευση του e και phi.
Τέλος αναμειγνύουμε το L στο S.

$$i = j = 0$$
$$A = B = 0$$

Κάνει 3n φορές (οπού το n είναι το μέγιστο του 2(r+1) και του c)

$$A = S_i = (S_i + A + B) <<< 3$$
$$B = L_j = (L_j + A + B) <<< (A + B)$$
$$i = (i + 1) \bmod 2(r + 1)$$
$$j = (j + 1) \bmod c$$

Το RC5 είναι βασικά μια οικογένεια αλγορίθμων. Καθορίσαμε ακριβώς RC5 με ένα τριανταδυάμπιτο μέγεθος λέξης και έναν εξηντατετράμπιτο block δεν υπάρχει κανένας λόγος για τον οποίο ο ίδιος αλγόριθμος δεν μπορεί να έχει ένα εξηντατετράμπιτο μέγεθος λέξης και ένα εκατονεικοσαοκτάμπιτο μέγεθος block. Για w=24 τα P και Q είναι Oxb7e15 1628aed2a6b και Ox9e3779b97f4a7c15 αντίστοιχα. Το Rivest υποδεικνύει τις ιδιαίτερες εφαρμογές του RC5 ως RC5-w/r/b, όπου το W είναι το μέγεθος λέξης, r είναι ο αριθμός κύκλων, και το b είναι το μήκος του κλειδιού σε bytes.Ο RC5 είναι νέος, αλλά τα εργαστήρια στο RSA έχουν ξοδέψει τον αρκετό χρόνο που αναλύοντας τον με ένα εξηντατετράμπιτο block. Μετά από 5 κύκλους, οι στατιστικές φαίνονται πολύ καλές. Μετά από 8 κύκλους, το bit plaintext έχει επιπτώσεις τουλάχιστον σε μια περιστροφή. Υπάρχει μια διαφορική επίθεση που απαιτεί 2^{24} επιλεγμένα plaintexts για 5 κύκλους, 2^{45} για 10 κύκλους, 2^{53} για 12 κύκλους, και 2^{68} για 15 κύκλους. Φυσικά, υπάρχουν μόνο 2^{64} πιθανά επιλεγμένα plaintexts, έτσι αυτή η επίθεση δεν θα λειτουργήσει για15 ή περισσότερους κύκλους.
Οι γραμμικές εκτιμήσεις κρυπτολογικής ανάλυσης δείχνουν ότι είναι ασφαλής μετά από 6 κύκλους. Το Rivest συστήνει τουλάχιστον 12 κύκλους, και ενδεχομένως 16.Αυτό το νούμερο πιθανώς να αλλάξει.

2.2.5.Ο αλγόριθμος rsa.

Ο αλγόριθμος RSA επινοήθηκε από μια ομάδα στο M.I.T. (Rívest, Shamir, Adleman) και η μέθοδος την οποία ακολούθησαν βασίζεται σε αρχές της Θεωρίας Αριθμών. Ο RSA βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων αριθμών (συνήθως της τάξης των 1024 με 2048 bits) και χρησιμοποιεί δυο κλειδιά. Ένα δημόσιο κλειδί κατά τη διαδικασία της κρυπτογράφησης και ένα ιδιωτικό κλειδί κατά τη διαδικασία της αποκρυπτογράφησης.

Για να παραγάγετε τα δύο κλειδιά:
α. Επιλέξτε δύο τυχαίους μεγάλους πρωταρχικούς αριθμούς, τους p και q, και για μέγιστη ασφάλεια επιλέξτε να έχουν το ίδιο μήκος.
β. Υπολογίστε το αποτέλεσμα :

N = pxq και z = (p - 1) × (q - 1).

γ. Επιλέξτε έναν πρώτο αριθμό ως προς το z και ονομάστε τον d.
δ. Βρείτε το e, έτσι ώστε e × d 1 mod z.

Διαιρέστε το κείμενο (που θεωρείται ως συρμός bit) σε μπλοκ, έτσι ώστε κάθε μήνυμα κειμένου P, να πέφτει στο διάστημα $0 \leq P < n$.

Για να κρυπτογραφήσετε το μήνυμα P, υπολογίστε το $C= P^e \pmod n$. Για να αποκρυπτογραφήσετε το C υπολογίστε το $P = C^d \pmod n$.
Για την κρυπτογράφηση χρειάζεστε τα e και n. Για την αποκρυπτογράφηση, χρειάζεστε τα Επομένως , το δημόσιο κλειδί αποτελείται από το ζευγάρι (e, n) και το μυστικό κλειδί αποτελείται από το ζευγάρι (d, n).
Η ασφάλεια της μεθόδου βασίζεται στη δυσκολία της παραγοντοποίησης μεγάλων αριθμών. Εάν ο κρυπταναλυτής μπορούσε να παραγοντοποιήσει το (δημόσια γνωστό) n, θα μπορούσε στη συνέχεια να βρει τα p και q και απ' αυτά το z. Εάν διαθέτει τα z και e, μπορεί να βρει το d με τη βοήθεια του αλγόριθμου του Ευκλείδη.
Σύμφωνα με τον Rívest και τους συναδέλφους του, η παραγοντοποίηση ενός αριθμού με 200 ψηφία απαιτεί 4 δισεκατομμύρια χρόνια υπολογιστικού χρόνου, ενώ η παραγοντοποίηση ενός αριθμού με 500 ψηφία απαιτεί 10^{25} χρόνια. Και στις δύο περιπτώσεις, υποθέτουν ότι διαθέτουν τον καλύτερο γνωστό αλγόριθμο κι έναν υπολογιστή με χρόνο εντολής 1 μsec. Ακόμα και αν οι υπολογιστές συνεχίσουν να γίνονται ταχύτεροι κατά μία τάξη μεγέθους ανά δεκαετία θα χρειαστούν αιώνες για να γίνει δυνατή η παραγοντοποίηση αριθμών με 500

ψηφία αλλά και τότε οι απόγονοί μας θα μπορούν απλώς να επιλέγουν ακόμα μεγαλύτερα p και q.

Στη συνέχεια θα δούμε ένα απλό παράδειγμα του αλγόριθμου RSA. Στο παράδειγμα αυτό επιλέχθηκε p = 3 και q = 11, που δίνουν n = 33 και z = 20. Μια κατάλληλη τιμή για το d είναι d = 7, επειδή το 7 και το 20 δεν έχουν κοινούς παράγοντες. Μ' αυτές τις επιλογές, το e μπορεί να βρεθεί λύνοντας την εξίσωση 7×e 1 (mod 20), που δίνει e = 3. ≡ 20

Κείμενο (P) **Κρυπτογράφημα (C)** **αποκρυπτογράφηση**

Σύμβολο	Αριθμός	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Σύμβολο
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	1	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	5	E

Το κρυπτογραφημένο κείμενο C για το μήνυμα κειμένου P, δίνεται από τη σχέση $C \equiv P^3 \pmod{33}$. Το κρυπτογραφημένο κείμενο αποκρυπτογραφείται από τον δέκτη σύμφωνα με τον κανόνα $PC\equiv^7 \pmod{33}$. Ως παράδειγμα, το σχήμα δείχνει την κρυπτογράφηση του κειμένου "SUZANNE".

Επειδή οι πρώτοι αριθμοί που επιλέχτηκαν σ' αυτό το παράδειγμα είναι πολύ μικροί, το P πρέπει να είναι πολύ μικρότερο από το 33, οπότε κάθε μπλοκ κειμένου μπορεί να περιέχει μόνο έναν χαρακτήρα. Το αποτέλεσμα είναι ένα κρυπτογράφημα μοναλφαβητικής αντικατάστασης, κάτι όχι και τόσο εντυπωσιακό. Εάν όμως είχαμε επιλέξει p και $q \approx 10^{100}$, θα είχαμε $n\approx 10^{200}$ οπότε κάθε μπλοκ θα μπορούσε να φθάσει έως τα 664 bit ($2^{664} \approx 10^{200}$) ή 83 χαρακτήρες των 8 bit, έναντι των 8 χαρακτήρων του DES.

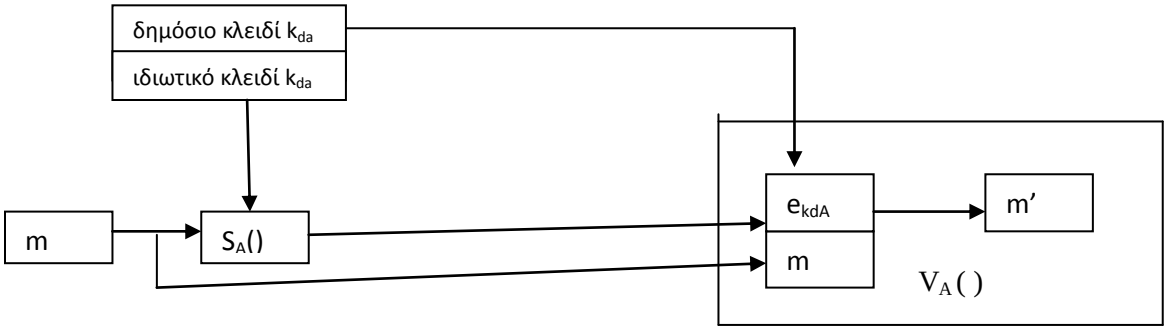
Ο RSA βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων αριθμών όπως αναφέραμε παραπάνω, είναι όμως υπερβολικά αργός για να κρυπτογραφήσει πραγματικά μεγάλες ποσότητες δεδομένων.

3. Ψηφιακές υπογραφές και ψηφιακά πιστοποιητικά.

3.1. Ψηφιακές υπογραφές ασύμμετρης κρυπτογραφίας.

Η ασύμμετρη κρυπτογραφία είναι ένα αποτελεσματικό μέσο για να πληρούν οι ψηφιακές υπογραφές όλες τις απαιτήσεις. Έτσι, στις ψηφιακές υπογραφές χρησιμοποιείται κατά κόρον η ασύμμετρη κρυπτογραφία.

Ένα απλό σύστημα ψηφιακής υπογραφής βασισμένο σε ασύμμετρη κρυπτογραφία παρουσιάζεται στο παρακάτω σχήμα .



Σχήμα 3.1. : Απλό σύστημα ψηφιακής υπογραφής

Το μήνυμα απλά κρυπτογραφείται με το ιδιωτικό κλειδί της Αλίκης και το κρυπτοκείμενο που προκύπτει αποτελεί την ψηφιακή υπογραφή της Αλίκης στο m. Η Αλίκη στέλνει το μήνυμα συνοδευόμενο με την ψηφιακή υπογραφή στον Βύρωνα. Ο Βύρων, ο οποίος κατέχει το δημόσιο κλειδί της Αλίκης, έχει τη δυνατότητα να επαληθεύσει την ψηφιακή υπογραφή, εκτελώντας την αποκρυπτογράφηση του κρυπτοκειμένου με το δημόσιο κλειδί της Αλίκης και να ελέγξει αν τα δύο μηνύματα συμπίπτουν.

Αυτό το απλό σύστημα έχει δύο μειονεκτήματα. Πρώτον, ο όγκος των μηνυμάτων που στέλνονται είναι διπλάσιος του μεγέθους του αρχικού μηνύματος m. Το μέγεθος της υπογραφής είναι μεταβλητό και εξαρτάται από το μέγεθος του μηνύματος. Σε δίκτυα όπου ανταλλάσσονται πολλά και μεγάλα μηνύματα, μπορεί να αυξηθεί απαγορευτικά η κίνηση και να μειωθεί η παραγωγή. Αν και το σύστημα της ψηφιακής υπογραφής ορίζει συνάρτηση υπογραφής η οποία είναι 1 – 1, δεν υπάρχει προστασία από επίθεση πλαστογραφίας, που είναι το δεύτερο μειονέκτημα του συστήματος. Η συνάρτηση της ψηφιακής υπογραφής είναι η αποκρυπτογράφηση του μηνύματος με το ιδιωτικό κλειδί. Αυτό σημαίνει ότι αν το μήνυμα έχει μεγαλύτερο μέγεθος από το μέγεθος που δέχεται η πράξη αποκρυπτογράφησης, τότε το μήνυμα θα διαιρεθεί σε μικρότερα τμήματα και θα κρυπτογραφηθεί το κάθε τμήμα χωριστά. Στην περίπτωση που ισχύει η ιδιότητα της αντιμετάθεσης στο ασύμμετρο κρυπτοσύστημα, τότε ο Βύρων μπορεί να κατασκευάσει μηνύματα επιλέγοντας και επαναλαμβάνοντας τμήματα του μηνύματος της αρεσκείας του και ταιριάζοντάς τα με τα αντίστοιχα τμήματα της ψηφιακής υπογραφής. Δηλαδή, σε αυτήν την επίθεση ο Βύρων μπορεί να κατασκευάσει έναν αριθμό από (m′, s′), από το αρχικό (m, s), έτσι ώστε $V_A(m', s') = 1$.

Στην περίπτωση που ο Βύρων έχει κάποια γνώση του μηνύματος, μπορεί η Αλίκη να στείλει μόνο την υπογραφή. Έτσι αν για παράδειγμα το μήνυμα είναι

γραμμένο στην Ελληνική, ο Βύρων εφαρμόζοντας την πράξη κρυπτογράφησης (που εδώ λειτουργεί ως αποκρυπτογράφηση) με το δημόσιο κλειδί της Αλίκης, μπορεί να εύκολα να διαπιστώσει αν το αποτέλεσμα που προκύπτει είναι Ελληνικά. Η Ελληνική γλώσσα όπως και κάθε φυσική γλώσσα έχει αρκετή περίσσεια, ώστε οποιαδήποτε τροποποίηση της υπογραφής θα έχει σαν αποτέλεσμα η κρυπτογράφησή του να οδηγήσει σε ασυνάρτητες για την Ελληνική γλώσσα λέξεις. Η γνώση του περιεχομένου του μηνύματος από τον παραλήπτη επιτρέπει μια άτυπη επαλήθευση της υπογραφής. Ένα τέτοιο σύστημα ψηφιακής υπογραφής έχει την ιδιότητα της **αυτοανάκτησης** (self recovery).

3.2. Τύποι κλειδιών.

Το σημείο αναφοράς της ασφάλειας ενός κρυπτοσυστήματος είναι οι ειδικές ποσότητες πληροφορίας που ονομάζουμε κλειδιά. Σε ένα καλά σχεδιασμένο κρυπτοσύστημα, η ασφάλειά του εξαρτάται αποκλειστικά από τα κλειδιά (αρχή του Kerchoff). Επομένως, η σωστή διαχείριση των κλειδιών συνιστά ενέργειες ζωτικής σημασίας για την ασφάλεια της επικοινωνίας δύο ή περισσοτέρων μελών.

Η διαχείριση κλειδιών αποτελείται από τη δημιουργία, διανομή, εγκατάσταση, χρήση, ανανέωση, ανάκληση, φύλαξη και καταστροφή κλειδιών. Εκτός από την καταστροφή των κλειδιών, όλες οι άλλες ενέργειες διαχείρισης μπορούν να περιλαμβάνουν κρυπτογραφικές τεχνικές.

Η ***κρυπτοπερίοδος*** ενός κλειδιού είναι ο χρόνος ο οποίος περιλαμβάνει τη δημιουργία, διανομή και χρήση ενός κλειδιού.

Η κρυπτοπερίοδος ενός κλειδιού εξαρτάται από τις ακόλουθες παραμέτρους:

- Μήκος του κλειδιού. Η κρυπτοπερίοδος αυξάνει με το μήκος του κλειδιού. Εφόσον το μήκος του κλειδιού είναι ένας από τους παράγοντες που επηρεάζουν την αποτελεσματικότητα της εξαντλητικής αναζήτησης, έπεται ότι η εξέλιξη της τεχνολογίας μειώνει την κρυπτοπερίοδο ενός κλειδιού με συγκεκριμένο μέγεθος.
- Ευαισθησία του απλού κειμένου ως προς την εμπιστευτικότητα. Όταν οι πληροφορίες που ανταλλάσσονται μεταξύ δύο ή περισσότερων μελών έχουν υψηλές απαιτήσεις εμπιστευτικότητας, τότε είναι επιθυμητό το κλειδί να αλλάζει συχνότερα, για να περιορίζει τη συλλογή πληροφοριών του αντιπάλου κάτω από το ίδιο κλειδί, το οποίο μπορεί να οδηγήσει σε επιτυχή κρυπτανάλυση. Επιπλέον, η τυχόν ανακάλυψη ενός κλειδιού θα αποκαλύψει μικρότερο τμήμα του απλού κειμένου.
- Τύπος του κλειδιού. Για δεδομένο μέγεθος κλειδιού, διαφορετικά κρυπτοσυστήματα έχουν και διαφορετική κρυπτοπερίοδο. Ισοδύναμα,

για δεδομένη κρυπτοπερίοδο αντιστοιχούν διαφορετικά μήκη κλειδιών σε διαφορετικά κρυπτοσυστήματα. Κλασσικά παραδείγματα είδαμε στα προηγούμενα κεφάλαια, όπου τα μεγέθη των κλειδιών μεταξύ συμμετρικών και ασύμμετρων κρυπταλγόριθμων έχουν διαφορές τάξης μεγέθους μεγαλύτερες του 10.

Το σύνολο των διαδικασιών που αποτελείται από τη διαδικασία δημιουργίας ενός κλειδιού, τη διανομή του, τη χρήση του και την αντικατάστασή του, ονομάζεται ***κύκλος ζωής*** του κλειδιού.

Τύποι κλειδιών

Τα κλειδιά ταξινομούνται ανάλογα με τον τύπο του κρυπταλγόριθμου και ανάλογα με τη χρήση για την οποία προορίζονται.
Ανάλογα με τον τύπο του κρυπταλγόριθμου, τα κλειδιά χωρίζονται σε τρεις κατηγορίες:

- μυστικό κλειδί, το οποίο ορίζεται σε συμμετρικό κρυπτοσύστημα. Το μυστικό κλειδί θα πρέπει να βρίσκεται στην κατοχή όλων των μελών που επικοινωνούν χρησιμοποιώντας συμμετρική κρυπτογραφία.

- δημόσιο κλειδί, το οποίο ορίζεται σε ασύμμετρο κρυπτοσύστημα. Το δημόσιο κλειδί είναι το κλειδί εκείνο το οποίο αναφέρεται σε κάποιο μέλος με το οποίο είναι επιθυμητή η επικοινωνία. Το δημόσιο κλειδί είναι γνωστό σε όλους.

- ιδιωτικό κλειδί, το οποίο ορίζεται σε ασύμμετρο κρυπτοσύστημα. Το ιδιωτικό κλειδί συνδέεται κρυπτογραφικά με το δημόσιο κλειδί και είναι γνωστό σε ένα μόνο μέλος.

Ανάλογα με τη χρήση για την οποία προορίζονται τα παραπάνω κλειδιά, διακρίνουμε τους ακόλουθους τύπους:

- κλειδί συνόδου (session key), το οποίο χρησιμοποιείται για την κρυπτογράφηση για μόνο μία περίοδο επικοινωνίας. Μετά το τέλος της επικοινωνίας, το κλειδί καταστρέφεται. Σε επόμενη περίοδο επικοινωνίας, δημιουργείται νέο κλειδί συνόδου.
- κλειδί τερματικού (terminal key). Στην περίπτωση που το κλειδί συνόδου δεν καταστρέφεται, αλλά χρησιμοποιείται για περισσότερες από μία επικοινωνίες ενός μέλους, τότε το κλειδί αυτό ονομάζεται κλειδί τερματικού.
- κύριο κλειδί (master key). Συνήθως ένα μέλος στην πράξη κατέχει πολλά κλειδιά συνόδου και κλειδιά τερματικού. Προκειμένου να απλουστευθεί η διαχείριση των κλειδιών, χρησιμοποιείται το κύριο κλειδί. Έτσι κατά την αποθήκευση των κλειδιών, αυτά κρυπτογραφούνται με το κύριο κλειδί,

οπότε ο έλεγχος της ασφαλούς αποθήκευσης εξαρτάται από μία και μόνον ποσότητα, το κύριο κλειδί. Επίσης, το κύριο κλειδί μπορεί να χρησιμοποιηθεί για τη δημιουργία κλειδιού τερματικού, ή κλειδιού συνόδου.

Οι παραπάνω τύποι κλειδιών έχουν διαφορετικές κρυπτοπεριόδους. Το κλειδί συνόδου ονομάζεται και βραχυπρόθεσμο κλειδί (short term key) και έχει τη μικρότερη κρυπτοπερίοδο από τους τρεις τύπους κλειδιών. Αντίθετα, το τερματικό κλειδί και το κύριο κλειδί είναι μακροπρόθεσμα κλειδιά (long term keys), με μεγαλύτερες κρυπτοπεριόδους. Μεταξύ των δύο αυτών κλειδιών, το κύριο κλειδί έχει μεγαλύτερη κρυπτοπερίοδο, αφού χρειάζεται για την αποθήκευση των υπολοίπων κλειδιών.

Η ύπαρξη των διαφορετικών τύπων κλειδιών με βάση τον προορισμό χρήσης τους, οφείλεται σε πρακτικούς λόγους. Όπως τονίζουμε κατ' επανάληψη σε αυτό το βιβλίο, η κρυπτογραφία δε λύνει τα προβλήματα, αλλά τα μετασχηματίζει σε μορφές όπου η διαχείριση του προβλήματος είναι αποτελεσματικότερη και ευκολότερη. Είδαμε ότι προστατεύοντας μια συγκριτικά μικρή ποσότητα πληροφορίας που ονομάζουμε «κλειδί», μπορούμε με τη χρήση της κρυπτογραφίας να προστατεύσουμε μια κατά πολύ μεγαλύτερη σε μέγεθος πληροφορία, το «απλό κείμενο». Αντίστοιχα, με τη διαχείριση των κλειδιών, χρησιμοποιούμε κλειδιά για να προστατεύσουμε άλλα κλειδιά. Η ανάγκη αυτή δημιουργήθηκε λόγω της ύπαρξης πολλών κλειδιών σε ένα σύστημα επικοινωνίας.

3.2.1. Υποδομές δημόσιου κλειδιού.

Οι υποδομές δημόσιου κλειδιού (public key infrastructures, PKIs) είναι μοντέλα τα οποία αναπτύχθηκαν με κύριο σκοπό την πιστοποίηση των οντοτήτων που συμμετέχουν σε ένα σύστημα επικοινωνίας. Έτσι, η ασφάλεια και η αξιοπιστία της διαδικασίας αυθεντικοποίησης των μελών που γίνεται με τη χρήση ενός PKI, συνδέεται με την κρυπτογραφική ισχύ των κρυπταλγόριθμων που υποστηρίζει το PKI. Ωστόσο, η συνολική ασφάλεια της διαδικασίας πιστοποίησης δεν εξαρτάται μόνον από την ισχύ του κρυπταλγόριθμου. Όπως θα δούμε στη συνέχεια, ένα PKI αποτελείται από διάφορες οντότητες, όπου η κάθε οντότητα έχει συγκεκριμένους ρόλους. Έτσι, η συνολική ασφάλεια εξαρτάται από την εκτέλεση των ρόλων από τις οντότητες. Θα διαπιστώσουμε για μια ακόμη φορά ότι η κρυπτογραφία μετασχηματίζει προβλήματα ασφάλειας σε μορφές που επιτρέπουν αποτελεσματικότερη διαχείριση, χωρίς όμως να λύνει τα προβλήματα αυτά.

Η διαδικασία αυθεντικοποίησης ενός μέλους ή γενικότερα μιας οντότητας χαρακτηρίζεται ισχυρή, αν η πιθανότητα απάτης είναι ικανοποιητικά μικρή. Η απάτη αφορά την προσπάθεια του αντιπάλου να προσποιηθεί άλλη ταυτότητα.

Επειδή η αυθεντικοποίηση ενός μέλους στην ασύμμετρη κρυπτογραφία γίνεται με τη χρήση του δημόσιου κλειδιού του μέλους, έπεται ότι η όλη διαδικασία αυθεντικοποίησης εξαρτάται από την αυθεντικότητα του δημόσιου κλειδιού. Αν κατά την αυθεντικοποίηση ενός μέλους δεν υπάρχει τρόπος να ελεγχθεί η αυθεντικότητα του δημόσιου κλειδιού του μέλους αυτού, τότε ο αντίπαλος θα μπορεί να αντικαταστήσει το δικό του δημόσιο κλειδί χωρίς αυτό να γίνει αντιληπτό.

Χωρίς τη συμμετοχή μιας έμπιστης τρίτης οντότητας, η λύση στο πρόβλημα της αυθεντικότητας των κλειδιών θα ήταν το κάθε μέλος να έχει στην κατοχή του τα δημόσια κλειδιά όλων των μελών, τα οποία τα έχει παραλάβει μέσω ενός καναλιού που προσφέρει υψηλή ακεραιότητα. Ας σημειωθεί ότι το κανάλι δεν απαιτείται να προσφέρει εμπιστευτικότητα, αφού τα κλειδιά είναι δημόσια. Η ακεραιότητα όμως απαιτείται να είναι υψηλή, ώστε ο αντίπαλος να μην έχει τη δυνατότητα να αντικαταστήσει τα δημόσια κλειδιά με τα δικά του. Εναλλακτικά, το κάθε μέλος θα μπορούσε να παραλάβει μόνον εκείνα τα δημόσια κλειδιά τα οποία θα χρειασθεί προκειμένου να επικοινωνήσει με τα αντίστοιχα μέλη. Ένα τέτοιο μοντέλο διανομής δημόσιων κλειδιών δεν είναι πρακτικό, αφού δεν μπορεί να κλιμακωθεί με ευκολία και απαιτεί διαρκώς ασφαλές κανάλι με υψηλή ακεραιότητα.

Η συμμετοχή μιας έμπιστης τρίτης οντότητας μπορεί να απλοποιήσει το παραπάνω πρόβλημα αποτελεσματικά. Αντί να απαιτείται η ασφαλής μεταφορά όλων των δημόσιων κλειδιών, αρκεί να διανεμηθεί με υψηλή ακεραιότητα το δημόσιο κλειδί της έμπιστης τρίτης οντότητας και να χρησιμοποιηθεί αυτό για να πιστοποιήσει τα δημόσια κλειδιά των υπολοίπων. Αυτό σε γενικές γραμμές είναι μια υποδομή δημόσιου κλειδιού, ή ένα PKI για συντομία, που θα εξετάσουμε στη συνέχεια.

3.2.2. Συστατικά ενός PKI.

Ένα PKI αποτελείται από τα εξής συστατικά:

- Αρχή Πιστοποίησης (Certification Authority). Η Αρχή Πιστοποίησης είναι το κεντρικό συστατικό ενός PKI. Αποτελεί την έμπιστη τρίτη οντότητα η οποία είναι υπεύθυνη για την πιστοποίηση των δημόσιων κλειδιών των μελών. Η ακεραιότητα όλης της υποδομής συγκεντρώνεται στην Αρχή Πιστοποίησης.
- Αρχή Εγγραφής (Registration Authority). Η Αρχή Εγγραφής είναι προαιρετική. Εμφανίσθηκε κυρίως για εμπορικούς λόγους και στην περίπτωση απουσίας αυτής, τα καθήκοντά της αναλαμβάνει η Αρχή

Πιστοποίησης. Η Αρχή Εγγραφής είναι υπεύθυνη για την αρχική εξακρίβωση των στοιχείων του μέλους, προτού πιστοποιηθεί το δημόσιό κλειδί του.

- Εντολέας (Principal). Είναι η οντότητα η οποία πιστοποιείται από την Αρχή Πιστοποίησης. Οι οντότητες με τις οποίες έχουμε ασχοληθεί είναι τα επικοινωνούντα μέλη, τα οποία είναι φυσικά πρόσωπα, αλλά μπορούν να είναι και υπολογιστές που βρίσκονται σε δίκτυο, μηχανές ATM των τραπεζών, κτλ.
- Πιστοποιητικό δημόσιου κλειδιού (Public key certificate). Το πιστοποιητικό δημόσιου κλειδιού είναι μια δομή δεδομένων η οποία αποτελείται από ένα σύνολο στοιχείων που περιλαμβάνει δύο μέρη. Το πρώτο μέρος αποτελείται από την περιγραφή του εντολέα και το δημόσιο κλειδί του. Το δεύτερο μέρος του πιστοποιητικού αποτελείται από την ψηφιακή υπογραφή της Αρχής Πιστοποίησης επάνω στα στοιχεία του πρώτου μέρους.
- Αποθήκη πιστοποιητικών (certificate repository). Αποτελεί τον χώρο αποθήκευσης των πιστοποιητικών ενός PKI. Στην πράξη αυτό υλοποιείται από υπηρεσία καταλόγου (directory service) στο οποίο μπορούν να απευθυνθούν τα μέλη προκειμένου να παραλάβουν το δημόσιο κλειδί του μέλους με το οποίο επιθυμούν να επικοινωνήσουν.
- Υπηρεσία ανάκλησης πιστοποιητικού (certificate revocation service). Η υπηρεσία ανάκλησης πιστοποιητικού συμμετέχει στη διαδικασία εξακρίβωσης της εγκυρότητας του πιστοποιητικού και παρέχει πληροφορίες σχετικά με την ανάκληση αυτού.
- Δήλωση Χρήσης Πιστοποιητικού (Certificate Practice Statement). Είναι ένα είδος συμφωνητικού το οποίο περιγράφει τους ρόλους, τις διαδικασίες, τα δικαιώματα και τις υποχρεώσεις καθενός από τα μέλη. Για παράδειγμα, περιγράφει τα δικαιολογητικά τα οποία θα πρέπει να κατατεθούν από τον εντολέα προκειμένου να του εκδοθεί το πιστοποιητικό.

Από την παραπάνω περιγραφή των συστατικών μπορεί να γίνει αντιληπτή η καίρια θέση της Αρχής Πιστοποίησης και η εξάρτηση της ασφάλειας του PKI από αυτήν. Η δύναμη που έχει η Αρχή Πιστοποίησης στο να δημιουργεί πιστοποιητικά για τα μέλη είναι και η συνέπεια της απαίτησης εμπιστοσύνης, η οποία καθιστά την Αρχή Πιστοποίησης ως Έμπιστη Τρίτη Οντότητα.

3.3. Συνάρτηση κατακερματισμού.

Η συνάρτηση κατακερματισμού χρησιμοποιείται ώστε να διασφαλιστεί η ακεραιότητα των δεδομένων και η αυθεντικότητα των μηνυμάτων. Η συνάρτηση κατακερματισμού δέχεται ως είσοδο ένα μήνυμα και παράγει ως αποτέλεσμα μια

σύνοψη του μηνύματος, αποτύπωμα ή τιμή κατακερματισμού. Πιο συγκεκριμένα μια συνάρτηση κατακερματισμού δέχεται μια πεπερασμένη σειρά από bits και την μετατρέπει σε μια σειρά σταθερού μήκους.

Έχει πεδίο ορισμού το D και πεδίο τιμών το R (h:D→R) και |D|>|R|. Είναι μονής κατεύθυνσης πράγμα που σημαίνει ότι η ύπαρξη συγκρούσεων (δηλαδή η πιθανότητα δυο μηνύματα να έχουν την ίδια σύνοψη) είναι εξαιρετικά μικρή. Πράγματι, αν έχουμε ως είσοδο μια t-bitσυμβολοσειρά (με t>n), αν η h ήταν τυχαία με την έννοια ότι όλες οι έξοδοι ήταν ισοπίθανες, τότε περίπου 2t-n θα συνοψιζόταν σε κάθε έξοδο, και δύο τυχαίες είσοδοι θα έδιναν το ίδιο αποτέλεσμα με πιθανότητα 2-n (ανεξάρτητο από το t).

Σε συνδυασμό με τις ψηφιακές υπογραφές η συνάρτηση κατακερματισμού εγγυάται την ακεραιότητα των δεδομένων. Το μήνυμα πρώτα κατακερματίζεται και μετά η τιμή του κατακερματισμού υπογράφεται αντί για το αρχικό μήνυμα. Μια ξεχωριστή κλάση
συναρτήσεων κατακερματισμού που ονομάζεται message authentication codes (MACs), μας βοηθάει να καταλάβουμε την αυθεντικότητα του μηνύματος με συμμετρικές τεχνικές. Ο αλγόριθμος MAC μπορεί να θεωρηθεί ως μια συνάρτηση κατακερματισμού που δέχεται δύο διακριτές εισόδους, ένα μήνυμα και ένα ιδιωτικό κλειδί και παράγει μια σταθερού μήκους έξοδο, με σκοπό να μην μπορεί κάποιος να παράγει το ίδιο αποτέλεσμα χωρίς την γνώση του κλειδιού.

Μπορούμε να εξασφαλίσουμε την ακεραιότητα των δεδομένων με τον τρόπο που περιγράφεται παρακάτω. Η τιμή του κατακερματισμού που είναι αποτέλεσμα της εφαρμογής της συνάρτησης κατακερματισμού σε ένα μήνυμα x μπορεί να υπολογισθεί την χρονική στιγμή T1. Η ακεραιότητα της τιμής του κατακερματισμού (αλλά όχι του ίδιου του μηνύματος) είναι εξασφαλισμένη με κάποιον τρόπο.

Σε κάποια ακόλουθη χρονική στιγμή T2 διεξάγεται ο ακόλουθος έλεγχος ώστε να διαπιστωθεί άμα έχει τροποποιηθεί το μήνυμα, με άλλα λόγια αν το μήνυμα x' είναι το ίδιο με το αρχικό. Έτσι υπολογίζεται η τιμή του κατακερματισμού για το μήνυμα x' και συγκρίνεται με την τιμή κατακερματισμού του αρχικού μηνύματος. Αν είναι ίδιες τότε κάποιος μπορεί να συμπεράνει ότι οι είσοδοι στην συνάρτηση κατακερματισμού είναι ίσες, οπότε το μήνυμα x δεν έχει τροποποιηθεί.

Συνεπώς το πρόβλημα που παρουσιάζεται όταν θέλουμε να επαληθεύσουμε την ακεραιότητα ενός μεγάλου μηνύματος μετατρέπεται στην διερεύνηση μιας σταθερού μεγέθους τιμής κατακερματισμού. Για να είναι αποτελεσματική μια τιμή κατακερματισμού θα πρέπει να είναι με μοναδικό τρόπο συνδεδεμένη με την είσοδο και οι συγκρούσεις να είναι υπολογιστικά δύσκολες να βρεθούν.

Ορισμός: Μια συνάρτηση κατακερματισμού είναι μια συνάρτηση, με τουλάχιστον, τις ακόλουθες ιδιότητες:

Συμπίεση-Η είσοδος της h είναι οποιουδήποτε μήκους, ενώ η έξοδος h(x) έχει πεπερασμένο, σταθερό μήκος.

Ευκολία στον υπολογισμό-Με δοσμένη την h και μια είσοδο x, η h(x) υπολογίζεται εύκολα.

3.3.1. Μέγεθος της σύνοψης.

Η επιτυχία εύρεσης συγκρούσεων σε μια συνάρτηση hash εξαρτάται τόσο από το σχεδιασμό των μετασχηματισμών της συνάρτησης, όσο και από το μέγεθος της σύνοψης. Για παράδειγμα, στην περίπτωση όπου η σύνοψη έχει μέγεθος ίσο με 1 bit, αναμένουμε τα μισά μηνύματα να αντιστοιχίζονται στην τιμή 0 και τα υπόλοιπα στην τιμή 1. Συνεπώς η επιλογή ενός επαρκούς μεγέθους της σύνοψης για να αποτρέψει τις συγκρούσεις είναι ένα σημαντικό βήμα στον καθορισμό μιας συνάρτησης hash.

3.3.2. Επίθεση γενεθλίων στις ψηφιακές υπογραφές.

Είναι σημαντικό να αναφερθεί πως η δυνατότητα παραγωγής δυο εγγράφων με την ίδια σύνοψη μπορεί να είναι χρήσιμη για κάποιον κακόβουλο και μάλιστα είναι σαφώς ευκολότερο από την παραγωγή ενός εγγράφου με συγκεκριμένη σύνοψη.

Η μέθοδος για να πραγματοποιηθεί αυτό είναι γνωστή ως ‘επίθεση γενεθλίων’ ή ‘παράδοξο των γενεθλίων’ και ονομάζεται έτσι επειδή αν ερωτηθεί μια ομάδα ατόμων άνω των 25 ετών για τα γενέθλια τους, υπάρχει μεγάλη πιθανότητα δύο άτομα να έχουν την ίδια ημέρα γενέθλια.

Για να εφαρμοσθεί αυτή η επίθεση στις συνόψεις αντικειμένων, πρέπει να πραγματοποιηθούν μια σειρά από ακόλουθες αλλαγές σε δυο αντικείμενα και κάθε φορά να παράγεται μια σύνοψη τους, ώστε να παραχθεί μια λίστα από συνόψεις για το κάθε αντικείμενο. Μετά από ένα πλήθος προσπαθειών, υπάρχει μεγάλη πιθανότητα κάποια εκδοχή των δύο αντικειμένων που παράγουν την ίδια σύνοψη θα έχει κατασκευαστεί.

Συνήθως, στόχος αυτής της επίθεσης είναι να υπογραφεί από το θύμα το ένα έγγραφο και στη συνέχεια να χρησιμοποιηθεί η υπογραφή του σαν να υπέγραψε το άλλο. Για την αποφυγή της επίθεσης γενεθλίων, οι συναρτήσεις Κατακερματισμού θα πρέπει να παράγουν αρκούντος μεγάλες συνόψεις. Συγκεκριμένα επειδή αυτή η επίθεση ελαττώνει αποτελεσματικά τη δυσκολία μιας επίθεσης περίπου στο μισό του πλήθους των bits της σύνοψης, οι συναρτήσεις κατακερματισμού πρέπει να παράγουν διπλάσια σύνοψη για να είναι ασφαλείς.

3.3.3. Αυθεντικοποίηση και ακεραιότητα μηνύματος.

Όπως αναφέρθηκε στην εισαγωγή της ενότητας των hash συναρτήσεων, οι συναρτήσεις αυτές μπορούν να προσφέρουν αυθεντικοποίηση και ακεραιότητα των δεδομένων. Οι οικογένειες των κρυπτογραφικών hash συναρτήσεων που χρησιμοποιούνται στην αυθεντικοποίηση και στην ακεραιότητα κατατάσσονται στις κατηγορίες των κωδικών αυθεντικοποίησης μηνυμάτων και των κωδικών ανίχνευσης τροποποίησης.

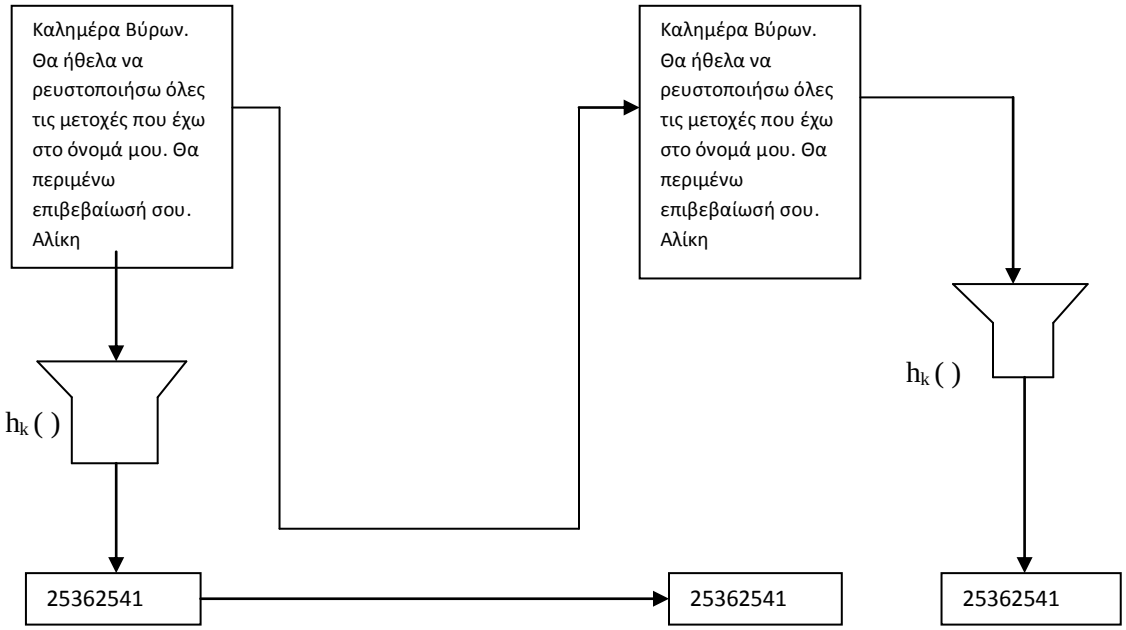
Ο ***κώδικας αυθεντικοποίησης μηνύματος*** (Message Authentication Code, MAC) είναι μια μονόδρομη κρυπτογραφική hash συνάρτηση με κλειδί, η οποία προσφέρει ασθενή αντίσταση σε συγκρούσεις:

- δοθέντων x, $h_k(x)$, είναι υπολογιστικά αδύνατο να βρεθεί x' τέτοιο ώστε $h_k(x') = h_k(x)$.

Ο ***κώδικας ανίχνευσης τροποποίησης*** (Modification Detection Code, MDC) είναι μια μονόδρομη κρυπτογραφική hash συνάρτηση άνευ κλειδιού, η οποία προσφέρει ασθενή αντίσταση σε συγκρούσεις:

- δοθέντων x, $h(x)$, είναι υπολογιστικά αδύνατο να βρεθεί x' τέτοιο ώστε $h(x') = h(x)$.

Η επιλογή μεταξύ του MAC και του MDC εξαρτάται από τις συγκεκριμένες συνθήκες της εφαρμογής καθώς και την υπόθεση της επίθεσης του αντιπάλου. Ο MAC αφορά περισσότερο δύο μέλη τα οποία επικοινωνούν άμεσα και οι πληροφορίες ανταλλάσσονται και προς τις δύο κατευθύνσεις. Στην περίπτωση που απαιτείται υψηλός βαθμός ακεραιότητας ενώ η εμπιστευτικότητα είναι χαμηλή, η Αλίκη και ο Βύρων μπορούν να χρησιμοποιήσουν ένα πρωτόκολλο ανταλλαγής μυστικού κλειδιού που θα χρησιμοποιηθεί στον υπολογισμό του MAC. Το κάθε μήνυμα που ανταλλάσσεται συνοδεύεται από τον αντίστοιχο MAC. Μόλις ο Βύρων λάβει το μήνυμα και το MAC, υπολογίζει ανεξάρτητα το MAC και ελέγχει αν είναι το ίδιο με το MAC που έχει λάβει. Αν οι δύο συνόψεις συμπίπτουν, τότε το μήνυμα που έλαβε είναι ακριβώς αυτό που έστειλε η Αλίκη. Η διαδικασία παρουσιάζεται στο σχήμα που ακολουθεί.



Σχήμα 3.2. : Έλεγχος ακεραιότητας με Mac.

Παράδειγμα περίπτωσης όπου απαιτείται μεγάλη ακεραιότητα και χαμηλή εμπιστευτικότητα είναι στα σήματα ελέγχου των μέσων μαζικής μεταφοράς. Η πληροφορία που φτάνει για παράδειγμα σε έναν πύργο ελέγχου εναέριας κυκλοφορίας θα πρέπει να είναι ακριβής και σωστή, γιατί στην αντίθετη περίπτωση ο χάρτης των θέσεων των αεροπλάνων δε θα συμπίπτει με την πραγματικότητα. Παρόμοια, τα σήματα ελέγχου των γραμμών των τρένων και οι εντολές αλλαγής των «ψαλιδιών» στις σιδηροδρομικές γραμμές δεν απαιτούν εμπιστευτικότητα, αλλά η αυθαίρετη αλλαγή αυτών μπορεί να προκαλέσει ατυχήματα.

Η χρήση του MDC συναντάται σε ασύμμετρη επικοινωνία, στις περιπτώσεις όπου ένας στέλνει ένα μήνυμα σε πολλούς. Στο Διαδίκτυο αυτό συναντάται συχνά στη λήψη ηλεκτρονικών αγαθών όπως ηλεκτρονικά βιβλία, λογισμικό κτλ. Όταν μια εταιρεία λογισμικού για παράδειγμα ανακοινώνει τη διάθεση αναβαθμίσεως του λογισμικού της, μπορεί να δημοσιεύσει τον αντίστοιχο MDC σε εφημερίδα, περιοδικό, ή γενικότερα σε κάποιο δημόσια διαθέσιμο μέσο. Ο πελάτης μπορεί να «κατεβάσει» το λογισμικό από το δικτυακό τόπο της εταιρείας και για να ελέγξει ότι το λογισμικό είναι ακριβώς αυτό που έχει προσφέρει η εταιρεία, υπολογίζει τον MDC και τον συγκρίνει με αυτόν που έχει δημοσιευθεί. Επειδή δεν υπάρχει κλειδί στο σχήμα αυτό, ο έλεγχος μπορεί να πραγματοποιηθεί από οποιονδήποτε πελάτη.

Όπως αναφέρεται συχνά σε βιβλία, η κρυπτογραφία δε λύνει το πρόβλημα αλλά το μετασχηματίζει σε μορφή τέτοια ώστε η διαχείριση του προβλήματος να είναι πιο αποτελεσματική. Με βάση το σκεπτικό αυτό, παρουσιάζουμε ένα

πρωτόκολλο ελέγχου ακεραιότητας ενός εγγράφου μεταξύ της Αλίκης και του Βύρωνα:

0. Η Αλίκη επιθυμεί να στείλει στον Βύρωνα ένα πολυσέλιδο έγγραφο όσο το δυνατόν γρηγορότερα. Η λύση να το στείλει διαβάζοντάς το μέσω τηλεφώνου δεν επαρκεί. Το τηλέφωνο προσφέρει ακεραιότητα επειδή ο Βύρων γνωρίζει τη φωνή της Αλίκης, επομένως είναι αδύνατο κάποιος αντίπαλος να αλλάξει τα λόγια της. Η Αλίκη και ο Βύρων αποφασίζουν να εκ-μεταλλευτούν την ακεραιότητα που προσφέρει η τηλεφωνική επικοινωνία ως εξής:
1. Η Αλίκη υπολογίζει τον MDC του εγγράφου και στη συνέχεια στέλνει με ηλεκτρονικό ταχυδρομείο το έγγραφο στον Βύρωνα.
2. Μόλις παραλάβει το έγγραφο ο Βύρων υπολογίζει τον MDC του εγγράφου.
3. Ο Βύρων τηλεφωνεί την Αλίκη και της εκφωνεί το αποτέλεσμα (σύνοψη) του υπολογισμού του MDC.
4. Η Αλίκη επιβεβαιώνει αν η σύνοψη του Βύρωνα ταυτίζεται με τη σύνοψη που έχει υπολογίσει η ίδια.

Η Αλίκη και ο Βύρων μπορούν να συμφωνήσουν μέσω της τηλεφωνικής επικοινωνίας για τον αλγόριθμο MDC που θα χρησιμοποιήσουν. Έτσι, ενώ αρχικά η απαίτηση να μεταδοθεί το έγγραφο μέσω τηλεφώνου προκειμένου να εξασφαλισθεί υψηλή ακεραιότητα, μετασχηματίζεται στη μετάδοση ενός μικρότερου μηνύματος μέσω τηλεφώνου, με τον ίδιο βαθμό ασφάλειας.

Παραδειγμα – Εφαρμογή του παραδόξου των γενεθλίων στην πλαστογραφία μηνύματος (Yuval, 1979). Σε αυτό το παράδειγμα αντίπαλος είναι η Αλίκη, παρόλο που επικοινωνεί με τον Βύρωνα για την υπογραφή κάποιου συμβολαίου. Η Αλίκη κλείνει μια συμφωνία με τον Βύρωνα και αναλαμβάνει να ετοιμάσει το αντίστοιχο συμβόλαιο για να το υπογράψει ο Βύρων.

1. Στην πραγματικότητα η Αλίκη ετοιμάζει δύο συμβόλαια, ένα όπως συμφώνησε με τον Βύρωνα και ένα ευνοϊκότερο για αυτήν και λιγότερο για τον Βύρωνα. Οι γνώσεις του Βύρωνα σχετικά με κρυπτογραφία δεν είναι αρκετές, οπότε η Αλίκη επιλέγει MDC ο οποίος υποκύπτει σε επίθεση εύρεσης συγκρούσεων.
2. Η Αλίκη υπολογίζει τη σύνοψη του αρχικού συμβολαίου και με βάση την τιμή αυτή, κάνει μικρές και ασήμαντες αλλαγές στο δεύτερο συμβόλαιο, προκειμένου να πετύχει μια σύνοψη ίδια με αυτήν του πρώτου συμβολαίου.
3. Η Αλίκη στέλνει το πρώτο συμβόλαιο στον Βύρωνα, ο οποίος υπολογίζει ανεξάρτητα τη σύνοψη αυτού και την υπογράφει (κρυπτογραφεί τη σύνοψη με το ιδιωτικό του κλειδί).

4. Ο Βύρων στέλνει την υπογεγραμμένη σύνοψη στην Αλίκη, η οποία καταστρέφει το πρώτο συμβόλαιο και επισυνάπτει την υπογραφή του Βύρωνα στο δεύτερο. Σε τυχόν διαφωνία, η Αλίκη είναι σε θέση να παρουσιάσει το δεύτερο συμβόλαιο που φαινομενικά έχει υπογραφεί από τον Βύρωνα.

Από το παράδειγμα φαίνεται ότι η απαίτηση να πληρούνται οι κρυπτογραφικές ιδιότητες μιας συνάρτησης hash εξαρτάται τόσο από την εφαρμογή, όσο και από την υπόθεση της επίθεσης του αντιπάλου. Μπορούμε να ταξινομήσουμε τις ευκαιρίες, ικανότητες και στόχους του αντιπάλου, ως προς τις MAC και MDC, όπως φαίνεται στον πίνακα.

κατηγορία μονόδρομης	στόχοι αντιπάλου	ευκαιρίες / ικανότητες
hash	Εντοπισμός κλειδιού	πλαστογραφία
MAC	Εντοπισμός χ΄, τέτοιου ώστε Για δεδομένο χ είναι $h_k(x) = h_k(x')$ (Με το κλειδί γνωστό στον αντίπαλο)	επίθεση γνωστού κειμένου x, $h_k(x)$
	Εντοπισμός δύο χ και χ' έτσι ώστε $h_k(x) = h_k(x')$ (με το κλειδί άγνωστο στον αντίπαλο)	επίθεση επιλεγμένου κειμένου x, $h_k(x)$
MDC	Εντοπισμός χ΄, τέτοιου ώστε για δεδομένο χ είναι h(x) = h(x')	επίθεση γνωστού κειμένου x, h(x)
	Εντοπισμός δύο χ και χ' έτσι ώστε h(x) = h(x')	επίθεση επιλεγμένου κειμένου x, h(x)

Πίνακας 3.3. : Ταξινόμηση στόχων και ικανοτήτων του αντιπάλου

Γενικά, αν και οι απαιτήσεις ασφάλειας μιας MAC συνάρτησης είναι παρόμοιες με αυτές των κρυπταλγόριθμων, υπάρχουν ορισμένες ουσιώδεις διαφορές. Πρώτον, στην περίπτωση των MAC ο σχεδιασμός των μονόδρομων συναρτήσεων έχει περισσότερους βαθμούς ελευθερίας, από τους κρυπταλγόριθμους. Στους κρυπταλγόριθμους η κρυπτογραφική πράξη θα πρέπει να είναι ενριπτική (injective), ώστε για κάθε κρυπτογράφηση να ορίζεται μοναδικά η αποκρυπτογράφηση. Στις MAC και γενικά στις μονόδρομες hash συναρτήσεις, η αντιστροφή δεν απαιτείται, οπότε οι υποψήφιες συναρτήσεις είναι πολύ περισσότερες.

Δεύτερον, μια συνάρτηση MAC προσφέρει αυθεντικοποίηση και όχι εμπιστευτικότητα. Για το λόγο αυτό δεν υπάρχουν νομικοί περιορισμοί στη χρήση της κρυπτογραφίας. Αντίθετα στην περίπτωση των κρυπταλγόριθμων όπου το μήνυμα κρυπτογραφείται, το μέγεθος του κλειδιού είναι νομικά ελεγχόμενο και εξαρτάται από τη χώρα στην οποία εκτελείται η κρυπτογράφηση. Στη Γαλλία για παράδειγμα είναι παράνομη η χρήση του κρυπταλγόριθμου Vigenère, όταν η κυβέρνηση δεν έχει αντίγραφο του κλειδιού. Ας θυμηθούμε ότι ο κρυπταλγόριθμος αυτός είναι μια απλή πρόσθεση modulo 2 του απλού κειμένου με κλειδί.

Από την πλευρά του αντιπάλου, αν και οι στόχοι και οι τρόποι επίθεσης των MAC έχουν ομοιότητες με αυτές των κρυπτοσυστημάτων, υπάρχουν βασικές διαφορές. Ανάλογα με την πληροφορία που μπορεί να έχει στην κατοχή του ο αντίπαλος, θα έχει και διάφορες ευκαιρίες επίθεσης. Στην περίπτωση ενός κρυπτοσυστήματος, θεωρούμε ότι ο αντίπαλος είτε προσπαθεί να βρει το κλειδί, είτε να αποκρυπτογραφήσει το κρυπτοκείμενο. Ανάλογα με τις δυνατότητες και ευκαιρίες που έχει ο αντίπαλος, υπάρχει το ενδεχόμενο να γνωρίζει ορισμένα ζευγάρια απλού κειμένου και κρυπτοκειμένου, οπότε στην περίπτωση αυτή μπορεί να εκτελέσει την επίθεση με γνωστό απλό κείμενο. Αν όμως ο αντίπαλος δεν έχει πρόσβαση σε απλό κείμενο, τότε το σενάριο επίθεσης τον περιορίζει στην επίθεση γνωστού κρυπτοκειμένου. Στην περίπτωση των μονόδρομων hash συναρτήσεων, σε ένα μήνυμα του οποίου η αυθεντικοποίηση προστατεύεται με μια συνάρτηση MAC, ο αντίπαλος γνωρίζει πάντοτε το απλό κείμενο και την αντίστοιχη σύνοψη. Για να «σπάσει» την αυθεντικοποίηση, ο αντίπαλος θα πρέπει να ανακαλύψει το κλειδί της MAC.

Επομένως, η ασφάλεια της αυθεντικοποίησης εξαρτάται από το μήκος του κλειδιού. Αν θεωρήσουμε ότι η μόνη επίθεση που μπορεί να εκτελέσει κανείς στη MAC είναι η εξαντλητική αναζήτηση στο κλειδί, τότε μπορούμε να δείξουμε ότι η προσπάθεια που απαιτείται για να ανακαλύψει το κλειδί είναι ίση ή μεγαλύτερη από την προσπάθεια που θα έκανε για να ανακαλύψει το ίδιο (σε μέγεθος) κλειδί, σε ένα κρυπτοσύστημα. Για να είναι οι επιθέσεις στη MAC και στο κρυπτοσύστημα συγκρίσιμες, θεωρούμε ότι ο αντίπαλος έχει δυνατότητα επίθεσης γνωστού απλού κειμένου στο κρυπτοσύστημα, αφού στην περίπτωση της MAC παρέχεται μόνο αυθεντικοποίηση και όχι εμπιστευτικότητα.

Όπως γνωρίζουμε, στην επίθεση γνωστού κειμένου σε ένα κρυπτοσύστημα με κλειδί $\boldsymbol{k}$, ο αντίπαλος γνωρίζει ζεύγη απλού κειμένου και κρυπτοκειμένου p_i, c_i και επιλέγει συστηματικά κλειδιά $\boldsymbol{k}_j \in \boldsymbol{K}$, ώσπου να ανακαλύψει το κλειδί $\boldsymbol{k}$ για το οποίο $p_i = d_{\boldsymbol{k}}(c_i)$, ή ισοδύναμα $c_i = e_{\boldsymbol{k}}(p_i)$. Με εξαντλητική αναζήτηση, οι αναμενόμενες δοκιμές του αντιπάλου είναι $2^k/2$ ή 2^{k-1}, όπου k το μήκος του κλειδιού σε bits. Στην περίπτωση της επίθεσης στη MAC, εξετάζουμε δύο περιπτώσεις:

- $k > n$, το μήκος του κλειδιού είναι μεγαλύτερο από το μήκος της σύνοψης. Τότε για ένα ζευγάρι μηνύματος και σύνοψης, m_1, $h_{\boldsymbol{k}}(m_1)$, ο αντίπαλος θα πρέπει να ανακαλύψει το κλειδί $\boldsymbol{k'} \in \boldsymbol{K}$ για το οποίο $h_{\boldsymbol{k'}}(m) = h_{\boldsymbol{k}}(m)$. Αυτή όμως η ισότητα δεν εγγυάται ότι $\boldsymbol{k'} = \boldsymbol{k}$. Επειδή υπάρχουν περισσότερα κλειδιά από ότι συνόψεις, αναγκαστικά ορισμένα (διαφορετικά) κλειδιά θα αντιστοιχίζουν ένα μήνυμα στην ίδια σωστή σύνοψη. Μάλιστα ο αναμενόμενος αριθμός κλειδιών που θα παράγουν τη σωστή σύνοψη θα είναι ίσος με $2^k/2^n = 2^{k-n}$. Επομένως το ζητούμενο κλειδί βρίσκεται ανάμεσα στα 2^{k-n} κλειδιά που έχουν ξεχωρίσει. Για να μειωθεί το σύνολο αυτό, ο αντίπαλος θα πρέπει να επαναλάβει τη διαδικασία εξαντλητικής αναζήτησης με διαφορετικό ζευγάρι μηνύματος και σύνοψης m_2, $h_{\boldsymbol{k}}(m_2)$. Ο αναμενόμενος αριθμός σωστών κλειδιών σε αυτόν το δεύτερο γύρο θα είναι ίσος με $2^{k-n}/2^n = 2^{k-2n}$. Από την ποσότητα αυτή μπορούμε να συμπεράνουμε ότι οι αναμενόμενοι γύροι που πρέπει να πραγματοποιήσει ο αντίπαλος για να καταλήξει σε ένα μόνο κλειδί είναι k/n.
- $k \leq n$, το μήκος του κλειδιού είναι μικρότερο ή ίσο από το μήκος της σύνοψης. Στην περίπτωση αυτή, η πιθανότητα να αντιστοιχεί ένα μόνο κλειδί σε ένα ζευγάρι μηνύματος και σύνοψης, είναι μεγάλη. Αυτό είναι το οπτιμιστικό σενάριο για τον αντίπαλο, οπότε οι αναμενόμενες προσπάθειες που απαιτούνται για την ανακάλυψη του κλειδιού είναι 2^{k-1}. Το πεσιμιστικό σενάριο είναι ότι περισσότερο από ένα κλειδιά μπορούν να παράγουν το δεδομένο ζευγάρι μηνύματος και σύνοψης, οπότε η προσπάθεια ακολουθεί την πρώτη περίπτωση.

Συμπεραίνουμε λοιπόν ότι στην καλύτερη περίπτωση ο αντίπαλος μπορεί να βρει το κλειδί που χρησιμοποιείται στη MAC με 2^{k-1} προσπάθειες. Επομένως η προσπάθεια ανάκτησης του κλειδιού σε μια συνάρτηση MAC είναι ίση ή μεγαλύτερη από την προσπάθεια αποκρυπτογράφησης μηνύματος που προέρχεται από κρυπτοσύστημα με κλειδί ίδιου μήκους.

3.4. Διάκριση ψηφιακών υπογραφών.

Δύο είναι οι γενικές κατηγορίες ψηφιακών υπογραφών:
1) Οι ψηφιακές υπογραφές με παράρτημα (digital signature schemes with appendix),
που απαιτούν το αρχικό μήνυμα σαν είσοδο στον αλγόριθμο επαλήθευσης και

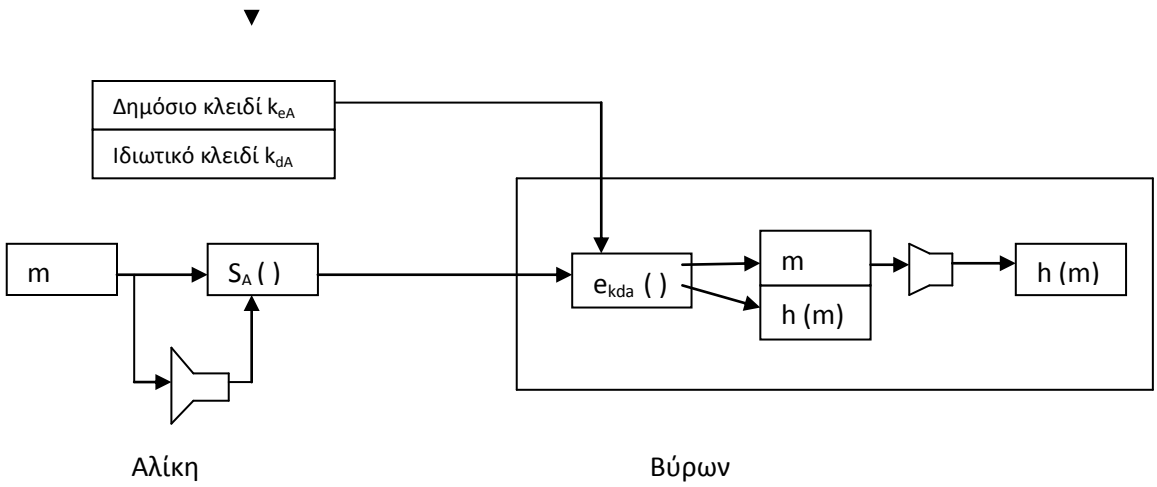
χρησιμοποιούν την συνάρτηση κατακερματισμού. Παραδείγματα ψηφιακών υπογραφών με παράρτημα: DSA, DSS, ELGamal, Schnorr.
2) Σχήματα ψηφιακών υπογραφών με ικανότητα ανάκτησης μηνύματος, τα οποία δεν απαιτούν το αρχικό μήνυμα σαν είσοδο στον αλγόριθμο επαλήθευσης. Εν αντιθέσει το αρχικό μήνυμα μπορεί να αναπαραχθεί από την ίδια την ψηφιακή υπογραφή. Παραδείγματα ψηφιακών υπογραφών με δυνατότητα ανάκτησης του μηνύματος: RSA, Rabin,Nyberg-Rueppel.
Οι κλάσεις αυτές μπορούν επιπλέον να διαιρεθούν με βάση αν το $|R| = 1$ ή όχι.
Ορισμός: Μια ψηφιακή υπογραφή (είτε με παράρτημα είτε με ανάκτηση μηνύματος) ονομάζεται τυχαιοποιημένη ψηφιακή υπογραφή αν $|R| = 1$, αλλιώς λέγεται ντετερμινιστική.

3.4.1. Ψηφιακές υπογραφές με αυτοανάκτηση.

Σε ένα σύστημα ψηφιακής υπογραφής με αυτοανάκτηση, η περίσσεια της γλώσσας του μηνύματος θα πρέπει να υπάρχει σε τέτοιο βαθμό, ώστε να είναι δυνατή η επαλήθευση της υπογραφής. Συνεπώς, όταν η γλώσσα του μηνύματος δεν έχει περίσσεια (ή όταν αυτή είναι μικρή), θα πρέπει με κάποιον τρόπο να προσθέσουμε περίσσεια. Αυτό θα έχει ως αποτέλεσμα την αύξηση του μεγέθους του μηνύματος. Η κωδικοποίηση των μηνυμάτων στα δίκτυα υπολογιστών συνήθως είναι τέτοια που η περίσσεια είναι ελάχιστη. Μάλιστα, οι αλγόριθμοι συμπίεσης δεδομένων αποβλέπουν στην εξάλειψη της περίσσειας έτσι ώστε το μήνυμα να καταλαμβάνει το μικρότερο δυνατό χώρο για την αποτελεσματική αποθήκευση και μεταφορά. Έτσι από τη μια ένας μηχανικός υπολογιστών επιδιώκει να μειώσει την περίσσεια, ενώ από την άλλη ένας κρυπτογράφος επιθυμεί να εισάγει περίσσεια. Συνεπώς η ισορροπία στην σύγκρουση των ενδιαφερόντων βρίσκεται στο να υπάρχει τόση περίσσεια ώστε να είναι ασφαλές το σύστημα ψηφιακών υπογραφών, όσον αφορά την αξιοπιστία της διαδικασίας επαλήθευσης της υπογραφής.

Οι υποψήφιες κρυπτογραφικές συναρτήσεις που χρησιμοποιούνται για να εισάγουν περίσσεια στο σύστημα, δεν είναι άλλες από τις κρυπτογραφικές μονόδρομες hash. Οι ιδιότητες των κρυπτογραφικών μονόδρομων hash τις καθιστούν ιδανικές για να εισάγουν περίσσεια στο μήνυμα. Η περίσσεια εξαρτάται από όλα τα σύμβολα του μηνύματος, έχει σταθερό μέγεθος και είναι ανθεκτική σε συγκρούσεις .

Στο Σχήμα 3.4 παρουσιάζεται ένα σύστημα ψηφιακής υπογραφής με αυτοανάκτηση.



Σχήμα 3.4. : Σύστημα ψηφιακής υπογραφής με αυτοανάκτηση

Η Αλίκη υπογράφει το μήνυμα m ως εξής. Αρχικά δημιουργεί μια σύνοψη του μηνύματος με τη βοήθεια της κρυπτογραφικής μονόδρομης hash h( ). Στη συνέχεια προσθέτει στο τέλος του μηνύματος m τη σύνοψη h(m) και τροφοδοτεί το συνδυασμό m||h(m) στη συνάρτηση υπογραφής S_A( ). Η συνάρτηση υπογραφής αποτελείται από την κρυπτογραφική πράξη της αποκρυπτογράφησης με το ιδιωτικό κλειδί της Αλίκης k_{dA}. Εδώ η αποκρυπτογράφηση είναι στην πραγματικότητα πράξη κρυπτογράφησης, αλλά για λόγους τυποποίησης δεχόμαστε ότι η κρυπτογραφική πράξη με το ιδιωτικό κλειδί θεωρείται αποκρυπτογράφηση και μπορεί να γίνει μόνον από τον κάτοχο του ιδιωτικού κλειδιού, σε αντίθεση με την πράξη κρυπτογράφησης που μπορεί να γίνει από όλους που έχουν στην κατοχή τους το δημόσιο κλειδί.
Ο Βύρων, μόλις λάβει την υπογραφή, την κρυπτογραφεί εφαρμόζοντας το δημόσιο κλειδί της Αλίκης προκειμένου να ανακτήσει τα δύο τμήματα, το μήνυμα και τη σύνοψη. Στη συνέχεια, υπολογίζει τη σύνοψη του πρώτου τμήματος που αντιστοιχεί στο αρχικό μήνυμα και ελέγχει αν αυτή είναι ίση με τη σύνοψη που έστειλε η Αλίκη. Αν οι δύο συνόψεις είναι ίσες, τότε η υπογραφή είναι έγκυρη.

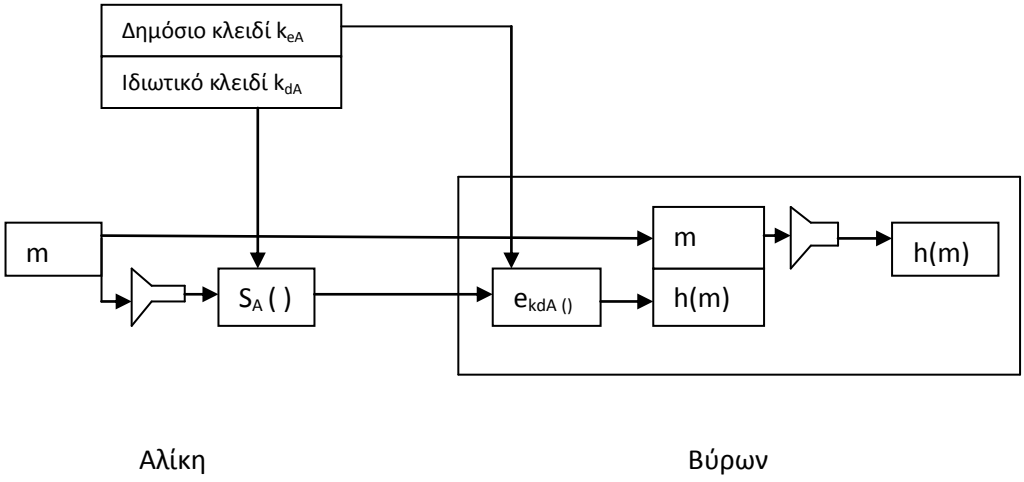
3.4.2. Ασφάλεια συστήματος ψηφιακής υπογραφής με αυτοανάκτηση.

Η επιλογή της κρυπτογραφικής μονόδρομης hash είναι κρίσιμη όσον αφορά την ασφάλεια του συστήματος ψηφιακής υπογραφής με αυτοανάκτηση. Επειδή το μήνυμα είναι μέρος της υπογραφής, η μονόδρομη hash θα πρέπει να έχει ασθενή αντίσταση σε συγκρούσεις.
Το σύστημα είναι ασφαλές σε επίθεση πλαστογραφίας, ακόμα και αν το ασύμμετρο κρυπτοσύστημα που χρησιμοποιείται διατηρεί την ιδιότητα της αντιμετάθεσης. Σε μια κρυπτογραφικά μονόδρομη hash η οποία έχει ασθενή αντίσταση σε συγκρούσεις, δεν ισχύει η αντιμεταθετικότητα, επομένως η σύνοψη

ενός πλαστού μηνύματος το οποίο προκύπτει από την αντιμετάθεση των τμημάτων του αρχικού μηνύματος θα είναι διαφορετική από τη σύνοψη του αρχικού μηνύματος.

3.4.3. Ψηφιακές υπογραφές με παράρτημα.

Το παραπάνω σύστημα ψηφιακής υπογραφής με αυτοανάκτηση έχει το μειονέκτημα ότι το μέγεθος της ψηφιακής υπογραφής δεν είναι σταθερό και εξαρτάται από το μέγεθος του αρχικού μηνύματος. Αυτό έχει ως αποτέλεσμα την αύξηση της ανάγκης για επεξεργασία του μηνύματος. Είναι κοινή πρακτική οι πράξεις στις οποίες εμπλέκεται ασύμμετρη κρυπτογραφία, να είναι όσο το δυνατόν περιορισμένες. Η ασύμμετρη κρυπτογραφία είναι αρκετές τάξεις μεγέθους πιο αργή από τη συμμετρική κρυπτογραφία. Η κρυπτογράφηση (ή αποκρυπτογράφηση) ενός μηνύματος με ασύμμετρη κρυπτογραφία θα πρέπει συστηματικά να αποφεύγεται για καθαρά πρακτικούς λόγους.
Με βάση τα παραπάνω, ορίζεται το σύστημα ψηφιακής υπογραφής με παράρτημα, όπως φαίνεται στο σχήμα.



Σχήμα 3.5. : Σύστημα ψηφιακής υπογραφής με παράρτημα.

Επειδή ο στόχος της ψηφιακής υπογραφής είναι η αυθεντικοποίηση και όχι η εμπιστευτικότητα, η ασύμμετρη κρυπτογραφία είναι προτιμότερο να αποδεσμευτεί από το μήνυμα. Έτσι, η αποκρυπτογράφηση κατά τη διαδικασία της δημιουργίας της ψηφιακής υπογραφής περιορίζεται στη σύνοψη του μηνύματος. Ο ξεχωριστός χειρισμός της σύνοψης από το μήνυμα έχει σαν αποτέλεσμα να στέλνονται δύο ανεξάρτητα τμήματα, το αρχικό μήνυμα το οποίο δεν έχει υποστεί κανέναν μετασχηματισμό, και η ψηφιακή υπογραφή που

συνήθως ακολουθεί το μήνυμα. Ο όρος «παράρτημα» οφείλεται στην προσκόλληση της ψηφιακής υπογραφής στο τέλος του μηνύματος, ως ανεξάρτητο αντικείμενο.

3.4.4.Ασφάλεια συστήματος ψηφιακής υπογραφής με παράρτημα.

Η ασφάλεια του συστήματος ψηφιακής υπογραφής με παράρτημα είναι συγκρίσιμη με αυτήν του συστήματος ψηφιακής υπογραφής με αυτοανάκτηση. Επειδή όμως ο αντίπαλος έχει πρόσβαση σε περισσότερα μηνύματα, η κρυπτογραφική μονόδρομη hash θα πρέπει να παρουσιάζει ισχυρή αντίσταση σε συγκρούσεις. Στην περίπτωση του συστήματος της ψηφιακής υπογραφής με αυτοανάκτηση, ο αριθμός των μηνυμάτων που μπορεί να κατασκευάσει ο αντίπαλος καθορίζεται από το συνδυασμό των τμημάτων του αρχικού μηνύματος. Αντίθετα στην περίπτωση του συστήματος ψηφιακής υπογραφής με παράρτημα, ο αντίπαλος έχει ολόκληρο το σύνολο των μηνυμάτων στη διάθεσή του.

Στην περίπτωση που απαιτείται εμπιστευτικότητα, το μήνυμα m κρυπτογραφείται είτε με το ιδιωτικό κλειδί του Βύρωνα, είτε με συμμετρικό κλειδί συνόδου. Αν η επικοινωνία μεταξύ της Αλίκης και του Βύρωνα είναι συχνή ή περιλαμβάνει μεγάλα μηνύματα, τότε προτιμάται η χρήση συμμετρικής κρυπτογραφίας για να κρυπτογραφηθεί το μήνυμα, για λόγους ταχύτητας.
Υπάρχουν δύο συνδυασμοί για την κρυπτογράφηση και την εφαρμογή ψηφιακής υπογραφής:

- κρυπτογράφηση του μηνύματος με το συμμετρικό κλειδί συνόδου και στη συνέχεια υπογραφή του κρυπτοκειμένου,
- υπογραφή του (απλού κειμένου) μηνύματος και στη συνέχεια κρυπτογράφηση του μηνύματος.

Από τις δύο εναλλακτικές, η πρώτη δεν προτιμάται για δύο βασικούς λόγους. Η ψηφιακή υπογραφή του κρυπτοκειμένου εισάγει και τη μεταβλητή του μυστικού κλειδιού συνόδου. Έτσι, ο Βύρων θα μπορούσε να αποκρυπτογραφήσει το κρυπτοκείμενο με κάποιο άλλο κλειδί και να ισχυρισθεί ότι το απλό κείμενο που προκύπτει είναι το μήνυμα το οποίο έστειλε η Αλίκη. Με άλλα λόγια, η ψηφιακή υπογραφή της Αλίκης είναι έγκυρη για 2^n μηνύματα, όπου n το μέγεθος του μυστικού κλειδιού συνόδου σε bits. Έτσι, ο Βύρων έχει τη δυνατότητα να πραγματοποιήσει **επιλεκτική πλαστογραφία**. Το πρόβλημα μπορεί να λυθεί αν η Αλίκη συμπεριλάβει στο μήνυμα και το μυστικό κλειδί και το υπογράψει. Όμως σε έναν τέτοιο διακανονισμό, ο κίνδυνος αποκάλυψης του κλειδιού σε τρίτους είναι μεγάλος και μπορεί να δημιουργήσει προβλήματα ασφάλειας, αν το κλειδί

αυτό χρησιμοποιείται για περαιτέρω επικοινωνία μεταξύ της Αλίκης και του Βύρωνα.
Ο δεύτερος λόγος είναι καθαρά δεοντολογικός. Η ενέργεια της υπογραφής υποδεικνύει γνώση του περιεχομένου που υπογράφεται. Η ψηφιακή υπογραφή σε κάποιο κρυπτοκείμενο δε στηρίζει την έννοια της υπογραφής, αφού η Αλίκη δε γνωρίζει άμεσα τι υπογράφει.

4.Συστήματα ψηφιακών υπογραφών.

4.1. Ψηφιακές υπογραφές με το κρυπτοσύστημα RSA.

Το κρυπτοσύστημα RSA μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός συστήματος ψηφιακών υπογραφών. Το σύστημα ψηφιακών υπογραφών RSA απαιτεί ότι όλες οι οντότητες έχουν στην κατοχή τους αντίστοιχα ζεύγη δημόσιου και ιδιωτικού κλειδιού.
Έστω p και q δύο πρώτοι αριθμοί και n = pq. Το σύστημα ψηφιακών υπογραφών RSA ορίζεται με

$M = S = \mathbf{Z}_n$, πράξη υπογραφής:

$$SA(m) = m^{KdA} \bmod n$$

και πράξη επαλήθευσης

$$VA(s) = S^{keA} \bmod n$$

όπου $k_{eA}k_{dA} \equiv 1 \pmod{\varphi(n)}$, με k_{eA} το δημόσιο κλειδί και k_{dA} το ιδιωτικό κλειδί της οντότητας Α.

Επειδή η ψηφιακή υπογραφή αποτελείται από το μήνυμα αποκρυπτογραφημένο με το ιδιωτικό κλειδί του αποστολέα, το παραπάνω σύστημα ψηφιακών υπογραφών RSA μπορεί να λειτουργήσει ως σύστημα ψηφιακής υπογραφής με αυτοανάκτηση, αν σταλεί μόνον η ψηφιακή υπογραφή χωρίς το μήνυμα.

Στη συνέχεια ακολουθεί ένα παράδειγμα συστήματος ψηφιακής υπογραφής RSA. Έστω το κρυπτοσύστημα RSA με τις εξής παραμέτρους:

$p = 29, q = 17, n = 29 \cdot 17 = 493, k_{dA} = 319, k_{eA} = 191.$

Αρχικά επαληθεύουμε την ορθότητα του ζεύγους των κλειδιών:

$k_{dA} \cdot k_{eA} = 319 \cdot 191 = 60929 \equiv 1 \pmod{448}$.

Το προς υπογραφή μήνυμα είναι το: [τέχνη], το οποίο αντιστοιχίζεται στο αριθμητικό ισοδύναμο: [28 14 31 22 16]. Για το παράδειγμά μας, επιλέξαμε την αντιστοίχιση Α10, Β11, …, ώστε όλα τα γράμματα να έχουν ίδιο μέγεθος, ίσο με

δύο ψηφία. Στη συνέχεια ομαδοποιούμε τα ψηφία του μηνύματος, ώστε να σχηματίζουν αριθμούς μικρότερους του δημόσιου modulus, 493: (281, 431,221, 6). Εφαρμόζοντας τέσσερις φορές το ιδιωτικό κλειδί, παίρνουμε την ψηφιακή υπογραφή:

$281^{319} \equiv 36 \bmod (493)$
$431^{319} \equiv 343 \bmod (493)$
$221^{319} \equiv 425 \bmod (493)$
$6^{319} \equiv 241 \bmod (493)$

και η υπογραφή που προκύπτει είναι η τετράδα (36, 343, 425, 241)

4.1.1.Ασφάλεια συστήματος ψηφιακών υπογραφών RSA.

Το κρυπτοσύστημα RSA διατηρεί την αντιμεταθετική ιδιότητα που σημαίνει ότι ένας αντίπαλος μπορεί να εκτελέσει ενεργητική επίθεση και να αναδιατάξει το μήνυμα και την υπογραφή του κατά τη μεταφορά τους από τον αποστολέα στον παραλήπτη. Οι αναδιατάξεις πραγματοποιούνται σε τμήματα των $\log_2(n)$ bits, όπου n το δημόσιο modulus του αποστολέα. Επίσης, ο αντίπαλος έχει τη δυνατότητα να επαναλάβει ορισμένα τμήματα του μηνύματος, σε θέσεις της επιλογής του, κατοπτρίζοντας τις επαναλήψεις και στα αντίστοιχα τμήματα της ψηφιακής υπογραφής.

Μια λύση είναι να κρυπτογραφηθεί η ψηφιακή υπογραφή με το δημόσιο κλειδί του παραλήπτη, εκμεταλλευόμενοι το γεγονός ότι όλα τα επικοινωνούντα μέλη που συμμετέχουν στην υποδομή του RSA θα έχουν δημόσια και ιδιωτικά κλειδιά. Έστω ότι η Αλίκη επιθυμεί να στείλει εμπιστευτικά στον Βύρωνα ένα μήνυμα m το οποίο να είναι συγχρόνως υπογεγραμμένο από την ίδια. Τα στοιχεία τα οποία απαιτούνται για τις κρυπτογραφικές πράξεις είναι οι παράμετροι RSA (k_{eA}, k_{dA}, n_A) της Αλίκης, καθώς και οι παράμετροι RSA (k_{eB}, k_{dB}, n_B) του Βύρωνα. Αρχικά η Αλίκη υπογράφει ψηφιακά το μήνυμα m:

Στη συνέχεια κρυπτογραφεί την υπογραφή με το δημόσιο κλειδί του Βύρωνα:

Έτσι, ο αντίπαλος θα έχει πρόσβαση μόνο στο μήνυμα και δε θα έχει τη δυνατότητα να πραγματοποιήσει τις αλλαγές του μηνύματος στην ψηφιακή υπογραφή.

Ωστόσο, η εξάρτηση του μεγέθους των δεδομένων που κρυπτογραφούνται από τις RSA παραμέτρους των μελών, έχει επιπτώσεις στην αντιστρεψιμότητα της πράξης της κρυπτογράφησης. Πιο συγκεκριμένα, αν τα modulus των δύο μελών είναι διαφορετικά με $n_A > n_B$, τότε υπάρχει πιθανότητα η κρυπτογραφημένη

υπογραφή να μην μπορεί να αποκρυπτογραφηθεί σωστά από τον Βύρωνα. Για την αποφυγή αυτού του ενδεχόμενου υπάρχουν οι εξής τακτικές:

- να προηγηθεί η κρυπτογράφηση του μηνύματος με το με το δημόσιο κλειδί του Βύρωνα της ψηφιακής υπογραφής, στην περίπτωση που $n_A > n_B$. Η τακτική αυτή δεν συστήνεται για τους λόγους που αναφέραμε στην προηγούμενη ενότητα
- να τμηματοποιηθεί η υπογραφή προκειμένου να είναι συμβατή με το n_B. Η τακτική αυτή δημιουργεί προβλήματα υλοποίησης, αυξάνοντας την πολυπλοκότητα και τις απαιτήσεις επεξεργασίας του συστήματος ψηφιακών υπογραφών.
- το κάθε μέλος να έχει δύο διαφορετικά ζεύγη κλειδιών, το ένα για ψηφιακή υπογραφή και το άλλο για κρυπτογράφηση, έτσι ώστε το modulus για την κρυπτογράφηση να είναι μεγαλύτερο από όλα τα moduli που χρησιμοποιούνται στις ψηφιακές υπογραφές.
- να μειωθεί η πιθανότητα μη αντιστρεψιμότητας της κρυπτογράφησης σε πρακτικώς ανεκτά επίπεδα. Έχει δειχθεί ότι αυτό μπορεί να γίνει αν η δυαδική αναπαράσταση του n έχει τη μορφή:
  n = (100...01)2

δηλαδή το σημαντικότερο bit θα πρέπει να είναι άσσος και στη συνέχεια να ακολουθήσουν k μηδενικά, όπου k αριθμός επιλογής μας. Επειδή το n είναι γινόμενο δύο αριθμών, υπάρχει τρόπος επιλογής των p και q έτσι ώστε το γινόμενο που προκύπτει να έχει την επιθυμητή μορφή. Έτσι η ψηφιακή υπογραφή θα είναι μικρότερη του n και θα έχει **0** στη θέση του σημαντικότερου bit.

Στην περίπτωση του συστήματος ψηφιακής υπογραφής RSA με παράρτημα, το κατώτατο μέγεθος της κρυπτογραφικής μονόδρομης hash θα πρέπει να είναι ίσο με 128 bit. Στη βιβλιογραφία το μέγεθος αυτό προτείνεται για τη μονόδρομη MD5, η οποία έχει αναλυθεί και θεωρείται ασφαλής. Στην περίπτωση που χρησιμοποιηθεί hash άλλη από την MD5, προτείνεται η hash να είναι ανθεκτική σε συγκρούσεις, με ελάχιστο μέγεθος σύνοψης ίσο με 160 bit.
Τέλος, όσον αφορά το μέγεθος των RSA παραμέτρων, αν το κρυπτοσύστημα RSA χρησιμοποιείται μόνο για ψηφιακές υπογραφές και όχι για εμπιστευτικότητα, τότε ο δημόσιος εκθέτης k_e μπορεί να έχει οποιαδήποτε τιμή, καθώς δεν έχουν αναφερθεί αδυναμίες για μικρές τιμές του k_e. Ο αριθμός n θα πρέπει να έχει μέγεθος το λιγότερο ίσο με 1024 bits, ενώ σε περιπτώσεις όπου απαιτείται μεγάλη διάρκεια ζωής των κλειδιών, προτείνεται το μέγεθος των 2048 bits.

4.2.Το σύστημα ψηφιακών υπογραφών Fiege-Fiat-Shamir.

Η υπεροχή του συστήματος ψηφιακών υπογραφών Fiege-Fiat-Shamir (FFS) έναντι των ψηφιακών υπογραφών με RSA είναι ο κατά πολύ μικρότερος χρόνος υπολογισμών. Το σύστημα ψηφιακών υπογραφών FFS απαιτεί περίπου το 4 τοις εκατό των modular πολλαπλασιασμών που απαιτεί το σύστημα RSA.

Το σύστημα περιλαμβάνει μια διαδικασία δημιουργίας των κλειδιών, ένα πρωτόκολλο δημιουργίας ψηφιακής υπογραφής και ένα πρωτόκολλο επαλήθευσης.

Θεωρούμε ότι η Αλίκη επιθυμεί να στείλει ένα υπογεγραμμένο μήνυμα m στον Βύρωνα. Η διαδικασία δημιουργίας των κλειδιών έχει ως εξής. Η Αλίκη επιλέγει δύο πρώτους αριθμούς p, q και υπολογίζει το γινόμενό τους n = pq, όπως και στο κρυπτοσύστημα RSA. Στη συνέχεια, επιλέγει μια ακολουθία k ακεραίων:

$Si \in Z^*n$,για $1 <= i <= k$

Το διάνυσμα $(s_1, s_2, \ldots, s_k)$ αποτελεί το ιδιωτικό κλειδί της Αλίκης. Από την ακολουθία δημιουργεί το δημόσιο κλειδί το οποίο είναι το διάνυσμα $(v_1, v_2, \ldots, v_k)$, όπου:

$Vi=Si^{-2} \pmod n$,για $1 <= i <= k$

Η δημιουργία της ψηφιακής υπογραφής υλοποιείται με το ακόλουθο πρωτόκολλο:

Αλίκη:

1. Επιλογή τυχαίου ακεραίου *r*, όπου $0 < r < n$.
2. Υπολογισμός του $u \equiv r^2 \pmod n$.
3. Υπολογισμός της σύνοψης $h(m||u) = (e1e2\ldots\ldots ek)2 = e$
4. Υπολογισμός του . $s \equiv r \prod_{i=1}^{k} si^{ei} \pmod n$. Η ψηφιακή υπογραφή είναι το (e ,s).

Αλίκη → Βύρων: m||(e, s).

Ο Βύρων μπορεί να πραγματοποιήσει επαλήθευση της ψηφιακής υπογραφής εφόσον γνωρίζει το δημόσιο κλειδί της Αλίκης, εκτελώντας τον ακόλουθο πρωτόκολλο:

<u>Βύρων:</u>

1. Υπολογισμός του . $w \equiv s^2 \cdot \prod_{i=1}^{k} vi^{ei} \pmod n$
2. Υπολογισμός της σύνοψης . $e' = h(m||w)$

3. Η υπογραφή θεωρείται έγκυρη αν και μόνο αν $e = e'$

Αν η υπογραφή είναι έγκυρη, τότε οι δύο συνόψεις θα πρέπει να είναι ίσες, που σημαίνει ότι u = w. Όντως, μπορούμε να επαληθεύσουμε ότι:

$$w \equiv s^2 \cdot \prod_{i=1}^{k} vi^{ei} \{ r^2 \cdot \prod_{i=1}^{k} si^{2ei} \} \prod_{i=1}^{k} vi^{ei} = r^2 \cdot \prod_{i=1}^{k} (si^2 \cdot vi)^{ei} \equiv r^2 \cdot \prod_{i=1}^{k} 1^{ei} \equiv r^2 \equiv u$$

4.2.1. Ασφάλεια του συστήματος ψηφιακών υπογραφών FFS

Η ασφάλεια του συστήματος ψηφιακών υπογραφών FFS βασίζεται στη δυσκολία υπολογισμού της τετραγωνικής ρίζας ενός ακεραίου, modulo n. Ο αντίπαλος (που μπορεί να είναι και ο Βύρων) γνωρίζει το s_i^{-2} και για να επιτύχει σε επίθεση πλαστογραφίας καλείται να ανακαλύψει το s_i.

Επειδή η Αλίκη δεν απαιτείται να γνωρίζει τους παράγοντες του n προκειμένου να δημιουργήσει το ιδιωτικό και το δημόσιο κλειδί συνιστάται, όπου είναι δυνατόν, οι παράγοντες του n να είναι κρυφοί από όλα τα μέλη που συμμετέχουν στο σύστημα των ψηφιακών υπογραφών FFS και να αναλάβει μια έμπιστη οντότητα να κατασκευάσει και να διαθέσει το n στα μέλη.

4.3. Το σύστημα ψηφιακών υπογραφών ElGamal

Η ασφάλεια του συστήματος των ψηφιακών υπογραφών ElGamal βασίζεται στη δυσκολία του υπολογισμού του διακριτού λογάριθμου από τον αντίπαλο. Για την υλοποίηση του συστήματος ψηφιακών υπογραφών ElGamal απαιτείται κρυπτογραφική μονόδρομη hash, της οποίας η σύνοψη είναι στοιχείο του συνόλου $\mathbf{Z}_p^*$, όπου p πρώτος αριθμός.

Η υποδομή ενός συστήματος ψηφιακών υπογραφών ElGamal απαιτεί την ακόλουθη διαδικασία δημιουργίας ζεύγους κλειδιών από τα μέλη. Αρχικά επιλέγεται ένας μεγάλος πρώτος αριθμός p και ένας ακέραιος a ο οποίος είναι γεννήτορας του συνόλου $\mathbf{Z}_p^*$. Στη συνέχεια επιλέγεται ένας ακέραιος b τέτοιος ώστε $0 < b < p-1$, και υπολογίζεται το:

$$y = a^b \pmod p .$$

Το δημόσιο κλειδί αποτελείται από τους τρεις ακέραιους (p, a, y) ενώ το ιδιωτικό κλειδί είναι ο εκθέτης b. Η παραπάνω διαδικασία εκτελείται από κάθε μέλος.

Κατά τη διαδικασία υπογραφής, εκτελείται το ακόλουθο πρωτόκολλο:

1. Επιλογή μυστικού ακεραίου k, με $0 < k < p–1$, και $\gcd(k, p–1) = 1$.
2. Υπολογισμός του $r \equiv a^{k} \pmod p$.
3. Υπολογισμός του $k^{-1} \bmod p$.
4. Υπολογισμός του $s \equiv k^{-1} (h(m) – br) \pmod{p–1}$.
5. Η υπογραφή για το μήνυμα m είναι το ζεύγος (r, s), το οποίο αποστέλλεται μαζί με το μήνυμα στον παραλήπτη.

Η διαδικασία επαλήθευσης πραγματοποιείται με το ακόλουθο πρωτόκολλο:

1. Έλεγχος ότι $0 < r < p–1$. Στην περίπτωση που το r δε βρίσκεται μεταξύ των ενδεδειγμένων ορίων, απορρίπτεται η ψηφιακή υπογραφή.
2. Υπολογισμός του $v \equiv y^{r} r^{s} \pmod p$.
3. Υπολογισμός της σύνοψης h(m) και υπολογισμός του $v' \equiv a^{h(m)} \pmod p$.
4. Η υπογραφή θεωρείται έγκυρη αν και μόνο αν $v = v'$.

Μπορούμε να επαληθεύσουμε την εγκυρότητα της υπογραφής με την ισοδυναμία του τελευταίου βήματος του πρωτοκόλλου επαλήθευσης ως εξής:

$S \equiv k^{-1}(h(m) – br) \pmod{p-1} \Rightarrow$

$ks \equiv h(m) – br \pmod{p-1} \Rightarrow$

$h(m) \equiv ks+br \pmod{p-1} \Rightarrow$

$a^{h(m)} \equiv a^{ks+br} \pmod p \Rightarrow$

$a^{h(m)} \equiv (a^{b})^{r} (a^{k})^{s} \pmod p \Rightarrow$

$a^{h(m)} \equiv y^{r} r^{s} \pmod p$

ή ισοδύναμα $v' = v$.

4.3.1.Ασφάλεια του συστήματος ψηφιακών υπογραφών ElGamal

Όπως αναφέραμε στην προηγούμενη ενότητα, η ασφάλεια του συστήματος ψηφιακών υπογραφών ElGamal βασίζεται στη δυσκολία υπολογισμού του διακριτού λογάριθμου. Ο αντίπαλος έχει στην κατοχή του το δημόσιο κλειδί (p, a, y) του υπογεγραμμένου και καλείται να ανακαλύψει το ιδιωτικό κλειδί b, το οποίο ικανοποιεί τη σχέση:

$$y \equiv a^{b} \pmod p .$$

Αν θεωρήσουμε ότι το πρόβλημα του διακριτού λογάριθμου είναι υπολογιστικά αδύνατο, τότε αν ο αντίπαλος επιλέξει στην τύχη έναν ακέραιο για υποψήφιο

ιδιωτικό κλειδί, η πιθανότητα να επιλέξει το σωστό κλειδί είναι ίση με 1/(p–1), εφόσον οι επιτρεπτές τιμές του ιδιωτικού κλειδιού βρίσκονται στο διάστημα 0 < b < p–1. Επομένως, το p θα πρέπει να είναι αρκετά μεγάλο ώστε η πιθανότητα εύρεσης του ιδιωτικού κλειδιού να είναι μικρή.

Ένα άλλο σημείο το οποίο θέτει σε κίνδυνο το σύστημα δίνοντας πλεονέκτημα για επιτυχή πλαστογραφία, είναι η επιλογή του τυχαίου ακέραιου k, κατά τη διαδικασία δημιουργίας της ψηφιακής υπογραφής. Πιο συγκεκριμένα, ο υπογεγραμμένος θα πρέπει να διατηρεί ιστορικό όλων των τυχαίων αριθμών που έχει επιλέξει, ώστε σε κάθε υπογραφή να χρησιμοποιείται διαφορετικός ακέραιος k.

ΠΑΡΑΔΕΙΓΜΑ – Επίθεση πλαστογραφίας λόγω κοινού τυχαίου ακεραίου. Έστω ότι η Αλίκη έχει υπογράψει δύο μηνύματα m_1 και m_2, χρησιμοποιώντας τον ίδιο τυχαίο ακέραιο k. Τότε για τις δύο υπογραφές (r_1, s_1) και (r_2, s_2), θα είναι $r_1 = r_2 = r$ ενώ για τα s_1 και s_2 θα είναι:

$$s_1 \equiv k^{-1}(h(m_1) – br) \pmod{p–1} \text{ και}$$

$$s_2 \equiv k^{-1}(h(m_2) – br) \pmod{p–1}$$

Αφαιρώντας τις δύο σχέσεις μεταξύ τους προκύπτει:

$$s_1 – s_2 \equiv k^{-1}((h(m_1) – br) – (h(m_2) – br) \pmod{p–1}$$

ή ισοδύναμα:

$$(s_1 – s_2)k \equiv h(m_1) – h(m_2) \pmod{p–1}$$

Αν

$$s_1 – s_2 \text{ T } 0 \pmod{p–1},$$

τότε μπορεί να υπολογιστεί ο k από την

$$k \equiv (s_1 – s_2)^{-1}(h(m_1) – h(m_2)) \pmod{p–1}.$$

Όλες οι μεταβλητές που βρίσκονται στο δεξί μέλος της παραπάνω ισοδυναμίας είναι γνωστές στον αντίπαλο. Η εύρεση του k αποκαλύπτει την ποσότητα $(h(m_1) – br)$ που υπάρχει στην s_1, από όπου ο αντίπαλος μπορεί να εξάγει το ιδιωτικό κλειδί b.

Τέλος, αν ο αρχικός έλεγχος στο πρωτόκολλο επαλήθευσης δεν πραγματοποιηθεί, τότε ο αντίπαλος είναι σε θέση να εκτελέσει πλαστογραφία δημιουργώντας ψηφιακή υπογραφή για οποιοδήποτε μήνυμα της επιλογής του. Αυτό οφείλεται στο γεγονός ότι στο σύνολο των ακεραίων ορίζονται άπειρες ισοδυναμίες, αν επιτρέψουμε το r να πάρει ανεξέλεγκτη τιμή, εκτός των ορίων 0 <

r < p–1. Αν και ο έλεγχος είναι φαινομενικά ένα ασήμαντο βήμα, η παράλειψη αυτού καθιστά όλο το σύστημα ευάλωτο σε επίθεση πλαστογραφίας.

ΠΑΡΑΔΕΙΓΜΑ – Επίθεση πλαστογραφίας λόγω παράλειψης του αρχικού ελέγχου 0 < r < p**–**1. Έστω ότι ο αντίπαλος έχει στην κατοχή του ένα μήνυμα m και την αντίστοιχη υπογραφή (r, s) στο μήνυμα αυτό. Αν h(m) T 0 (mod p**–**1), τότε ο αντίπαλος μπορεί να επιλέξει ένα δικό του μήνυμα m′ και στη συνέχεια να υπολογίσει την ποσότητα:

$$w \equiv h(m') h(m)^{-1} \pmod{p-1}$$

Στη συνέχεια ο αντίπαλος υπολογίζει την υπογραφή έτσι ώστε:

$$s' \equiv sw \pmod{p-1}$$

και r′ τέτοιο ώστε:

$$r' \equiv rw \pmod{p-1} \text{ και}$$

$$r' \equiv r \pmod{p}$$

Είναι φανερό ότι η πλαστογραφημένη υπογραφή (r′, s′) περνάει με επιτυχία το πρωτόκολλο επαλήθευσης, αν παραληφθεί το πρώτο βήμα.

4.4. Το Πρότυπο Ψηφιακής Υπογραφής (DSS)

Το Πρότυπο Ψηφιακής Υπογραφής (Digital Signature Standard, DSS), δημοσιεύθηκε από το Εθνικό Ινστιτούτο Τυποποίησης και Τεχνολογίας (NIST) το οποίο καθορίζει ένα σύστημα ψηφιακών υπογραφών, για γενική χρήση. Το DSS περιγράφει έναν αλγόριθμο ψηφιακής υπογραφής, τον DSA (Digital Signature Algorithm), οποίος βασίζεται σε ασύμμετρη κρυπτογραφία. Σε αντίθεση με τα συστήματα ψηφιακών υπογραφών που περιγράψαμε, ο DSA αναφέρεται αποκλειστικά σε σύστημα ψηφιακών υπογραφών και δεν μπορεί να χρησιμοποιηθεί ως κρυπτοσύστημα. Επίσης, το DSS προβλέπει τη χρήση της SHA-1 ως κρυπτογραφική μονόδρομη hash, η οποία συμμετέχει στη δημιουργία της ψηφιακής υπογραφής.

Ο DSA είναι μια τροποποίηση του συστήματος ψηφιακής υπογραφής ElGamal. Επομένως, η ασφάλειά του βασίζεται στο πρόβλημα του υπολογισμού του διακριτού λογάριθμου.

Όπως όλα τα συστήματα ψηφιακών υπογραφών που εξετάσαμε παραπάνω, έτσι και ο DSA αποτελείται από τον καθορισμό των ασύμμετρων παραμέτρων (των κλειδιών), το πρωτόκολλο ψηφιακής υπογραφής και το πρωτόκολλο επαλήθευσης της υπογραφής.

Κατά τη δημιουργία των κλειδιών, το κάθε μέλος θα πρέπει να εκτελέσει τα ακόλουθα βήματα. Αρχικά, επιλέγεται ένας πρώτος αριθμός q τέτοιος ώστε $2^{159} < q < 2^{160}$. Από τα όρια αυτά φαίνεται ότι το μέγεθος του αριθμού q θα είναι ίσο με 160 bits. Στη συνέχεια επιλέγεται πρώτος αριθμός p τέτοιος ώστε $2^{t-1} < p < 2^{t}$, με

$512 \leq t \leq 1024$, και ο t να είναι ακέραιο πολλαπλάσιο του 64. Επίσης ο q θα πρέπει να διαιρεί τον (p–1).

Με βάση τους πρώτους αριθμούς p και q, επιλέγεται γεννήτορας a μιας κυκλικής υποομάδας τάξης q της ομάδας $\mathbf{Z}_p^*$. Αυτό επιτυγχάνεται επιλέγοντας $g \in \mathbf{Z}_p^*$ τέτοιο ώστε:

$$g^{(p-1)/q} \bmod p > 1$$

και θέτουμε

$$a \equiv g^{(p-1)/q} \pmod p$$

Στη συνέχεια, επιλέγεται τυχαίος ακέραιος τέτοιος ώστε $0 < b < q$, και υπολογίζεται ο:

$$y \equiv a^b \pmod p .$$

Η τετράδα (p, q, a, y) αποτελεί το δημόσιο κλειδί, ενώ ο b αποτελεί το ιδιωτικό κλειδί.

Το πρωτόκολλο υπογραφής ενός μηνύματος m αποτελείται από τα ακόλουθα βήματα:

1. Επιλογή τυχαίου μυστικού ακέραιου k τέτοιου ώστε $0 < k < q$.
2. Υπολογισμός του $r \equiv (a^k \bmod p) \pmod q$.
3. Υπολογισμός του $k^{-1} \bmod q$.
4. Υπολογισμός του $s \equiv k^{-1}(h(m) + br) \pmod q$.

Η ψηφιακή υπογραφή του μηνύματος m είναι το ζεύγος (s, r). Κατά την επαλήθευση της ψηφιακής υπογραφής εκτελείται το ακόλουθο πρωτόκολλο:

1. Έλεγχος ότι $0<r,s<q$. Σε περίπτωση που κάποιο από τα r,s δεν είναι εντός των καθορισμένων ορίων, η υπογραφή απορρίπτεται.
2. Υπολογισμός του $w = s^{-1} \bmod q$.
3. Υπολογισμός των:
   $u_1 \equiv wh(m) \pmod q$
   $u_2 \equiv rw \pmod q$
4. Υπολογισμός του $r \equiv a^{u1} y^{u2} \pmod q$.
5. Η υπογραφή θεωρείται έγκυρη αν και μόνο αν $r = r'$.

Το παράδοξο της επαλήθευσης της υπογραφής του τελευταίου βήματος είναι ότι η ποσότητα r δεν εξαρτάται από το μήνυμα, οπότε δεν είναι ευθέως φανερό πως μπορεί να πραγματοποιηθεί η επαλήθευση χωρίς την άμεση συμβολή του μηνύματος που υπογράφηκε. Ωστόσο, μπορούμε να επαληθεύσουμε την εγκυρότητα της υπογραφής με την ισοδυναμία του τελευταίου βήματος του πρωτοκόλλου επαλήθευσης ως εξής:

$$S \equiv k^{-1}(h(m) + br) \pmod p \Rightarrow$$

$$ks \equiv h(m) + br \pmod p \Rightarrow$$

$$wks \equiv wh(m) + wbr \pmod p \Rightarrow$$

(ws) $k \equiv u_{1} + u_{2}b \pmod p \Rightarrow$

$k \equiv u_1+u_2b \pmod p \Rightarrow$

$(a^k \bmod p) \bmod q = (a^{u1} y^{u2} \bmod p) \bmod q$
ή ισοδύναμα r΄=r.

4.5.Άλλες κατηγορίες ψηφιακών υπογραφών.

4.5.1.Ψηφιακές υπογραφές μιας χρήσης.

Οι ψηφιακές υπογραφές μιας χρήσης είναι γνωστές εδώ και τουλάχιστον δύο δεκαετίες και έχουν μελετηθεί κυρίως για την θεωρητική τους αξία. Αυτά τα σχήματα υπογραφών
επιτρέπουν την υπογραφή ενός μόνο μηνύματος. Το πλεονέκτημα τους είναι ότι είναι σχετικά γρήγορες. Βέβαια, αυτά τα σχήματα τείνουν να είναι δυσκίνητα όταν είναι να υπογραφούν πολλά μηνύματα, γιατί τα επιπλέον δεδομένα απαιτούν υπογραφή και επαλήθευση τους για κάθε μήνυμα. Σε αντίθεση, με τα συνηθισμένα σχήματα ψηφιακής υπογραφής όπως το RSA, το ίδιο κλειδί μπορεί να χρησιμοποιηθεί για την υπογραφή πολλαπλών μηνυμάτων. Οι δημόσιες πληροφορίες που είναι αναγκαίες για την επαλήθευση υπογραφών μιας χρήσης αναφέρονται σαν παράμετροι επικύρωσης. Τα σχήματα υπογραφών μιας χρήσης βρίσκουν εφαρμογή σε έξυπνες κάρτες που δεν χρειάζονται υψηλή υπολογιστική πολυπλοκότητα.

4.5.2. Ψηφιακή υπογραφή μιας χρήσης Rabin.

Η ψηφιακή υπογραφή μιας χρήσης Rabin είναι ένα από τα πρώτα σχήματα αυτού του είδους. Στο σχήμα αυτό για να πραγματοποιηθεί η επαλήθευση χρειάζεται την συνεισφορά του υπογράφοντα και αυτού που θέλει να επαληθεύσει την υπογραφή. Όπως και κάθε σχήμα ψηφιακής υπογραφής αυτού του είδους επιτρέπει την υπογραφή ενός μόνο μηνύματος. Η διαφορά με άλλα σχήματα είναι ότι ο αλγόριθμος επαλήθευσης μπορεί να πραγματοποιηθεί μονάχα μία φορά.

Χρήσιμα σύμβολα:

- M0 : 0l είναι η συμβολοσειρά από 0 μήκους l.
- M0(i) : 0l-e||be-1...b1b0 όπου τα bi είναι η δυαδική αναπαράσταση του i.
- K : ένα σύνολο των συμβολοσειρών με l-bit μέγεθος.
- E : ένα σύνολο μετασχηματισμών κρυπτογράφησης.
- Et : ένας μετασχηματισμός κρυπτογράφησης στον E με t∈K . Το Et απεικονίζει συμβολοσειρές των l-bit σε συμβολοσειρές των l-bit.
- h : μια μονόδρομη συνάρτηση κατακερματισμού με πεδίο ορισμού {0,1}* και πεδίο

τιμών {0,1}l και είναι δημόσια γνωστή.
• n : ένα σταθερός θετικός αριθμός και είναι μια παράμετρος ασφαλείας.
Αλγόριθμος-Παραγωγή κλειδιού ψηφιακής υπογραφής μιας χρήσης Rabin
Περίληψη: Η Alice επιλέγει ένα σχήμα κρυπτογράφησης συμμετρικού κλειδιού E, παράγει2n τυχαίες συμβολοσειρές και ένα σύνολο παραμέτρων επικύρωσης.
Η Alice πρέπει να κάνει τα ακόλουθα:
1) Να επιλέξει ένα σχήμα κρυπτογράφησης συμμετρικού κλειδιού E.
2) Να παράγει 2n τυχαίες μυστικές συμβολοσειρές $k1 , k2 ,... , k2n \in K$, η κάθε μια με μέγεθος l-bit.
3) Να υπολογίσει $yi = Eki (M0(i)), 1 \leq i \leq 2n$.
4) Το δημόσιο κλειδί της Alice είναι (y1,y2,...,y2n) και το ιδιωτικό κλειδί της (k1,k2,...,k2n).
Αλγόριθμος-Παραγωγή και επαλήθευση της ψηφιακής υπογραφής μιας χρήσης Rabin
Περίληψη: Η Alice υπογράφει ένα δυαδικό μήνυμα m πεπερασμένου μήκους. Η επαλήθευση υπογραφών γίνεται με την συνεργασία της Alice.
1) Παραγωγή υπογραφής. Η Alice πρέπει να κάνει τα ακόλουθα:
   a) Να υπολογίσει h(m).
   b) Να υπολογίσει $si = Eki (h(m)), 1 \leq i \leq 2n$.
   c) Η υπογραφή της Alice για το m είναι (s1,s2,...,s2n).
2) Επαλήθευση. Ο Bob για να επαληθεύσει ότι η υπογραφή της Alice είναι η (s1,s2,...,s2n) για το m, πρέπει να κάνει τα ακόλουθα:
   a) Να αποκτήσει το αυθεντικό δημόσιο κλειδί της Alice (y1,y2,...,y2n).
   b) Να υπολογίσει την h(m).
   c) Να επιλέξει n διακριτούς αριθμούς rj, $1 \leq rj \leq 2n$, για $1 \leq j \leq n$.
   d) Να ζητήσει από την Alice τα κλειδιά krj , $1 \leq j \leq n$.
   e) Να επαληθεύσει την αυθεντικότητα των κλειδιών αυτών υπολογίζοντας zj = Ekr j (M0(r j)) και να ελέγξει ότι zj = y rj , για κάθε $1 \leq j \leq n$.
   f) Να επαληθεύσει ότι srj=Ekrj (h (m)), $1 \leq j \leq n$.

Το μέγεθος των κλειδιών σε αυτό το σχήμα εξαρτάται από το Et το οποίο δίνει ως έξοδο l-bit. Οπότε το δημόσιο και ιδιωτικό κλειδί αποτελείται από 2nl bits το κάθε ένα.

Έτσι για παράδειγμα αν n = 80 και l =64, τα κλειδιά που θα παραχθούν θα έχουν μήκος 1280 bytes το κάθε ένα.

4.5.3. Ασφάλεια

Στο σχήμα ψηφιακής υπογραφής Rabin μιας χρήσης μπορεί να προκύψουν κάποιες αντιδικίες μεταξύ της Alice και του Bob. Οι αντιδικίες αυτές εμφανίζονται όταν η Alice θεωρήσει ότι πλαστογραφήθηκε η υπογραφή της, ενώ ο Bob θεωρεί ότι είναι αυθεντική. Για την επίλυση αυτού, εμπλέκεται ένα τρίτο έμπιστο πρόσωπο και πραγματοποιείται η παρακάτω διαδικασία:

1) Ο Bob δίνει το μήνυμα m και την υπογραφή της Alice (s1,s2,...,s2n) σε ένα τρίτο έμπιστο πρόσωπο (TTP).
2) Ο TTP αποκτά τα k1,k2,...,k2n από την Alice.
3) Ο TTP επαληθεύει την αυθεντικότητα του ιδιωτικού κλειδιού υπολογίζοντας zi =Eki (M0(i)) και ελέγχει αν yi = zi, 1≤i≤2n . Αν αυτός ο έλεγχος αποτύχει, ο TTPενημερώνει τον Bob ότι η υπογραφή είναι έγκυρη και τον δικαιώνει.
4) Ο TTP υπολογίζει ui = Eki (h(m)), 1≤i≤2n . Μετά ελέγχει αν ui = si για το πολύ n τιμές του i και ενημερώνει την Alice ότι η υπογραφή της έχει πλαστογραφηθεί και την δικαιώνει. Αν για n+1 ή και για περισσότερες τιμές του i προκύπτει ui = si, η υπογραφή θεωρείται αυθεντική και ο TTP δικαιώνει τον Bob.

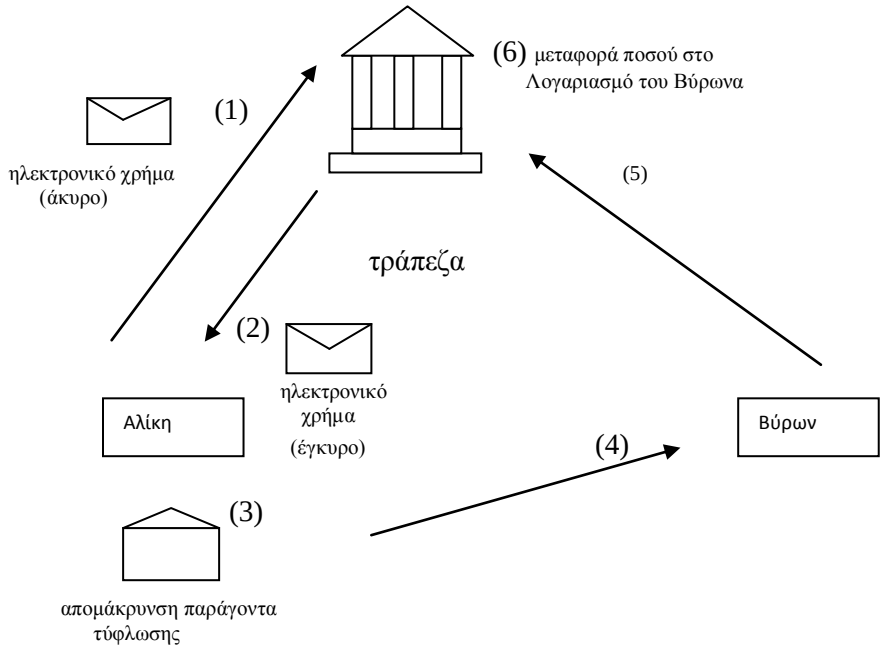
Η διαδικασία αυτή βασίζεται στον εξής συλλογισμό. Η Alice μπορεί να δημιουργήσει μια υπογραφή και για κάποιον λόγο στο μέλλον να αμφισβητήσει την αυθεντικότητα της. Τότε θα πρέπει να διασφαλίσει ότι ui = si για ακριβώς n τιμές του i και να ευελπιστεί ότι ο Bob θα επιλέξει ακριβώς αυτές τις τιμές (αυτό συμβαίνει με πολύ μικρή πιθανότητα). Από την πλευρά του Bob, άμα προσπαθήσει να διαπράξει αυτός πλαστογραφία για ένα μήνυμα m', θα πρέπει να δημιουργήσει τουλάχιστον ένα παραπάνω κλειδί k'. Δημιουργεί αυτό το κλειδί έτσι ώστε τουλάχιστον n+1 τιμές του i να προκύψει ui = si. Ένας άλλος τρόπος για να επιτύχει τον σκοπό του μπορεί να προσδιορίσει κατάλληλο m' για το οποίο ισχύει h(m) = h(m'). Για να αποτραπεί αυτή η απάτη θα πρέπει να επιλεγεί προσεκτικά ο αλγόριθμος παραγωγής συμμετρικού κλειδιού και η συνάρτηση κατακερματισμού.

4.5.4. Συστήματα τυφλών ψηφιακών υπογραφών.

Οι τυφλές ψηφιακές υπογραφές παρουσιάζουν πρακτικό ενδιαφέρον σε πολλές εφαρμογές, όπως στο ηλεκτρονικό χρήμα και στις ηλεκτρονικές εκλογές. Η χαρακτηριστική ιδιότητα που καθιστά μια υπογραφή τυφλή είναι το γεγονός ότι ο υπογράφων δε γνωρίζει το περιεχόμενο του μηνύματος που υπογράφει.
Η αναλογία της τυφλής υπογραφής παριστάνεται στο ακόλουθο παράδειγμα. Έστω ότι απαιτείται να υπογραφεί ένα έγγραφο χωρίς να γνωρίζει ο υπογράφων το περιεχόμενο του. Το έγγραφο μπορεί να μπει σε φάκελο, μαζί με ένα φύλλο καρμπόν και να σφραγισθεί. Στη συνέχεια, ο υπογράφων βάζει την υπογραφή του επάνω στο φάκελο και λόγω της παρεμβολής του καρμπόν, η υπογραφή μεταφέρεται στο κλειστό έγγραφο. Στη συνέχεια, ο παραλήπτης του εγγράφου μπορεί να ανοίξει το φάκελο και να παραλάβει το υπογεγραμμένο έγγραφο.
Η παραπάνω αναλογία είναι χρήσιμη στο ηλεκτρονικό χρήμα ως εξής. Ο πελάτης της ηλεκτρονικής τράπεζας ετοιμάζει ηλεκτρονικά χρήματα, τα οποία επικυρώνονται από την ηλεκτρονική τράπεζα. Η επικύρωση πραγματοποιείται όταν η ηλεκτρονική τράπεζα υπογράφει τα ηλεκτρονικά χρήματα του πελάτη, τα οποία αυτόματα μετατρέπονται σε ηλεκτρονικό χρήμα. Μια βασική ιδιότητα του

φυσικού χρήματος είναι η ανωνυμία ξοδέματος (anonymity of spending). Η τράπεζα δεν μπορεί να ανιχνεύσει που ξοδεύονται τα φυσικά χρήματα τα οποία έχει διανέμει στους πολίτες. Αυτή η ιδιότητα είναι επιθυμητή και στον ηλεκτρονικό κόσμο.

Αν η ηλεκτρονική τράπεζα ήταν σε θέση να γνωρίζει τα χρήματα που υπογράφει, τότε θα είχε τη δυνατότητα να αναγνωρίσει τον αγοραστή σε μια συναλλαγή. Ο κύκλος του ηλεκτρονικού χρήματος παριστάνεται στο σχήμα 4.1.



Σχήμα 4.1.: Ο κύκλος του ηλεκτρονικού χρήματος

Η Αλίκη αποφασίζει να αγοράσει ένα σαξόφωνο από τον μουσικό οίκο του Βύρωνα. Αρχικά, δημιουργεί ένα ηλεκτρονικό «χαρτονόμισμα» που αναγράφει την αξία του σαξόφωνου (ας χρησιμοποιήσουμε καταχρηστικά τον όρο «χαρτονόμισμα» προς χάριν της παραστατικής περιγραφής). Στη συνέχεια, το τοποθετεί σε ηλεκτρονικό φάκελο, εφαρμόζοντας έναν μυστικό παράγοντα τύφλωσης (blinding factor) και στέλνει τον ηλεκτρονικό φάκελο στην Τράπεζα (1). Η Τράπεζα με τη σειρά της υπογράφει ψηφιακά τον φάκελο, καθιστώντας έγκυρο το περιεχόμενό του και στέλνει το αποτέλεσμα πίσω στην Αλίκη (2). Η Αλίκη απομακρύνει τον παράγοντα τύφλωσης, το οποίο ισοδυναμεί με την εξαγωγή του έγκυρου πλέον χαρτονομίσματος από τον φάκελο (3) και το μεταβιβάζει στον Βύρωνα (4). Ο Βύρων ελέγχει την εγκυρότητα της υπογραφής, εφόσον γνωρίζει το αντίστοιχο δημόσιο κλειδί της Τράπεζας και παραδίδει το προϊόν στην Αλίκη. Τέλος, ο Βύρων στέλνει το χαρτονόμισμα στην Τράπεζα η οποία ενημερώνει το λογαριασμό του Βύρωνα με το αναγραφόμενο ποσό.

Η παραπάνω περιγραφή του κύκλου του ηλεκτρονικού χρήματος δίνει μόνον την αρχή λειτουργίας μιας υποδομής ηλεκτρονικού χρήματος. Στην πράξη εφαρμόζονται ποικίλα πρωτόκολλα τα οποία ανταλλάσσονται μεταξύ των επικοινωνούντων μελών, για την προστασία αυτών. Τα πρωτόκολλα απαιτούνται για να μειωθούν ή και να εξαλειφθούν σοβαρές απειλές του συστήματος. Ίσως η σημαντικότερη από αυτές είναι η απειλή του διπλού ξοδέματος (double spending). Καθώς το ηλεκτρονικό χρήμα δεν είναι τίποτε άλλο από μια σειρά δυαδικών ψηφίων, η Αλίκη θα μπορούσε να κρατήσει ένα αντίγραφο του χαρτονομίσματος και να το παρουσιάσει σε κάποιο άλλο κατάστημα για να πραγματοποιήσει αγορά με το ίδιο χαρτονόμισμα. Παρόμοια και ο Βύρων θα μπορούσε να χρησιμοποιήσει το χαρτονόμισμα της Αλίκης για να πραγματοποιήσει δική του αγορά. Για λεπτομέρειες σχετικά με τα πρωτόκολλα ηλεκτρονικού χρήματος παραπέμπουμε τον αναγνώστη στη βιβλιογραφία, καθώς στο σημείο αυτό θα ασχοληθούμε αποκλειστικά με τα συστήματα τυφλών υπογραφών.

4.5.5.Σύστημα τυφλών ψηφιακών υπογραφών RSA.

Η ανακάλυψη των τυφλών υπογραφών αποδίδεται στον Chaum ο οποίος είναι και ο βασικός ερευνητής στο συγκεκριμένο χώρο. Το πρώτο και απλούστερο σύστημα ψηφιακών υπογραφών που κατασκευάσθηκε βασίζεται στις κρυπτογραφικές πράξεις του ασύμμετρου κρυπτοσυστήματος RSA.

Έστω ότι η Αλίκη επιθυμεί να παραλάβει υπογεγραμμένο το μήνυμα m από τον Βύρωνα, χωρίς αυτός να γνωρίζει το περιεχόμενο του μηνύματος. Θεωρούμε ότι το δημόσιο κλειδί του Βύρωνα είναι (e, n) και το ιδιωτικό του κλειδί είναι το d. Επίσης, για το μήνυμα ισχύει $m < n$.

Αρχικά η Αλίκη επιλέγει τον παράγοντα τύφλωσης ο οποίος είναι ένας μυστικός ακέραιος k, τέτοιος ώστε $0 < k < n$ και $\gcd(k, n) = 1$. Ένα σύστημα τυφλών ψηφιακών υπογραφών αποτελείται από τρεις διαδικασίες: την τύφλωση, την υπογραφή και την απομάκρυνση του παράγοντα τύφλωσης. Στο σύστημά μας, οι τρεις διαδικασίες ορίζονται ως εξής:

- (τύφλωση). Υπολογισμός του $m' \equiv mk^e \pmod n$ από την Αλίκη.
  Αλίκη → Βύρων: m'
- (υπογραφή). Υπολογισμός του $s \equiv (m')^d \pmod n$ από τον Βύρωνα.
  Βύρων → Αλίκη: s
- (απομάκρυνση του παράγοντα τύφλωσης). Υπολογισμός του $sk^{-1} \bmod n$. Το αποτέλεσμα του υπολογισμού θα είναι η υπογραφή του Βύρωνα στο μήνυμα m.

4.5.6. Ψηφιακές υπογραφές συμμετρικής κρυπτογραφίας

Αν και οι ψηφιακές υπογραφές είναι κατεξοχήν θέμα ασύμμετρης κρυπτογραφίας, έχουν προταθεί εναλλακτικά συστήματα ψηφιακών υπογραφών που βασίζονται σε συμμετρική κρυπτογραφία.

Τα συστήματα ψηφιακών υπογραφών συμμετρικής κρυπτογραφίας χωρίζονται σε συστήματα ψηφιακών υπογραφών με τη συμμετοχή τρίτης έμπιστης οντότητας και σε συστήματα ψηφιακών υπογραφών χωρίς τη συμμετοχή της έμπιστης οντότητας. Επειδή η τρίτη έμπιστη οντότητα χρησιμοποιείται στην ασύμμετρη κρυπτογραφία, στα συστήματα ψηφιακών υπογραφών χρησιμοποιείται ο όρος **διαιτητής** (arbitrator), ο οποίος περιγράφει με ικανοποιητική ακρίβεια το ρόλο της έμπιστης οντότητας σε ένα σύστημα ψηφιακών υπογραφών.

4.5.7. Σύστημα ψηφιακής υπογραφής χωρίς τη συμμετοχή διαιτητή.

Θα παρουσιάσουμε το σύστημα ψηφιακής υπογραφής του Lamport. Το σύστημα ψηφιακής υπογραφής εφαρμόζει την ψηφιακή υπογραφή σε μήνυμα του ενός bit, δηλαδή $m \in \{0, 1\}$. Η αρχική πρόταση του συστήματος χρησιμοποιεί τον συμμετρικό κρυπταλγόριθμο DES, αλλά μπορεί να χρησιμοποιηθεί οποιοσδήποτε συμμετρικός κρυπταλγόριθμος.

Όπως και στα συστήματα ψηφιακών υπογραφών ασύμμετρης κρυπτογραφίας, υπάρχει το στάδιο δημιουργίας των κλειδιών. Εφόσον στη συμμετρική κρυπτογραφία δεν ορίζεται η έννοια του δημόσιου και ιδιωτικού κλειδιού, θα ονομάσουμε τις απαιτούμενες αντίστοιχες ποσότητες ως «ισοδύναμο ιδιωτικό» και «ισοδύναμο δημόσιο» κλειδί, των οποίων οι ρόλοι θα είναι ίδιοι με τα ασύμμετρα κλειδιά των συστημάτων ψηφιακής υπογραφής που εξετάσαμε.

Έστω $e_k(\cdot)$ η πράξη κρυπτογράφησης ενός συμμετρικού κρυπτοσυστήματος. Ο υπογράφων επιλέγει δύο κλειδιά k_0 και k_1, καθώς και δύο απλά κείμενα, p_0 και p_1. Από τα δύο απλά κείμενα, το p_0 αντιστοιχεί στο **0** ενώ το p_1 αντιστοιχεί στο **1**. Ας σημειωθεί ότι τα μεγέθη των δύο κρυπτοκειμένων είναι προκαθορισμένα όπως απαιτεί ο συμμετρικός κρυπταλγόριθμος, τα οποία θα είναι ασφαλώς μεγαλύτερα του ενός bit. Έχουμε δηλαδή μεγάλη αύξηση της περίσσειας, αφού απαιτούνται n bits προκειμένου να περιγράψουμε πληροφορία ενός bit (όπου n το μέγεθος του τμήματος του απλού κειμένου που απαιτεί ο συμμετρικός κρυπταλγόριθμος).

Στη συνέχεια, ο υπογράφων κρυπτογραφεί με το συμμετρικό κρυπταλγόριθμο τα δύο απλά κείμενα, όπου στο κάθε απλό κείμενο εφαρμόζει διαφορετικό κλειδί:

$C_0 = e_{k0}$ (p0) και

$C_1 = e_{k1}$ (p1)

Η παραπάνω κρυπτογράφηση ολοκληρώνει τη διαδικασία δημιουργίας των κλειδιών. Το ισοδύναμο δημόσιο κλειδί αποτελείται από τα (p_0, p_1, c_0, c_1), ενώ το ισοδύναμο ιδιωτικό κλειδί αποτελείται από τα μυστικά κλειδιά (k_0, k_1).

Η δημοσίευση του ισοδύναμου δημόσιου κλειδιού περικλείει και τη διαδικασία υπογραφής του μηνύματος. Με αυτόν τον τρόπο δεν υπάρχει ξεχωριστή διαδικασία υπογραφής. Πιο συγκεκριμένα, η εκτέλεση της ψηφιακής υπογραφής είναι η κρυπτογράφηση των δύο απλών κειμένων.

Κατά τη διαδικασία της επαλήθευσης, ο υπογράφων αποκαλύπτει ένα από τα κλειδιά. Αν το μήνυμα είναι το m = **0**, τότε ο υπογράφων αποκαλύπτει το κλειδί k_0, ενώ αν το μήνυμα είναι το m = **1**, τότε ο υπογράφων αποκαλύπτει το κλειδί k_1. Έτσι ο παραλήπτης του υπογεγραμμένου bit μπορεί να εκτελέσει την ίδια συμμετρική κρυπτογράφηση με τον υπογράφοντα και να ελέγξει αν το κλειδί είναι αυτό που αντιστοιχίζει το απλό κείμενο στο κρυπτοκείμενο, όπως περιγράφονται στο ισοδύναμο δημόσιο κλειδί.

Ασφάλεια και μειονεκτήματα του συστήματος ψηφιακής υπογραφής του Lamport

Η ασφάλεια του συστήματος ψηφιακής υπογραφής που παρουσιάσαμε είναι ισοδύναμη με την ασφάλεια του συμμετρικού κρυπταλγόριθμου, που χρησιμοποιείται. Η επίθεση της πλαστογραφίας σε αυτήν την περίπτωση είναι η πρόκληση του αντιπάλου να ανακαλύψει το κλειδί το οποίο δεν έχει αποκαλυφθεί από τον υπογράφοντα. Ο αντίπαλος γνωρίζει ένα ζεύγος απλού κειμένου και του αντίστοιχου κρυπτοκειμένου, επομένως θα επιχειρήσει επίθεση γνωστού απλού κειμένου. Έτσι, η ασφάλεια του συστήματος ψηφιακών υπογραφών εξαρτάται από την κρυπτογραφική δύναμη του συμμετρικού κρυπταλγόριθμου. Επιπλέον, η φύλαξη των μυστικών κλειδιών είναι προφανής απαίτηση ασφάλειας του συστήματος ψηφιακής υπογραφής.

Η εξάρτηση της ασφάλειας του συστήματος ψηφιακής υπογραφής από την κρυπτογραφική δύναμη του συμμετρικού κρυπταλγόριθμου είναι το κριτήριο επιλογής ενός συστήματος ψηφιακής υπογραφής συμμετρικής κρυπτογραφίας, έναντι ενός συστήματος ασύμμετρης κρυπτογραφίας. Το μακρύ ιστορικό των τεχνικών σχεδιασμού, καθώς και της αξιολόγησης της ασφάλειας και των κρυπτογραφικών ιδιοτήτων των κρυπτογραφικών συναρτήσεων που αφορά τη συμμετρική κρυπτογραφία προτιμάται από πολλούς έναντι της ασύμμετρης κρυπτογραφίας, η οποία βασίζεται σε «δύσκολα» προβλήματα.

Ωστόσο, ένα σύστημα ψηφιακής υπογραφής συμμετρικού κρυπτοσυστήματος όπως αυτό του Lamport που παρουσιάσαμε, έχει σοβαρά πρακτικά μειονεκτήματα. Αν υπολογίσουμε τον αριθμό των συνολικών bits που απαιτούνται προκειμένου να υπογραφεί ένα bit, θα διαπιστώσουμε ότι το υπολογιστικό κόστος καθώς και το κόστος αποθήκευσης είναι μεγάλα. Αν υποθέσουμε ότι ο κρυπταλγόριθμος είναι ο DES (όπως ήταν και στην αρχική πρόταση του συστήματος), για την υπογραφή ενός bit, το ισοδύναμο δημόσιο κλειδί θα έχει μέγεθος ίσο με 256 bits ενώ η υπογραφή (το ισοδύναμο ιδιωτικό κλειδί) θα έχει μήκος ίσο με 52 bits.
Ένα άλλο μειονέκτημα είναι ότι δεν μπορούν να επαναχρησιμοποιηθούν το ισοδύναμο δημόσιο και ιδιωτικό κλειδί. Από τη στιγμή που υπογραφεί ένα bit, θα πρέπει να δημιουργηθούν από την αρχή νέα ισοδύναμα κλειδιά. Αυτό σημαίνει ότι αν χρησιμοποιηθεί (για οικονομία!) μια κρυπτογραφική μονόδρομη hash για να υπογραφούν τα bits αυτής, τότε με βάση το παράδειγμα του DES, ο όγκος των δημόσιων κλειδιών θα είναι ίσος με ν·256 bits, όπου ν το μέγεθος της σύνοψης σε bits.

ΠΑΡΑΔΕΙΓΜΑ – Υπολογισμός ασφαλούς συστήματος ψηφιακής υπογραφής με σημερινά δεδομένα. Έστω ότι επιθυμούμε να κατασκευάσουμε το σύστημα ψηφιακών υπογραφών Lamport ώστε να είναι ασφαλές με τα σημερινά δεδομένα υπολογιστικής ισχύος. Θα χρησιμοποιήσουμε τον κρυπταλγόριθμο AES με μεγέθη απλού κειμένου, κρυπτοκειμένου και κλειδιού ίσα με 128 bits. Επίσης, μπορούμε να χρησιμοποιήσουμε την κρυπτογραφική hash MD5, η οποία θεωρείται ανθεκτική σε συγκρούσεις.

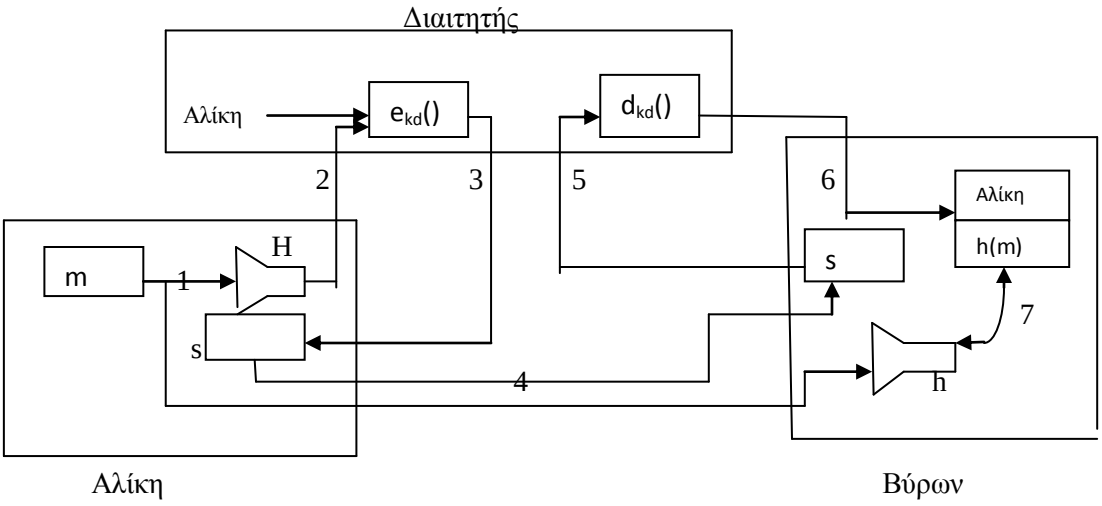
- Δεδομένης της σημερινής υπολογιστικής ισχύος, προκειμένου να είναι υπολογιστικά αδύνατο να βρεθούν συγκρούσεις στην hash, επιλέγουμε το μέγεθος της σύνοψης να είναι 160 bits.
- Για κάθε bit της σύνοψης που θα υπογράφεται, απαιτείται διαφορετικό ισοδύναμο δημόσιο και ιδιωτικό κλειδί. Το μέγεθος του ισοδύναμου δημόσιου κλειδιού θα είναι ίσο με: 4·128 = 512 bits. Το ιδιωτικό κλειδί θα έχει μέγεθος ίσο με 256 bits (για τα δύο κλειδιά), ενώ η ψηφιακή υπογραφή του για το συγκεκριμένο bit θα έχει μέγεθος 128 bits.
- Συνολικά, για τα 160 bits της σύνοψης, ο όγκος των ισοδύναμων δημόσιων κλειδιών ανέρχεται στα 512·160 = 81920 bits, ενώ η ψηφιακή υπογραφή θα έχει μέγεθος ίσο με 128·160 = 20480 bits.

4.5.8. Σύστημα ψηφιακής υπογραφής με διαιτητή.

Τα μειονεκτήματα του συστήματος ψηφιακής υπογραφής συμμετρικής κρυπτογραφίας άνευ διαιτητού που περιγράψαμε, καθιστούν πρακτικά άχρηστο

ένα τέτοιο σύστημα, σε πολλές εφαρμογές. Η εισαγωγή του διαιτητή στο σύστημα έχει στόχο να ξεπεράσει τα μειονεκτήματα. Βέβαια, η ανάγκη εμπιστοσύνης μιας τρίτης οντότητας μειώνει την ασφάλεια του συστήματος, αφού στην περίπτωση που η οντότητα δεν αποδώσει την επιθυμητή εμπιστοσύνη, τότε υπάρχει κίνδυνος κατάρρευσης του συστήματος. Για μια ακόμη φορά είμαστε αναγκασμένοι να εντοπίσουμε τη χρυσή τομή μεταξύ του πρακτικού και της ασφάλειας· για μια ακόμη φορά η κρυπτογραφία δε δίνει λύσεις αλλά δίνει τα εργαλεία για να μετασχηματίσουμε ένα πρόβλημα σε μορφή που η διαχείρισή του θα είναι ευκολότερη.

Το σύστημα ψηφιακής υπογραφής συμμετρικής κρυπτογραφίας με τη συμμετοχή διαιτητή που θα παρουσιάσουμε στη συνέχεια είναι των Needham και Schroeder. Περιλαμβάνει μια κρυπτογραφική μονόδρομη hash και έναν συμμετρικό κρυπταλγόριθμο. Η hash εκτελείται από τα επικοινωνούντα μέλη, ενώ η κρυπτογράφηση και αποκρυπτογράφηση εκτελούνται από το διαιτητή. Έστω ότι η Αλίκη υπογράφει ένα μήνυμα m για να το στείλει στον Βύρωνα. Η διαδικασία παρουσιάζεται στο Σχήμα 4.2.



Σχήμα 4.2 : Σύστημα ψηφιακής υπογραφής με διαιτητή.

Υποθέτουμε ότι όλα τα κανάλια επικοινωνίας μεταξύ των τριών συμμετασχόντων του μοντέλου του σχήματος προσφέρουν αυθεντικοποίηση και ακεραιότητα των μηνυμάτων. Αυτό μπορεί να γίνει με τη βοήθεια κάποιου κέντρου διανομής κλειδιών. Τα κλειδιά αυτά μπορούν να χρησιμοποιηθούν σε μονόδρομη MAC. Οι διαδικασίες αυθεντικοποίησης και ακεραιότητας δεν φαίνονται στο παραπάνω σχήμα. Το σύστημα ψηφιακών υπογραφών αποτελείται από τα εξής βήματα:

1. Η Αλίκη υπολογίζει τη σύνοψη του μηνύματος m και στη συνέχεια στέλνει το αποτέλεσμα στον διαιτητή, μαζί με την ταυτότητά της. Ο διαιτητής θα

πρέπει να είναι σε θέση να γνωρίζει την ταυτότητα της υπογράφουσας για να την συμπεριλάβει στην ψηφιακή υπογραφή, όπως θα δούμε στη συνέχεια.

2. Ο διαιτητής δημιουργεί ένα νέο μήνυμα το οποίο αποτελείται από την ταυτότητα της Αλίκης και τη σύνοψη που παρέλαβε. Στη συνέχεια, κρυπτογραφεί το μήνυμα με το μυστικό του κλειδί kd:

   $S = e_{kd}$ (Αλίκη || h (m))

3. Το αποτέλεσμα της παραπάνω συμμετρικής κρυπτογράφησης είναι η ψηφιακή υπογραφή, την οποία στέλνει ο διαιτητής πίσω στην Αλίκη.

4. Όταν η Αλίκη αποφασίσει να στείλει το υπογεγραμμένο μήνυμα στον Βύρωνα, προσκολλά την υπογραφή s στο μήνυμα m και τα στέλνει στον Βύρωνα.

5. Μόλις ο Βύρων λάβει το μήνυμα και την υπογραφή αυτού (m||s), στέλνει την υπογραφή s στον διαιτητή.

6. Ο διαιτητής αποκρυπτογραφεί την υπογραφή με το μυστικό του κλειδί και το αποτέλεσμα που προκύπτει στέλνεται ως απάντηση στον Βύρωνα. Το αποτέλεσμα είναι η ταυτότητα της Αλίκης και η σύνοψη υπό μορφή απλού κειμένου.

7. Τέλος, ο Βύρων εξακριβώνει την ταυτότητα της Αλίκης στο πρώτο τμήμα της αποκρυπτογραφημένης υπογραφής και στη συνέχεια υπολογίζει τη σύνοψη του μηνύματος (h(m)) και τη συγκρίνει με αυτήν που παρέλαβε από τον διαιτητή. Αν οι δύο συνόψεις συμπίπτουν, τότε δέχεται την ψηφιακή υπογραφή.

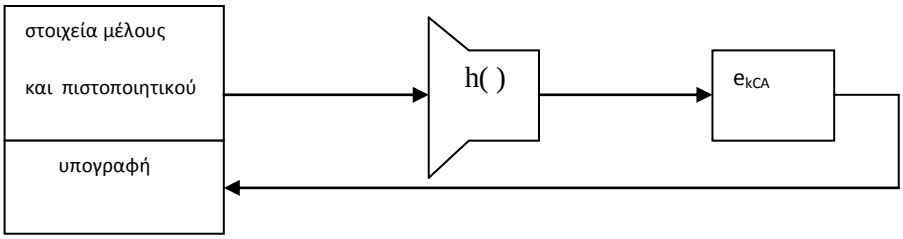
Από την παραπάνω περιγραφή είναι φανερό ότι οι ψηφιακές υπογραφές κατασκευάζονται από τον διαιτητή. Στην πραγματικότητα, η ψηφιακή υπογραφή μοιράζεται μεταξύ της Αλίκης και του διαιτητή, καθώς ο διαιτητής δε γνωρίζει το μήνυμα το οποίο υπογράφεται. Η Αλίκη βασίζεται στον διαιτητή για να ολοκληρώσει τη διαδικασία της ψηφιακής υπογραφής, αλλά αντίθετα, ο διαιτητής έχει τη δυνατότητα να πλαστογραφήσει μήνυμα της Αλίκης, εφόσον γνωρίζει τη κρυπτογραφική μονόδρομη hash που χρησιμοποιείται. Έτσι, η ασφάλεια του συστήματος εξαρτάται από την εμπιστοσύνη του διαιτητή, την κρυπτογραφική δύναμη του συμμετρικού κρυπταλγόριθμου που χρησιμοποιεί ο διαιτητής και από τη μυστικότητα και σωστή φύλαξη του συμμετρικού κλειδιού του διαιτητή.

5.Ψηφιακά Πιστοποιητικά και Αρχές Πιστοποίησης.

5.1.Ψηφιακά Πιστοποιητικά.

Το πιστοποιητικό αποτελείται από δύο μέρη, από τα δεδομένα και από την ψηφιακή υπογραφή. Τα δεδομένα περιλαμβάνουν στοιχεία του εντολέα, στοιχεία του πιστοποιητικού, καθώς και πληροφορίες σχετικά με τις κρυπτογραφικές συναρτήσεις που χρησιμοποιήθηκαν στη δημιουργία της ψηφιακής υπογραφής.

Η διαδικασία δημιουργίας ενός ψηφιακού πιστοποιητικού παριστάνεται στο παρακάτω σχήμα.



Σχήμα 5.1. : Διαδικασία δημιουργίας ψηφιακού πιστοποιητικού

Η Αρχή Πιστοποίησης δημιουργεί με τη βοήθεια μιας μονόδρομης hash μια σύνοψη των στοιχείων του πρώτου μέρους το πιστοποιητικού, και στη συνέχεια το κρυπτογραφεί με το ιδιωτικό της κλειδί k_{dCA} .

5.2.Πιστοποιητικό X.509.

Το πιστοποιητικό X.509 είναι η τυποποίηση που κυριαρχεί στα PKI που χρησιμοποιούν τεχνολογίες του Διαδικτύου. Τα πεδία του X.509 φαίνονται στον πίνακα που ακολουθεί.

Όνομα πεδίου	Χρήση
version	Η έκδοση του προτύπου X.509. Ορίζονται 3 εκδόσεις του X.509. Η έκδοση 1 δεν περιέχει τα πεδία *issuer unique identifier, subject unique identifier* τα οποία προστέθηκαν στην έκδοση 2, καθώς και το πεδίο *extensions* το οποίο προστέθηκε στην έκδοση 3.
serial number	Ένας μοναδικός ακέραιος που καθορίζεται από την Αρχή Πιστοποίησης για να αναγνωρίσει το πιστοποιητικό.

signature algorithm identifier	Το πεδίο αυτό αποτελείται στην ουσία από 2 πεδία, τα ονόματα των κρυπτογραφικών συναρτήσεων που συμμετέχουν, καθώς και από τις σχετικές παραμέτρους αυτών.
issuer name	Το όνομα της Αρχής Πιστοποίησης
period of validity	Αποτελείται από δύο ημερομηνίες, από την ημερομηνία ενεργοποίησης του πιστοποιητικού και από την ημερομηνία λήξης του πιστοποιητικού
subject name	Το όνομα της οντότητας που πιστοποιείται
algorithms	Το όνομα του κρυπταλγόριθμου που χρησιμοποιεί η οντότητα για να διαθέσει το δημόσιο κλειδί της
parameters	Οι σχετικές παράμετροι που προσδιορίζουν τη λειτουργία του παραπάνω κρυπταλγόριθμου
subject's public key	Το δημόσιο κλειδί της οντότητας που αναγνωρίζεται από το πεδίο subject name. Η οντότητα αυτή κατέχει το ιδιωτικό κλειδί.
issuer unique identifier	Ο αριθμός αυτός χρησιμοποιείται σε συνδυασμό με το όνομα της Αρχής Πιστοποίησης για να ενισχύσει την αναγνώριση αυτής.
subject unique identifier	Ο αριθμός αυτός χρησιμοποιείται σε συνδυασμό με το όνομα της οντότητας για να προσδώσει μοναδικότητα στο πιστοποιητικό, σε περίπτωση που το όνομα της οντότητας χρησιμοποιείται για άλλο πιστοποιητικό.
extensions	Εδώ μπορούν να προστεθούν επιπλέον στοιχεία για να υποστηρίξουν ειδικές απαιτήσεις της εφαρμογής.
signature	Η ψηφιακή υπογραφή με το ιδιωτικό κλειδί της Αρχής Πιστοποίησης επάνω σε όλες τις προαναφερθείσες πληροφορίες.

Πίνακας 5.2: Πεδία του πιστοποιητικού X.509

Η δομή και μορφή του ονόματος της Αρχής Πιστοποίησης καθορίζεται από το πρότυπο ονομασίας X.500, όπου το βασικό πεδίο είναι το ***διακεκριμένο όνομα*** (distinguished name), το οποίο έχει την εξής μορφή:

dn = όνομα _ΑΠ

Το διακεκριμένο όνομα μαζί με άλλα πεδία καθορίζουν πλήρως την Αρχή Πιστοποίησης.

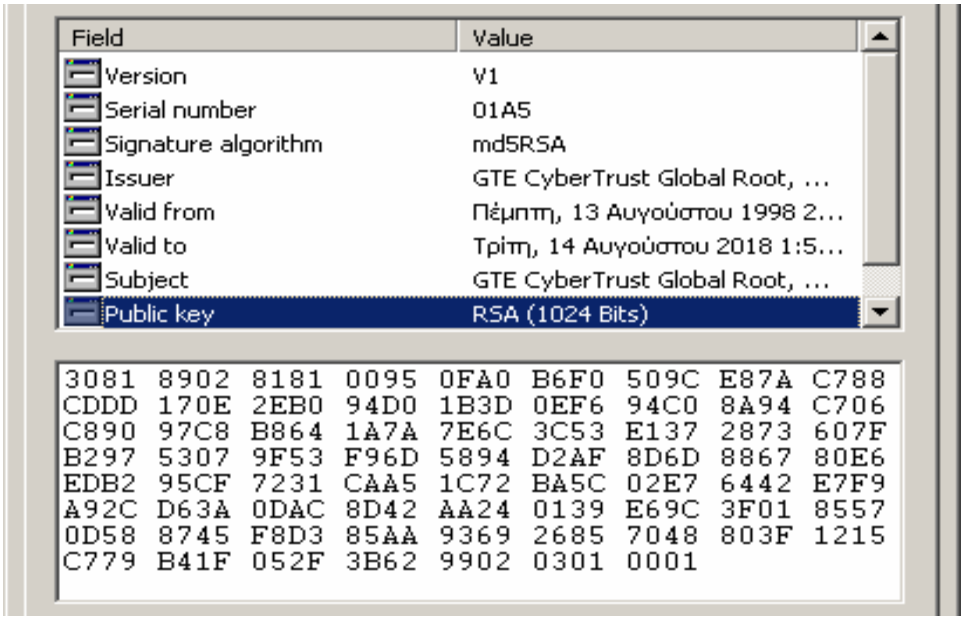
5.3.Διαδικασίες δημιουργίας, ελέγχου και ανάκλησης.

Σε μια υποδομή δημόσιου κλειδιού η διαχείριση των κλειδιών πραγματοποιείται με πλήρως καθορισμένες διαδικασίες. Από τεχνικής πλευράς, οι διαδικασίες αυτές χρησιμοποιούν πρωτόκολλα προκειμένου να εκτελεσθούν.

Η πρώτη διαδικασία που πραγματοποιείται κατά την εκκίνηση λειτουργίας ενός PKI είναι η ίδρυση της Αρχής Πιστοποίησης και η δημοσίευση του πιστοποιητικού της. Η δημοσίευση γίνεται ανάλογα με το περιβάλλον στο οποίο δρα το PKI.

Για παράδειγμα στο Διαδίκτυο υπάρχουν περισσότερες από 10 Αρχές Πιστοποίησης. Η Αρχή Πιστοποίησης επικοινωνεί με τους παροχείς των λογισμικών πελατών (client software) που χρησιμοποιούνται για πρόσβαση στις υπηρεσίες του Διαδικτύου και τους παρέχει μέσω ασφαλούς καναλιού το πιστοποιητικό που περιέχει το δημόσιο κλειδί της Αρχής Πιστοποίησης.

Στην εικόνα 5.3 φαίνεται το πιστοποιητικό της GTE CyberTrust που συνοδεύει τον Internet Explorer της Microsoft.



Εικόνα 5.3:Ψηφιακό πιστοποιητικό για υπηρεσίες www

Διαδικασία δημιουργίας και δημοσίευσης του πιστοποιητικού του χρήστη

Ο σκοπός του πιστοποιητικού είναι να συνδεθεί ένα όνομα με ένα δημόσιο κλειδί. Έτσι, απαραίτητη προϋπόθεση είναι η δημιουργία ενός ζεύγους δημόσιου και ιδιωτικού κλειδιού. Το δημόσιο κλειδί θα κατατεθεί στην Αρχή Εγγραφής μαζί με τα στοιχεία του χρήστη. Υπάρχουν δύο εναλλακτικές όπου μπορεί να δημιουργηθεί το ζεύγος του κλειδιού:

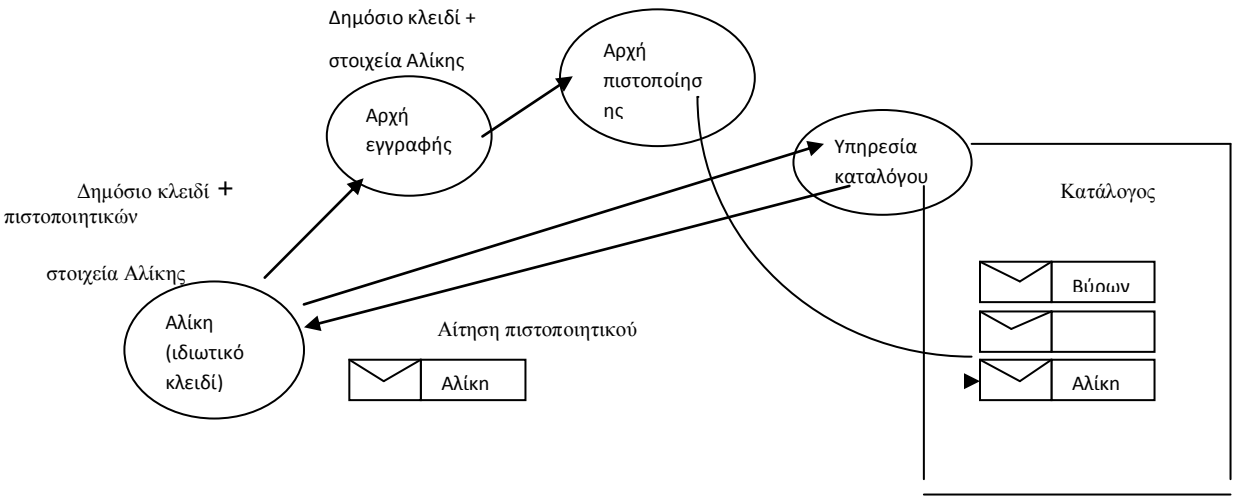
- Στο περιβάλλον του χρήστη. Στην περίπτωση αυτή το ρίσκο να αποκαλυφθεί το ιδιωτικό κλειδί είναι ελάχιστο, αφού ο μόνος γνώστης του κλειδιού είναι ο χρήστης. Ωστόσο, αν το κλειδί χρησιμοποιείται για κρυπτογράφηση μηνυμάτων και όχι για αυθεντικοποίηση, η απώλεια του κλειδιού θα καταστήσει αδύνατη την αποκρυπτογράφηση των μηνυμάτων που έχουν κρυπτογραφηθεί με το αντίστοιχο δημόσιο κλειδί.
- Στο περιβάλλον της Αρχής Εγγραφής ή Πιστοποίησης. Η δημιουργία του ζεύγους κλειδιών σε τοποθεσία διαφορετική από τον νόμιμο κάτοχο του ιδιωτικού κλειδιού έχει επίπτωση στην αυξημένη πολυπλοκότητα του μοντέλου επικοινωνίας. Αρχικά θα πρέπει να υπάρχει ένα ασφαλές κανάλι από το οποίο θα μεταφερθεί το ιδιωτικό κλειδί στον χρήστη. Επίσης, ο βαθμός εμπιστοσύνης και οι απαιτήσεις ασφάλειας της Αρχής Εγγραφής θα είναι πολύ μεγαλύτερες, γιατί σε περίπτωση επιτυχούς επίθεσης εκτίθενται τα ιδιωτικά κλειδιά των χρηστών. Το πλεονέκτημα της δημιουργίας του ζεύγους κλειδιών στην Αρχή Εγγραφής ή Πιστοποίησης επιτρέπει την ασφαλή αποθήκευση του ιδιωτικού κλειδιού και την ανάκτησή του αν ο χρήστης χάσει το κλειδί.

Σε ένα ανοικτό Διαδικτυακό περιβάλλον τα κλειδιά δημιουργούνται στο περιβάλλον του χρήστη, ενώ σε εταιρικά περιβάλλοντα υπάρχει συνήθως μια υπηρεσία η οποία δημιουργεί και παρέχει τα κλειδιά στους χρήστες.

Όποια εναλλακτική και να ακολουθηθεί, το ιδιωτικό κλειδί καταλήγει στο ***Ασφαλές Προσωπικό Περιβάλλον*** του χρήστη (Personal Security Environment) το οποίο μπορεί να είναι ο σκληρός δίσκος, αποσπώμενος δίσκος ή έξυπνη κάρτα. Από τα τρία, η ασφαλέστερη αποθήκευση είναι η έξυπνη κάρτα, η οποία θεωρείται ανθεκτική σε εξωτερικές επεμβάσεις (tamper proof) και έχει τη δυνατότητα να δημιουργεί τις ψηφιακές υπογραφές χωρίς να απαιτείται το ιδιωτικό κλειδί να μεταφερθεί σε λιγότερο ασφαλές περιβάλλον, όπως ο προσωπικός υπολογιστής του χρήστη.

Όταν η Αρχή Πιστοποίησης υπογράψει τα στοιχεία του χρήστη μαζί με το δημόσιό του κλειδί, το πιστοποιητικό που προκύπτει μεταφέρεται στον χρήστη είτε άμεσα, είτε μέσω της υπηρεσίας καταλόγου. Στη δεύτερη περίπτωση, η Αρχή Πιστοποίησης δημοσιεύει το πιστοποιητικό σε κάποιο κατάλογο ο οποίος διατίθεται δημόσια. Από το δημόσιο κατάλογο όλα τα μέλη έχουν πρόσβαση όπου επιτρέπεται μόνον η ανάγνωση. Αντίθετα, η Αρχή Πιστοποίησης έχει δυνατότητα πρόσβασης ανάγνωσης και εγγραφής. Οι απαιτήσεις ασφάλειας του καταλόγου είναι σχετικά μικρές, αφού η αυθαίρετη τροποποίηση ενός ή περισσοτέρων πιστοποιητικών μπορεί να ανιχνευθεί. Ο αντίπαλος που θα επιχειρήσει να μεταβάλλει το πιστοποιητικό κάποιου χρήστη θα πρέπει να γνωρίζει το ιδιωτικό κλειδί της Αρχής Πιστοποίησης. Η όλη διαδικασία

δημιουργίας και δημοσίευσης των πιστοποιητικών των χρηστών παριστάνεται στο Σχήμα 5.4.



Σχήμα 5.4.: Διαδικασία δημιουργίας και δημοσίευσης πιστοποιητικών

Διαδικασία ελέγχου του πιστοποιητικού

Θεωρούμε τη διαδικασία όπου η Αλίκη επιθυμεί να επικοινωνήσει με τον Βύρωνα. Επίσης θεωρούμε ότι η ασφαλής επικοινωνία απαιτεί αμοιβαία αυθεντικοποίηση των δύο μελών και καθορισμό κλειδιού συνόδου. Ο καθορισμός του κλειδιού συνόδου εξετάσθηκε στις προηγούμενες παραγράφους. Εδώ θα περιγράψουμε τη διαδικασία αυθεντικοποίησης των μελών από τα ψηφιακά χαρακτηριστικά.

Αρχικά, η Αλίκη επικοινωνεί με τον Βύρωνα ή με τον κατάλογο, προκειμένου να προσκομίσει το δημόσιο κλειδί του Βύρωνα. Στη συνέχεια, εκτελεί τις ακόλουθες δύο ενέργειες ελέγχου:

1. Έλεγχος των στοιχείων του πιστοποιητικού. Κατά τον έλεγχο αυτό, η Αλίκη εξετάζει τα στοιχεία του πιστοποιητικού που περιγράφουν τον Βύρωνα, καθώς και την επικαιρότητα του πιστοποιητικού. Το πιστοποιητικό θεωρείται επίκαιρο, αν η ημερομηνία λήξης είναι μεγαλύτερη από την τρέχουσα ημερομηνία.

2. Έλεγχος ανάκλησης του πιστοποιητικού. Πολλές φορές, λόγω κακής χρήσης του πιστοποιητικού ή λόγω υποψίας διαρροής του ιδιωτικού κλειδιού, το πιστοποιητικό μπορεί να λήξει πριν από την αναγραφόμενη ημερομηνία λήξης. Η τεχνητή αυτή λήξη ονομάζεται ανάκληση του πιστοποιητικού. Υπάρχουν δύο τεχνολογίες ανάκλησης του πιστοποιητικού: οι ***λίστες ανακληθέντων πιστοποιητικών*** (certificate revocation lists) και το ***πρωτόκολλο κατάστασης πιστοποιητικού*** (online certificate status protocol). Οι λίστες ανακληθέντων

πιστοποιητικών είναι πιστοποιητικά ειδικού τύπου τα οποία υπογράφει και εκδίδει η Αρχή Πιστοποίησης, όπου φαίνονται όλα τα πιστοποιητικά τα οποία έχουν ανακληθεί. Το πρωτόκολλο κατάστασης πιστοποιητικού προϋποθέτει σύνδεση με την αντίστοιχη υπηρεσία της Αρχής Πιστοποίησης η οποία παρέχει πληροφορίες σχετικά με την ανάκληση ενός συγκεκριμένου πιστοποιητικού.

Μετά την επιτυχή ολοκλήρωση των δύο παραπάνω ελέγχων και από τις δύο πλευρές, ακολουθεί πρωτόκολλο αυθεντικοποίησης το οποίο βασίζεται σε ασύμμετρη κρυπτογραφία.

Διαδικασία ανάκλησης του πιστοποιητικού

Η ανάκληση του πιστοποιητικού γίνεται σε δύο περιπτώσεις:

- Στην περίπτωση που ο χρήστης υποψιασθεί ότι το ιδιωτικό του κλειδί έχει εκτεθεί και έχει γίνει γνωστό σε τρίτους.
- Στην περίπτωση που γίνει κακή χρήση του πιστοποιητικού από τον χρήστη. Κακή χρήση ορίζεται η οποιαδήποτε χρήση του πιστοποιητικού πέραν της προβλεπόμενης.

Ο προορισμός χρήσης των πιστοποιητικών καθορίζεται από την Αρχή Πιστοποίησης. Ένα πιστοποιητικό μπορεί να χρησιμοποιηθεί για αυθεντικοποίηση, για εμπιστευτικότητα, ή και για τις δύο υπηρεσίες. Λόγω των νομικών περιορισμών, ή για καθαρά πρακτικούς λόγους, η χρήση των πιστοποιητικών είναι συγκεκριμένη. Για την κρυπτογράφηση μηνυμάτων για παράδειγμα, υπάρχουν νομικοί περιορισμοί που διαφέρουν από χώρα σε χώρα. Οι νομικοί περιορισμοί επικεντρώνονται στο μέγεθος του ιδιωτικού κλειδιού. Αντίθετα, στην περίπτωση της αυθεντικοποίησης με τη χρήση της ψηφιακής υπογραφής, δεν υπάρχει ουσιαστικός περιορισμός. Έτσι, η κρυπτογράφηση με ένα κλειδί το οποίο χρησιμοποιείται για αυθεντικοποίηση ενδεχομένως μπορεί να αποτελέσει αδίκημα.

Ο διαχωρισμός της χρήσης των πιστοποιητικών για αυθεντικοποίηση και εμπιστευτικότητα, συμβάλλει στην καλύτερη διαχείριση των κλειδιών. Στην περίπτωση των πιστοποιητικών αυθεντικοποίησης δεν απαιτείται εφεδρική αποθήκευση του ιδιωτικού κλειδιού, διότι εάν ο χρήστης χάσει το κλειδί του, μπορεί να ζητήσει νέο πιστοποιητικό χωρίς να υπάρξουν πρακτικές συνέπειες. Στην περίπτωση όμως που ο χρήστης χάσει το ιδιωτικό κλειδί του πιστοποιητικού που χρησιμοποιεί για εμπιστευτικότητα, τότε αν δεν υπάρχει εφεδρική αποθήκευση του ιδιωτικού κλειδιού, δεν θα είναι σε θέση να αποκρυπτογραφήσει όλα τα κρυπτοκείμενα που κρυπτογραφήθηκαν με το αντίστοιχο δημόσιο κλειδί. Συνεπώς, η εφεδρική αποθήκευση του ιδιωτικού κλειδιού ενός πιστοποιητικού εμπιστευτικότητας είναι επιθυμητή, αφού συμβάλει στη μείωση του ρίσκου άρνησης υπηρεσίας.

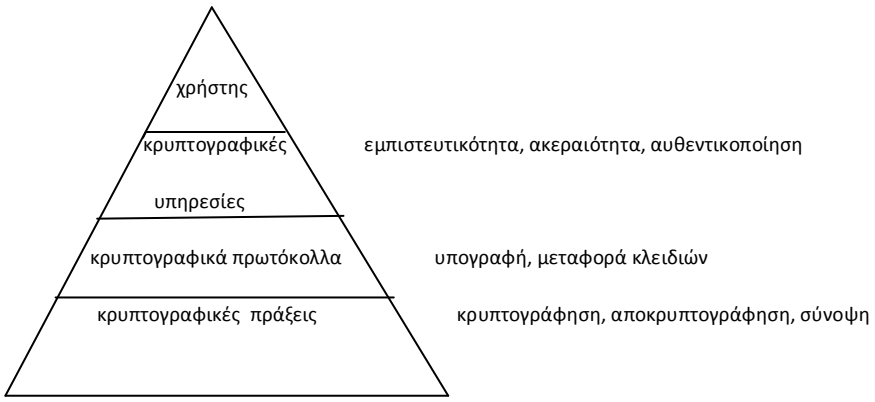
Όταν η Αρχή Πιστοποίησης κρίνει ότι απαιτείται ανάκληση του πιστοποιητικού ενός χρήστη, ανανεώνει τη λίστα ανακληθέντων πιστοποιητικών και τη δημοσιεύει στον κατάλογο που χρησιμοποιεί για τα πιστοποιητικά. Έτσι κατά τον έλεγχο ανάκλησης, ο χρήστης μπορεί να παραλάβει τη λίστα από τον κατάλογο. Σε κρίσιμες εφαρμογές, η Αρχή Πιστοποίησης (ή η υπηρεσία ανάκλησης, αν αυτή είναι διαφορετική από την Αρχή Πιστοποίησης) αναλαμβάνει τη μετάδοση της λίστας απευθείας στους χρήστες, όποτε γίνεται ανανέωση του περιεχομένου της.

Εναλλακτικά, ο χρήστης μπορεί να επικοινωνήσει με την υπηρεσία ανάκλησης για να πληροφορηθεί σχετικά με την εγκυρότητα ενός πιστοποιητικού, μέσω κάποιου πρωτοκόλλου ανάκλησης, όπως το πρωτόκολλο ανάκλησης πιστοποιητικού, OCSP.

6.Πρωτόκολλα κρυπτογράφησης.

6.1.Ορισμός πρωτοκόλλου κρυπτογράφησης.

Ένα κρυπτογραφικό πρωτόκολλο είναι ένα πρωτόκολλο το οποίο υλοποιείται με κρυπτογραφικούς μηχανισμούς. Η ανάγκη χρησιμοποίησης κρυπτογραφικού πρωτοκόλλου φαίνεται στο παρακάτω σχήμα.



Σχήμα 6.1.: Κρυπτογραφικές πράξεις, πρωτόκολλα και υπηρεσίες

Ο χρήστης ενός συστήματος αντιλαμβάνεται την ασφάλεια με τη μορφή των κρυπτογραφικών υπηρεσιών (εμπιστευτικότητα, αυθεντικοποίηση, ακεραιότητα). Οι κρυπτογραφικές υπηρεσίες προσφέρονται με την υλοποίηση των κρυπτογραφικών πράξεων. Οι κρυπτογραφικές πράξεις όμως θα πρέπει να συνδυασθούν και να εκτελεσθούν με συγκεκριμένο τρόπο, προκειμένου να προσφέρουν τις επιθυμητές κρυπτογραφικές υπηρεσίες. Η περιγραφή με την οποία θα δράσουν οι κρυπτογραφικές πράξεις βρίσκεται στο κρυπτογραφικό πρωτόκολλο. Επομένως, ένα κρυπτογραφικό πρωτόκολλο χαρακτηρίζεται από την αυστηρή περιγραφή του τρόπου λειτουργίας και δράσης των

κρυπτογραφικών πράξεων, διότι όπως είδαμε σε πολλές περιπτώσεις, μια μικρή αλλαγή στη λειτουργία μιας κρυπτογραφικής πράξης μπορεί να έχει τεράστιες επιπτώσεις στην ασφάλεια.

Πολλές φορές ένα κρυπτογραφικό πρωτόκολλο παίρνει το όνομα της υπηρεσίας που παρέχει. Έτσι μπορούμε να έχουμε πρωτόκολλα αυθεντικοποίησης, ελέγχου, ακεραιότητας, κοκ.

Ένα πρωτόκολλο έχει τα ακόλουθα χαρακτηριστικά:

• Είναι καθορισμένο εκ των προτέρων. Δηλαδή ο σχεδιασμός ενός πρωτοκόλλου έχει ολοκληρωθεί προτού το πρωτόκολλο χρησιμοποιηθεί.

• Αμοιβαία συμφωνία. Όλα τα μέλη συμφωνούν να εκτελέσουν τα βήματα του πρωτοκόλλου με τη σειρά που υποδεικνύει το πρωτόκολλο.

• Σαφήνεια. Η εκτέλεση όλων των βημάτων του πρωτοκόλλου θα πρέπει να είναι σαφής, έτσι ώστε κανένα από τα μέλη να μην παρερμηνεύσει τα βήματα που του αναλογούν.

• Πληρότητα. Για οποιαδήποτε κατάσταση που μπορεί να βρεθεί οποιοδήποτε μέλος, θα πρέπει να υπάρχουν προκαθορισμένες ενέργειες.

6.2. Ο αντίπαλος.

Εξετάζοντας την ασφάλεια ενός συστήματος στο επίπεδο των πρωτοκόλλων, ή έννοια του αντιπάλου είναι πιο διευρυμένη σε σχέση με τον αντίπαλο που επιτίθεται στις κρυπτογραφικές πράξεις. Το κρυπτογραφικό πρωτόκολλο παρέχει ένα σύνολο κανόνων με το οποίο θα γίνει ανταλλαγή και μετάδοση συγκεκριμένων πληροφοριών, ώστε να προστατευθεί το κάθε μέλος από τον αντίπαλο. Εκτός από τον αντίπαλο που συναντάμε συχνά να επιβλέπει ή να παρεμβάλει στην επικοινωνία μεταξύ της Αλίκης και του Βύρωνα, υπάρχει και ο αντίπαλος που μπορεί να είναι η Αλίκη, ο Βύρων ή και οι δύο. Σε πολλές περιπτώσεις, η απειλή σε μια επικοινωνία είναι ένα ή περισσότερα από τα επικοινωνούντα μέλη. Ένα σύστημα επικοινωνίας δεν μπορεί να θεωρηθεί ασφαλές αν εμπιστεύεται όλα τα μέλη σε ανεξέλεγκτο βαθμό. Όταν η Αλίκη και ο Βύρων εκτελούν κάποια συναλλαγή από την οποία αναδεικνύεται σύγκρουση ενδιαφερόντων, τότε είναι σφάλμα το σύστημα συναλλαγής να εμπιστεύεται ότι η Αλίκη και ο Βύρων θα εκτελέσουν με συνέπεια τη συναλλαγή. Υπάρχει πληθώρα σεναρίων όπου η Αλίκη και ο Βύρων έρχονται σε διαφωνία και ο ένας προσπαθεί να εξαπατήσει τον άλλον. Μερικά παραδείγματα που παραθέσαμε στα

προηγούμενα κεφάλαια είναι η πλαστογραφία της υπογραφής, η απάρνηση παραλαβής ενός μηνύματος και η απάρνηση αποστολής ενός μηνύματος.

Η κατάσταση όπου ένας αντίπαλος καταφέρνει, με κατάλληλο χειρισμό των μηχανισμών ενός πρωτοκόλλου, να καταστήσει το πρωτόκολλο αδύναμο στο να προσφέρει την κρυπτογραφική υπηρεσία, ονομάζεται αποτυχία πρωτοκόλλου (protocol failure).

Ο χειρισμός των μηχανισμών ενός πρωτοκόλλου αναφέρεται στην αυθαίρετη αλλαγή των μηνυμάτων που ανταλλάσσονται μεταξύ των μελών κατά τα διάφορα βήματα εκτέλεσης του πρωτοκόλλου. Συνεπώς, τα κρυπτογραφικά πρωτόκολλα εφαρμόζονται τόσο για την προστασία των επικοινωνούντων μελών από «εξωτερικούς» αντιπάλους, όσο και για την προστασία ενός μέλους, όταν τα άλλα μέλη δεν είναι έντιμα.

6.3. Ανάλυση πρωτοκόλλων κρυπτογράφησης.

Η ανάλυση των κρυπτογραφικών πρωτοκόλλων έχει στόχο τη διαπίστωση ότι το πρωτόκολλο έχει τη δυνατότητα να προσφέρει την υπηρεσία για την οποία είναι σχεδιασμένο να προσφέρει. Στη βιβλιογραφία υπάρχουν διάφορες τεχνικές ανάλυσης των κρυπτογραφικών πρωτοκόλλων, αλλά φυσικά η ανάλυση δεν περιορίζεται στις τεχνικές αυτές. Γενικά οι τεχνικές ανάλυσης συσχετίζουν το πρωτόκολλο με τους πόρους που απαιτείται να έχει ο αντίπαλος, προκειμένου να καταστήσει το πρωτόκολλο αδύναμο να προσφέρει την επιθυμητή υπηρεσία. Οι κυριότερες τεχνικές ανάλυσης πρωτοκόλλων είναι οι εξής:

• ανάλυση με βάση τη θεωρία της πληροφορίας. Η ανάλυση επικεντρώνεται στην πληροφορία που περιέχουν τα μηνύματα που ανταλλάσσουν τα μέλη που εκτελούν το πρωτόκολλο, τόσο μεταξύ τους, όσο και σε τρίτους. Ο αντίπαλος θεωρείται ότι έχει άπειρη υπολογιστική ισχύ, οπότε ένα πρωτόκολλο το οποίο αποδεικνύεται ασφαλές από πλευράς θεωρίας της πληροφορίας, δεχόμαστε ότι είναι ασφαλές άνευ όρων (unconditionally secure).

• ανάλυση με βάση τη θεωρία πολυπλοκότητας. Σύμφωνα με την ανάλυση αυτή, ο αντίπαλος αναλύεται ως προς την υπολογιστική ισχύ και το χρόνο που απαιτείται για να καταρρίψει ένα πρωτόκολλο. Έτσι ένα πρωτόκολλο θεωρείται υπολογιστικά ασφαλές, αν ο αντίπαλος δεν μπορεί να αντεπεξέλθει στους πόρους που απαιτούνται (ισχύς, χρόνος) για να καταρρίψει το πρωτόκολλο.

• αναγωγή σε «δύσκολα» προβλήματα. Η ανάλυση αυτή σχετίζεται με την αναγωγή ασφάλειας του πρωτοκόλλου σε ισοδύναμα δύσκολα προβλήματα. Με

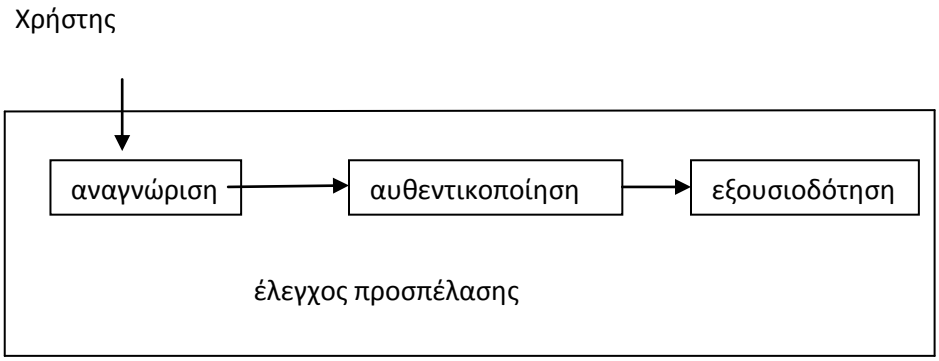
την τεχνική ανάλυσης με αναγωγή, ένα πρωτόκολλο θεωρείται αποδείξιμα ασφαλές (provably secure).

• τυπική ανάλυση. Η τυπική ανάλυση των πρωτοκόλλων περιλαμβάνει εργαλεία ανάλυσης τα οποία είναι κατασκευασμένα ειδικά για τη συγκεκριμένη εργασία. Τα εργαλεία ανάλυσης αποτελούνται από μια γλώσσα ανάλυσης των πρωτοκόλλων και από ένα λογικό μοντέλο. Το πρωτόκολλο μοντελοποιείται και περιγράφεται με τη γλώσσα ανάλυσης και στη συνέχεια εξετάζονται με μια σειρά λογικών κανόνων αν το πρωτόκολλο δύναται να προσφέρει την επιθυμητή υπηρεσία και σε ποιο βαθμό. Ένα από τα πιο επιτυχημένα λογικά μοντέλα ανάλυσης είναι το μοντέλο των Burrows, Abadi και Needham, το οποίο ονομάζεται λογική BAN, από τα αρχικά των δημιουργών του. Η λογική BAN αναλύει το πρωτόκολλο με βάση την πίστη και τη γνώση των μελών για κάποια κατάσταση.

6.4. Πρωτόκολλα αυθεντικοποίησης ταυτότητας

Στον ηλεκτρονικό κόσμο, όταν αναφερόμαστε σε κρυπτογραφικά πρωτόκολλα συνήθως εννοούμε τα πρωτόκολλα που έχουν στόχο την αυθεντικοποίηση της ταυτότητας ενός χρήστη, συστατικού του δικτύου, ή ενός μηνύματος. Επειδή στα δίκτυα υπολογιστών δεν υπάρχει άμεση σύνδεση μεταξύ δύο οντοτήτων αλλά παρεμβάλλονται τρίτοι, η επιβεβαίωση της ταυτότητας με την οντότητα που ανταλλάσουμε μηνύματα είναι από τις υψηλότερες προτεραιότητες. Έτσι, το πρώτο στάδιο επικοινωνίας περιλαμβάνει διαδικασίες αναγνώρισης των επικοινωνούντων μελών, το οποίο υλοποιείται με πρωτόκολλα αυθεντικοποίησης ταυτότητας.

Η αυθεντικοποίηση ταυτότητας είναι ένα τμήμα της διαδικασίας ελέγχου προσπέλασης σε ένα σύστημα. Ο έλεγχος προσπέλασης είναι ακρογωνιαίος λίθος στην ασφάλεια των πληροφοριακών συστημάτων και αποτελείται από τη διαδικασία αναγνώρισης, αυθεντικοποίησης και εξουσιοδότησης, όπως φαίνεται στο σχήμα 6.2.



Σχήμα 6.2.: Στάδια ελέγχου προσπέλασης

Από τις τρεις διαδικασίες του ελέγχου προσπέλασης, το βιβλίο αυτό επικεντρώνεται στη διαδικασία αυθεντικοποίησης, καθώς αυτή συγκεντρώνει τον κύριο όγκο των κρυπτογραφικών μηχανισμών. Ωστόσο, θα παρουσιάσουμε συνοπτικά τα χαρακτηριστικά της αναγνώρισης και της εξουσιοδότησης προκειμένου να δικαιολογήσουμε τις απαιτήσεις της διαδικασίας αυθεντικοποίησης.

6.4.1. Κατηγορίες αναγνώρισης.

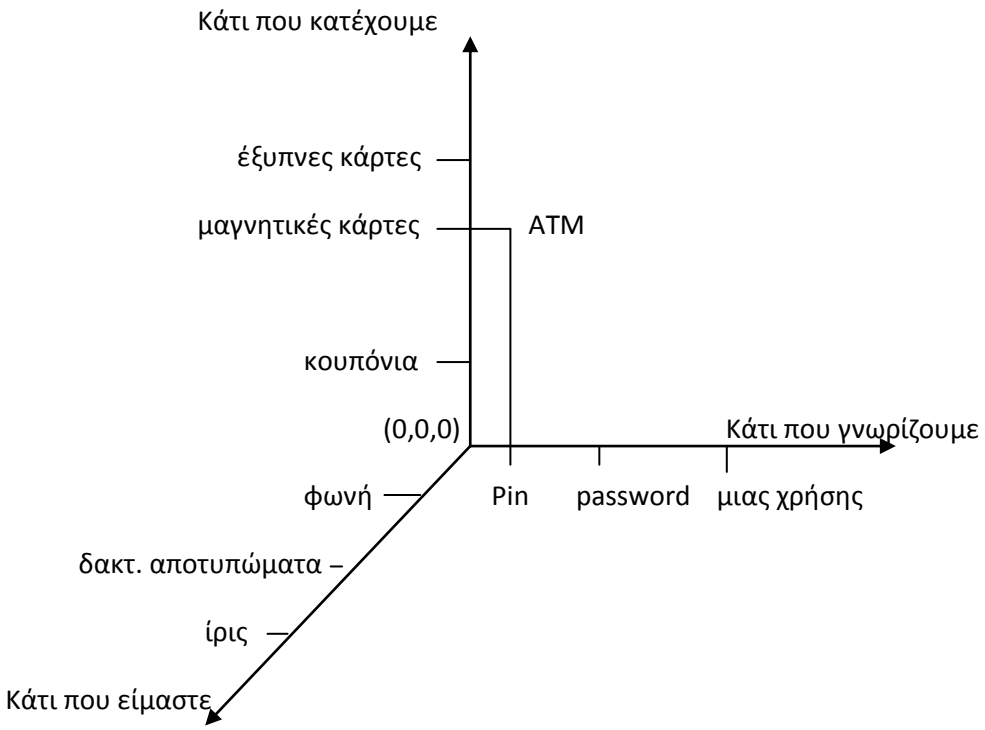
Κατά την αναγνώριση ενός χρήστη συλλέγονται τα πρωτογενή στοιχεία τα οποία περικλείουν πληροφορίες για την ταυτότητα του χρήστη. Τα στοιχεία αυτά αναλύονται σε τρεις διαστάσεις:

• «Κάτι που γνωρίζει ο χρήστης». Τα πρωτογενή στοιχεία της διάστασης αυτής περιλαμβάνουν κωδικούς πρόσβασης, κλειδιά, PIN και γενικά, δεδομένα τα οποία γνωρίζει ο χρήστης και τα οποία παρουσιάζει στο σύστημα είτε με πρωτόκολλο μιας φοράς, είτε με πρωτόκολλο πρόκλησης-απόκρισης.

• «Κάτι που κατέχει ο χρήστης». Τα στοιχεία αυτά περιλαμβάνουν φυσικά αντικείμενα όπως κουπόνια, μαγνητικές κάρτες, ή έξυπνες κάρτες.

• «Κάτι που είναι ο χρήστης». Τα στοιχεία αυτά αποτελούνται από τα προσωπικά χαρακτηριστικά, όπως φωνή, δακτυλικά αποτυπώματα, χαρακτηριστικά προσώπου, κτλ.

Γενικά όσες διαστάσεις αναγνώρισης χρησιμοποιούνται, τόσο ισχυρότερη είναι η αναγνώριση και τόσο μικρότερη είναι η πιθανότητα εσφαλμένης αναγνώρισης. Στο σχήμα φαίνονται οι τρεις διαστάσεις αναγνώρισης, ταξινομημένες κατά αύξουσα διάταξη.



Σχήμα 6.3.: Οι τρείς διαστάσεις της αναγνώρισης

Στο σημείο (0, 0, 0) η αβεβαιότητα αναγνώρισης είναι μέγιστη (δηλαδή δε γνωρίζει τίποτε για την ταυτότητα του χρήστη), ενώ όσο μεγαλώνει η απόσταση από το σημείο αυτό, τόσο μικραίνει η αβεβαιότητα.

Η επιλογή του συνδυασμού των στοιχείων αναγνώρισης εξαρτάται από το ρίσκο που είμαστε διατεθειμένοι να δεχθούμε. Για παράδειγμα, στο σημείο (ATM) του σχήματος λειτουργεί η αναγνώριση των πελατών μιας τράπεζας κατά τη συναλλαγή με ATM. Οι τράπεζες δέχονται ότι το ρίσκο για αναγνώριση με μαγνητική κάρτα και PIN είναι αρκετά μικρό, ώστε να μπορούν να πραγματοποιηθούν συναλλαγές. Η ενδεχόμενη χρήση βιομετρικών τεχνικών (π.χ. αναγνώριση δακτυλικού αποτυπώματος) μειώνει το ρίσκο από τη μια, αλλά από την άλλη αυξάνει την πολυπλοκότητα και τις απαιτήσεις σε τέτοιο βαθμό ώστε το σύστημα θα γινόταν δύσχρηστο. Έτσι το σημείο ισορροπίας βρίσκεται στο σημείο (ATM), το οποίο δέχονται όλες οι τράπεζες. Το PIN έχει μικρό χώρο αναζήτησης. Για παράδειγμα, για ένα τυπικό PIN τεσσάρων ψηφίων, ο χώρος είναι μόνο 10000 κλειδιά.

Αυτό η τράπεζα το αντισταθμίζει εφαρμόζοντας την πολιτική ασφάλειας του «μεγίστου αριθμού προσπαθειών». Έτσι ο χρήστης για παράδειγμα, έχει τη δυνατότητα να δώσει στο σύστημα λάθος PIN μέχρι τρεις φορές. Αν υπερβεί τον

αριθμό εσφαλμένων απαντήσεων, τότε το σύστημα θεωρεί ότι επιχειρείται επίθεση και εκτελεί «διαδικασία χειρισμού περιστατικού ασφάλειας», όπου διακόπτει τη συναλλαγή και δεσμεύει την κάρτα.

6.4.2. Εξουσιοδότηση

Κατά το στάδιο της εξουσιοδότησης, το σύστημα έχει γνώση της ταυτότητας του χρήστη (θεωρούμε ότι τα πρωτόκολλα αυθεντικοποίησης έχουν εκτελέσει με επιτυχία τα καθήκοντά τους), οπότε με βάση κανόνων πρόσβασης ελέγχει αν επιτρέπεται στο χρήστη να έχει πρόσβαση σε κάποιον πόρο του συστήματος και σε ποιο βαθμό. Το ποιο γνωστό μοντέλο εξουσιοδότησης είναι το μοντέλο των ρόλων (role based), όπου μόλις ολοκληρωθεί με επιτυχία η αυθεντικοποίηση της ταυτότητας του χρήστη, το σύστημα του αναθέτει κάποιο ρόλο. Ο ρόλος καθορίζει τους πόρους στους οποίους ο χρήστης έχει πρόσβαση, καθώς και το είδος της προσπέλασης (ανάγνωση, τροποποίηση, διαγραφή, κτλ.).

6.4.3. Αυθεντικοποίηση με κωδικούς πρόσβασης.

Η συντριπτική πλειοψηφία των υπολογιστικών συστημάτων χρησιμοποιούν αυθεντικοποίηση της ταυτότητας όπου η αναγνώριση γίνεται με κωδικούς πρόσβασης. Αν και το ρίσκο είναι αρκετά μεγάλο, παραμένει εντός ανεκτών ορίων για πολλές εφαρμογές.

Ένα απλό πρωτόκολλο αυθεντικοποίησης μεταξύ ενός χρήστη και ενός συστήματος είναι το εξής (θεωρούμε ότι η αυθεντικοποίηση γίνεται από κάποιον server αυθεντικοποίησης):

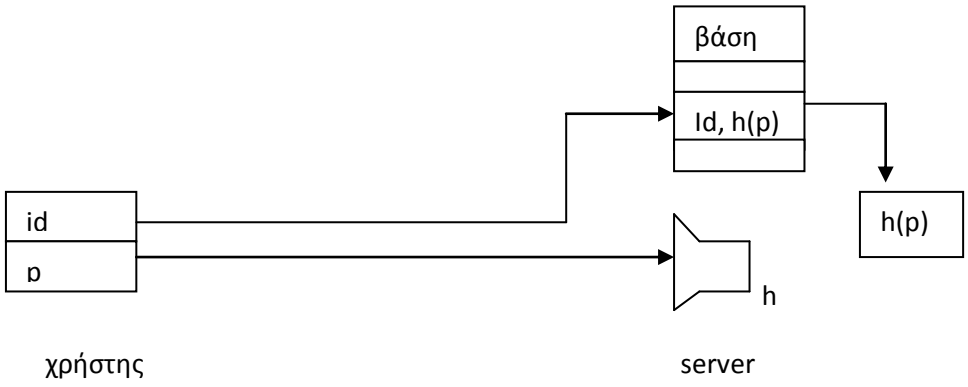
Χρήστης → Server: ID, p

όπου ID, η ταυτότητα (π.χ. όνομα) του χρήστη και p, ο κωδικός πρόσβασης για το χρήστη. Ο server στη συνέχεια ελέγχει τον κωδικό που έλαβε από το χρήστη με αυτόν που έχει αποθηκευμένο στη βάση των κωδικών των χρηστών. Το πρωτόκολλο αυτό έχει μεγάλα μειονεκτήματα. Αρχικά, η μεταφορά του κωδικού από το χρήστη στο server απαιτεί κανάλι εμπιστευτικότητας, διότι ένας υποκλοπέας μπορεί να καταγράψει τον κωδικό του χρήστη και στη συνέχεια να τον χρησιμοποιήσει για να κερδίσει πρόσβαση στο σύστημα. Δεύτερον, προκειμένου να μπορεί ο server να ελέγξει την ορθότητα του κωδικού θα πρέπει να έχει έναν χώρο αποθήκευσης (βάση) των κωδικών πρόσβασης όλων των χρηστών. Αυτό δημιουργεί μεγάλες απαιτήσεις ασφάλειας στη φύλαξη των κωδικών. Στην περίπτωση που ο αντίπαλος καταφέρει να έχει πρόσβαση στη

βάση αυτή, θα καταρρεύσει η υπηρεσία αυθεντικοποίησης του συστήματος. Μια βελτίωση θα ήταν να κρυπτογραφούνταν οι κωδικοί πρόσβασης με κάποιο κύριο κλειδί, οπότε η φύλαξη ενός κλειδιού είναι πρακτικότερη από τη φύλαξη όλης της βάσης.

Ωστόσο, η χρήση ενός κρυπτοσυστήματος για την προστασία της βάσης των κωδικών πρόσβασης επιτρέπει την απόπειρα κρυπτανάλυσης, σε περίπτωση που ο αντίπαλος καταφέρει να αποκομίσει ένα αντίγραφο της βάσης. Στην περίπτωση που ο αντίπαλος ανακαλύψει το κύριο κλειδί, θα έχει αυτόματα πρόσβαση σε όλους τους κωδικούς. Θα ήταν επομένως προτιμότερο σε περίπτωση που ο αντίπαλος έχει στην κατοχή του τη βάση, η απόπειρα κρυπτανάλυσης να του επιφέρει λιγότερο κέρδος. Λιγότερο κέρδος σημαίνει ότι σε μια απόπειρα κρυπτανάλυσης θα ανακαλύψει λίγα ή μόνο ένας από τους κωδικούς πρόσβασης και για κάθε επιπλέον κωδικό θα είναι αναγκασμένος να επαναλάβει την επίθεση από την αρχή.

Η απαίτηση που μόλις περιγράψαμε μπορεί να υλοποιηθεί με τη χρήση μονόδρομης συνάρτησης (σχήμα 6.4) στη θέση του κρυπτοσυστήματος.



Σχήμα 6.4. : Αυθεντικοποίηση με τη χρήση μονόδρομης συνάρτησης

Ο server στη βάση έχει αποθηκευμένες την ταυτότητα του χρήστη και τη σύνοψη του κωδικού πρόσβασης. Το πρωτόκολλο περιλαμβάνει ανταλλαγή των εξής μηνυμάτων:

Χρήστης → Server: ID, p

Server: h(p) = ? [h(p)]′

Ο server δέχεται τον κωδικό πρόσβασης μαζί με την ταυτότητα του χρήστη και στη συνέχεια υπολογίζει τη σύνοψη του κωδικού. Ο έλεγχος γίνεται με βάση τη σύνοψη που υπολογίζει και τη σύνοψη που είναι αποθηκευμένη στη βάση του. Αν οι δύο συνόψεις είναι ίσες, τότε συμπεραίνεται ότι και τα αρχικά μηνύματα (κωδικοί πρόσβασης) είναι ίσα.

Το πλεονέκτημα της χρήσης της μονόδρομης hash έναντι ενός κρυπτοσυστήματος (συμμετρικού ή ασύμμετρου) είναι ότι δεν απαιτούνται καθόλου κλειδιά για τη φύλαξη της βάσης. Ωστόσο, αν και ο αντίπαλος με μια επίθεση δεν έχει άμεσα όλους τους κωδικούς πρόσβασης, μπορεί με μια πλήρη επίθεση εξαντλητικής αναζήτησης να ανακαλύψει τους κωδικούς σταδιακά. Επιπλέον, αν ο αντίπαλος έχει μεγάλη αποθηκευτική ικανότητα, τότε μπορεί να δημιουργήσει λίστες μηνυμάτων με τη σύνοψή τους ως βάση αναφοράς για να επιταχύνει την ανακάλυψη των κωδικών. Αυτό μπορεί να γίνει επειδή οι κωδικοί πρόσβασης προέρχονται από ένα σχετικά μικρό σύνολο μηνυμάτων, αφού χρησιμοποιούνται οι χαρακτήρες πληκτρολογίου.

Προκειμένου να αποφευχθεί η δυνατότητα ανακάλυψης των κωδικών με μία και μόνο εξαντλητική αναζήτηση, εισάγεται μια επιπλέον πληροφορία η οποία εκφράζεται με τη χρήση δεδομένων αλατισμού (salting). Αλατισμός είναι η διαδικασία όπου η σύνοψη του κωδικού πρόσβασης παράγεται από τον κωδικό πρόσβασης και έναν τυχαίο αριθμό, ο οποίος είναι διαφορετικός για κάθε χρήστη.

Έτσι, ο αντίπαλος είναι αναγκασμένος να δημιουργήσει διαφορετικές λίστες- επομένως και διαφορετική αναζήτηση – για κάθε κωδικό πρόσβασης. Ο τυχαίος αριθμός αποθηκεύεται μαζί με τα υπόλοιπα στοιχεία του χρήστη στη βάση και ο server πραγματοποιεί τον ακόλουθο έλεγχο:

Server: $h(s||p) = ? [h(s || p)]'$

S/Key

Το σύστημα αυθεντικοποίησης της ταυτότητας με αλατισμό της σύνοψης επιδιορθώνει τα προβλήματα προστασίας των κωδικών στη μεριά του server. Το πρόβλημα όμως της εμπιστευτικής μεταφοράς του κωδικού από το χρήστη στο server παραμένει. Το σύστημα S/Key είναι ένας αποτελεσματικός τρόπος αποστολής του κωδικού με τον οποίο δεν απαιτείται εμπιστευτικό κανάλι.

Το S/Key παραμένει ένα στάδιο αρχικοποίησης, όπου ο χρήστης επιλέγει ένα τυχαίο μήνυμα r και στη συνέχεια υπολογίζει αναδρομικά τη σύνοψη xn, για κάποιο n:

Χρήστης: $X_n = h(X_{n-1})$,

όπου h( ) μια κρυπτογραφική μονόδρομη hash και x0 = r. Μπορούμε να παρατηρήσουμε ότι λόγω της μονόδρομης συνάρτησης, μόνο ο χρήστης που γνωρίζει την αρχική τιμή x0 έχει τη δυνατότητα να υπολογίσει το xn, για

οποιοδήποτε n. Αυτό όμως σημαίνει ότι αν ανακαλυφθεί ή γίνει γνωστό κάποιο από τα xi για i < n, τότε μπορούν να υπολογισθούν με ευκολία όλα τα xj, για i ≤ j ≤ n.

Το S/Key βασίζεται στις παραπάνω παρατηρήσεις. Έστω ότι n = 100. Κατά τη διαδικασία αρχικοποίησης, ο χρήστης υπολογίζει το x100 και το στέλνει στο server, ο οποίος το αποθηκεύει στη βάση. Επιπλέον, ο χρήστης θέτει έναν μετρητή i στην αρχική τιμή 99.

Κατά το στάδιο της αυθεντικοποίησης, εκτελείται το ακόλουθο πρωτόκολλο:

Χρήστης → Server: xi

Χρήστης: i ← i – 1

Server: έλεγχος xi = ? h(xi-1).

Αν ναι, τότε αποθηκεύει το xi-1 στη θέση του xi και η αυθεντικοποίηση ολοκληρώνεται με επιτυχία.

Σε κάθε εκτέλεση του πρωτοκόλλου ο δείκτης i μειώνεται κατά ένα, υποδεικνύοντας το xi που θα χρησιμοποιηθεί. Όταν ο δείκτης μηδενισθεί, απαιτείται νέα διαδικασία αρχικοποίησης.

Στο σύστημα S/Key, η υποκλοπή του xi κατά την εκτέλεση του πρωτοκόλλου αυθεντικοποίησης δεν παρέχει ιδιαίτερο πλεονέκτημα στον αντίπαλο, καθώς η τιμή αυτή χρησιμοποιείται μόνο μια φορά. Επιπλέον, ο server που έχει αποθηκευμένο στη βάση το xi, δε γνωρίζει το xi-1 παρά μόνο όταν σταλεί από το χρήστη.

Έτσι μια πιθανή κλοπή της βάσης δε δίνει μεγάλη πληροφορία στον αντίπαλο. Η ασφάλεια του συστήματος στηρίζεται στην κρυπτογραφική ισχύ της μονόδρομης συνάρτησης, η οποία θα πρέπει να είναι ανθεκτική σε συγκρούσεις και το μέγεθος της σύνοψης να είναι αρκετά υψηλό. Μια ενδεικτική τιμή του μεγέθους της σύνοψης είναι 160 bits.

6.4.4. Αυθεντικοποίηση με ψηφιακές υπογραφές

Σε μια υποδομή δημόσιου κλειδιού, η αυθεντικοποίηση μπορεί να πραγματοποιηθεί με τη χρήση των ψηφιακών πιστοποιητικών. Η βάση του server σε αυτήν την περίπτωση θα έχει τα πιστοποιητικά όλων των χρηστών, από όπου ο server μπορεί να αναζητήσει το πιστοποιητικό του χρήστη.

Έστω ότι η Αλίκη επιθυμεί πρόσβαση στο σύστημα. Ο server γνωρίζει το δημόσιο της κλειδί, επομένως μπορεί να χρησιμοποιηθεί πρωτόκολλο πρόκλησης απόκρισης, ώστε να εξακριβωθεί αν η Αλίκη κατέχει το ιδιωτικό κλειδί της. Αυτό μπορεί να πραγματοποιηθεί με το ακόλουθο πρωτόκολλο:

Αλίκη → Server: ID_A

Server→ Αλίκη: c

Αλίκη → $r=d_{kdA}(C)$

Server: $e_{keA}(r) = c$

όπου:

ID_A η ταυτότητα της Αλίκης,

c το μήνυμα-πρόκληση του server,

r το μήνυμα-απόκριση της Αλίκης

e ( ) ,d( ) η πράξη κρυπτογράφησης και αποκρυπτογράφησης,

kdA, keA το ιδιωτικό και το δημόσιο κλειδί της Αλίκης, αντίστοιχα.

Αν υποθέσουμε ότι μόνον η Αλίκη γνωρίζει το ιδιωτικό της κλειδί, τότε μόνον η Αλίκη έχει τη δυνατότητα να βρει ένα μήνυμα r τέτοιο ώστε η κρυπτογράφηση αυτού με το δημόσιο κλειδί της να δίνει το προεπιλεγμένο μήνυμα c.
Από πρακτική πλευρά, ένα σύστημα ψηφιακών υπογραφών χρησιμοποιεί την αναγνώριση του «κάτι που κατέχει» ο χρήστης. Όπως είδαμε σε προηγούμενη ενότητα η ασύμμετρη κρυπτογραφία απαιτεί πολύ μεγαλύτερα κλειδιά από αυτά που απαιτεί η συμμετρική κρυπτογραφία. Επιπλέον τα ασύμμετρα κλειδιά γεννιούνται από μαθηματικούς μετασχηματισμούς, με αποτέλεσμα τα κλειδιά αυτά να μην είναι φιλικά προς το χρήστη. Έτσι, από τη στιγμή που είναι δύσκολο να απομνημονευθούν τα ασύμμετρα κλειδιά, ο χρήστης υποχρεώνεται να τα φυλάξει σε αποθηκευτικές συσκευές. Ένα ιδιωτικό κλειδί μπορεί να αποθηκευθεί σε σκληρό ή αποσπώμενο δίσκο του υπολογιστή ως λογισμικό κουπόνι (software token), σε μαγνητική κάρτα ή σε έξυπνη κάρτα. Από τις εναλλακτικές αυτές, η ασφαλέστερη είναι η αποθήκευση σε έξυπνη κάρτα, διότι η έξυπνη κάρτα έχει τη δυνατότητα εκτέλεσης της κρυπτογραφικής πράξης με αποτέλεσμα να μην χρειάζεται το ιδιωτικό κλειδί να διατεθεί εκτός της κάρτας.

Αμοιβαία αυθεντικοποίηση

Έστω ότι η Αλίκη και ο Βύρων επιθυμούν να αυθεντικοποιήσουν ο ένας την ταυτότητα του άλλου με τη χρήση των ψηφιακών υπογραφών. Ένα μη ασφαλές πρωτόκολλο είναι το εξής:

Αλίκη → Βύρων: keA
Βύρων → Αλίκη: keB, c_B
Αλίκη → Βύρων: $r_B = d_{kdA}(c_B)$, c_A
Βύρων → Αλίκη: $r_A = d_{kdB}(c_A)$

όπου c_A, c_B η πρόκληση της Αλίκης και του Βύρωνα αντίστοιχα και r_A και r_B οι αποκρίσεις στις προκλήσεις. Το πρωτόκολλο ολοκληρώνεται με επιτυχία και από τις δύο πλευρές όταν επιβεβαιώσουν ότι οι αποκρίσεις ταιριάζουν κρυπτογραφικά στις προκλήσεις.

Το παραπάνω πρωτόκολλο της αμοιβαίας αυθεντικοποίησης δεν είναι ασφαλές διότι υποπίπτει σε επίθεση του ενδιάμεσου ατόμου. Ο αντίπαλος ο οποίος παρεμβάλλεται στο κανάλι επικοινωνίας της Αλίκης και του Βύρωνα, ελέγχει όλα τα μηνύματα που διακινούνται και συνεπώς μπορεί να αντικαταστήσει τα δημόσια κλειδιά με το δικό του, πλαστογραφώντας με τον τρόπο αυτό την Αλίκη στον Βύρωνα και αντίστροφα.

Μια τροποποίηση του πρωτοκόλλου είναι η πρόκληση να είναι προκαθορισμένα μηνύματα, γνωστά στην Αλίκη και στον Βύρωνα. Έτσι τα c_A, c_B δεν στέλνονται σαν απλό κρυπτοκείμενο, αλλά κρυπτογραφημένα με το ιδιωτικό κλειδί του αντίστοιχου μέλους. Αν και το πρωτόκολλο αμοιβαίας αυθεντικοποίησης με προκαθορισμένα μυστικά είναι και αυτό ευάλωτο στην επίθεση του ενδιάμεσου ατόμου, μια μικρή τροποποίηση στη μετάδοση των μηνυμάτων μπορεί να αποτρέψει τη συγκεκριμένη επίθεση. Η τροποποίηση προτάθηκε από τους Rivest και Shamir και το πρωτόκολλο που προέκυψε το ονόμασαν **πρωτόκολλο συναρμογής** (inter-lock protocol) το οποίο έχει στόχο τη μείωση της πιθανότητας επιτυχίας επίθεσης του ενδιάμεσου ατόμου. Το πρωτόκολλο συναρμογής έχει ως εξής:

Αλίκη → Βύρων: keA
Βύρων → Αλίκη: keB
Αλίκη: $r_B = d_{kdA}(c_B) = r^L_B \,||\, r^L_B$
Αλίκη → Βύρων: r^L_B
Βύρων: $r_A = d_{kdB}(c_A) = r^L_A \,||\, r^R_B$
Βύρων → Αλίκη: r^L_A
Αλίκη → Βύρων: r^R_B
Βύρων → Αλίκη: r^R_A

Με άλλα λόγια, η Αλίκη και ο Βύρων υπογράφουν αντίστοιχα τα κοινά μυστικά c_A, c_B, αλλά στη συνέχεια χωρίζουν την υπογραφή σε δύο τμήματα και στέλνουν τα τμήματα χωριστά. Η Αλίκη στέλνει το αριστερό τμήμα της υπογραφής της, στη συνέχεια ο Βύρων στέλνει το αριστερό τμήμα της υπογραφής του και η διαδικασία επαναλαμβάνεται με τα δεξιά τμήματα. Ο παραλήπτης ο οποίος έχει μόνο ένα τμήμα της υπογραφής, δεν έχει τη δυνατότητα να εκτελέσει την απαιτούμενη κρυπτογραφική πράξη. Έτσι το ενδιάμεσο άτομο όταν θα έχει στην κατοχή του και τα δύο τμήματα, θα είναι πια αργά.

7. Νομική ευθύνη για τις ψηφιακές υπογραφές.

7.1.Υπηρεσίες Παροχών Πιστοποίησης και νομική ευθύνη.

Μια αρχή πιστοποίησης (certification authority) CA είναι υπεύθυνη για την υπογραφή πιστοποιητικών. Για να παρέχεται οποιαδήποτε αξιοπιστία σε αυτή την υπογραφή από την πλευρά της αρχής πιστοποίησης, θα πρέπει αυτή να ασκεί ένα είδος ελέγχου στο πιστοποιητικό πριν το υπογράψει.
Γενικά, οι δημόσιες αρχές πιστοποίησης διενεργούν αυτό τον έλεγχο ή τον αναθέτουν στις αρμόδιες αρχές εγγραφής τους. Ωστόσο προσπαθούν να αποποιηθούν των ευθυνών τους σε περίπτωση που ο απαραίτητος έλεγχος δεν διενεργηθεί αποτελεσματικά.

Οι ιδιωτικές αρχές πιστοποίησης , δηλαδή αυτές που λειτουργούν μόνο στα πλαίσια εντός ενός οργανισμού, ασχολούνται συχνότερα με πιστοποιητικά πελατών.
Πρέπει να σημειωθεί ότι ένας από τους ελέγχους που οφείλει να διενεργήσει μια αρχή Πιστοποίησης είναι ο έλεγχος εάν ο αιτών είναι κάτοχος του ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί του πιστοποιητικού. Αυτό επιτυγχάνεται μέσω μιας υπογραφής με αίτημα του πιστοποιητικού και όχι μέσω της παραγωγής του ιδιωτικού κλειδιού από την ίδια την αρχή πιστοποίησης για λογαριασμό του αιτούντα.

Αν η ίδια η αρχή πιστοποίησης παράγει ένα ζεύγος κλειδιών και το αποδώσει στον αιτούντα, μπορεί να διασφαλιστεί ότι εκείνη ακριβώς τη στιγμή ο αιτών έχει στην κατοχή του το ιδιωτικό κλειδί και ότι κανένας άλλος εκτός από την αρχή πιστοποίησης δεν έχει πρόσβαση σε αυτό. Αυτό εξυπηρετεί την αρχή πιστοποίησης αφού με τον τρόπο αυτό μπορεί να πιστοποιήσει ότι ο αιτών είναι το μόνο πρόσωπο με το κλειδί στην κατοχή του. Ωστόσο αυτό δεν εξυπηρετεί τον αιτούντα, ο οποίος θα πρέπει να θεωρεί το γεγονός της πρόσβασης της αρχής πιστοποίησης στο κλειδί ως σημαντική αδυναμία της ασφάλειας. Από την άλλη πλευρά, αν ο αιτών επιμείνει στη δημιουργία του ιδιωτικού κλειδιού από τον ίδιο και στην απόδοση μόνο του δημοσίου κλειδιού του στην αρχή πιστοποίησης, η

αρχή πιστοποίησης δεν είναι σε θέση να γνωρίζει με βεβαιότητα μετά την απόδοση του κλειδιού στον αιτούντα, ακόμη και στην περίπτωση που αυτή δημιουργούσε το ζεύγος κλειδιών, οπότε το κέρδος ασφάλειας σε αυτή την περίπτωση είναι ελάχιστο.

Η παροχή υπηρεσιών πιστοποίησης ηλεκτρονικών υπογραφών δεν υπόκειται σε καθεστώς αδειοδότησης και άρα μπορεί οποιοδήποτε φυσικό ή νομικό πρόσωπο να λειτουργήσει ως πάροχος υπηρεσιών πιστοποίησης και να εκδώσει αναγνωρισμένα ή όχι πιστοποιητικά. Μόνη υποχρέωση ενός παρόχου υπηρεσιών πιστοποίησης προς την εποπτεύουσα αρχή ΕΕΤΤ είναι η δήλωση της έναρξης λειτουργίας και η εγγραφή του στο σχετικό Μητρώο Παρόχων Υπηρεσιών Πιστοποίησης καθώς και η αποστολή Ετήσιων εκθέσεων σχετικά με τη λειτουργία τους.

Για να εκδόσει ένας πάροχος υπηρεσιών πιστοποίησης «αναγνωρισμένα πιστοποιητικά προς το κοινό» θα πρέπει να ικανοποιεί τις απαιτήσεις ασφαλείας, αξιοπιστίας και παροχής ολοκληρωμένων υπηρεσιών που επιβάλλονται στους όρους της σχετικής ευρωπαϊκής οδηγίας 99/93/ΕΚ. Ένας πάροχος υπηρεσιών πιστοποίησης που εκδίδει αναγνωρισμένα πιστοποιητικά έχει επίσης τη δυνατότητα να διαπιστευθεί εθελοντικά ως προς το επίπεδο των παρεχόμενων υπηρεσιών του και τη συμόρφοσή του σε καθιερωμένα πρότυπα (standards). Με την εθελοντική διαπίστευση ο πάροχος υπηρεσιών πιστοποίησης αποκτά «δικαίωμα επίκλησης» της συγκεκριμένης διαπίστευσής του προς τρίτους, υποβάλλεται όμως σε περαιτέρω υποχρεώσεις και ελέγχους που συνήθως επιβάλει ο σχετικός φορέας.

Κάθε πάροχος υπηρεσιών πιστοποίησης με την έκδοση οποιουδήποτε είδους πιστοποιητικού, αναλαμβάνει ευθύνες τόσο έναντι του συνδρομητή του, όσο και έναντι κάθε τρίτου προσώπου που ευλόγως βασίζεται στο πιστοποιητικό του. Οι ευθύνες αυτές κρίνονται καταρχήν, κατά τις γενικές διατάξεις περί ευθύνης και τις διατάξεις περί προστασίας των καταναλωτών, ενώ προσδιορίζονται ειδικότερα στους συμβατικούς όρους που συμφωνούνται με το συνδρομητή της πιστοποίησης, καθώς και τους όρους τους οποίους οφείλει να αποδεχθεί οποιοσδήποτε τρίτος, πριν αποφασίσει να βασιστεί στα περιεχόμενα των πιστοποιητικών και των συναφών υπηρεσιών του Παρόχου Υπηρεσιών πιστοποίησης.

Σε περίπτωση όμως που ο πάροχος υπηρεσιών πιστοποίησης εκδίδει αναγνωρισμένα πιστοποιητικά προς το κοινό, η ευθύνη του έναντι κάθε αποδέκτη των εκδιδόμενων πιστοποιητικών του προκύπτει απευθείας από το νόμο και αφορά την «ακρίβεια στην πληρότητα των πληροφοριών» που αναγράφονται σε αυτά καθώς και τη «διαβεβαίωση της κατοχής των σχετικών κλειδιών» από τα πιστοποιούμενα υποκείμενα. Το ίδιο συμβαίνει και ως προς την παράλειψη του παρόχου υπηρεσιών πιστοποίησης να καταγράψει και να δημοσιοποιήσει την

τυχόν ανάκληση ενός «αναγνωρισμένου πιστοποιητικού» καθώς και ως προς τη μη σωστή λειτουργία των σχετικών κρυπτογραφικών κλειδιών του υποκειμένου.

Η ευθύνη του παρόχου Υπηρεσιών Πιστοποίησης έναντι των τρίτων μπορεί να περιοριστεί σε συγκεκριμένα όρια και για συγκεκριμένες αρνήσεις του πιστοποιητικού, εφόσον όμως οι περιορισμοί αυτοί προσδιορίζονται ρητά στην ‘’Πολιτική Πιστοποιητικού’’(certificate Polity) που διέπει το συγκεκριμένο πιστοποιητικό και είναι εμφανείς και αναγνωρίσιμο σε κάθε αποδέκτη του. Ο πάροχος Υπηρεσιών Πιστοποίησης μπορεί να απαλλαχθεί εντελώς από την ευθύνη εκ του νόμου εάν αποδείξει ότι η σχετική πράξη ή παράλειψή του προήλθε από αμέλεια.

Οι βασικές υπηρεσίες οι οποίες προσφέρει υποχρεωτικά ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορούν να διακριθούν σε οργανωμένες ξεχωριστές λειτουργικές οντότητες και συγκεκριμένα σε:

-Υπηρεσία εγγραφής/καταχώρησης (Registrations Authority) RA

-Υπηρεσία έκδοσης πιστοποιητικών (certification Authority) CA που εκδίδει και υπογράφει τα τελικά πιστοποιητικά των συνδρομητών

-Υπηρεσία Διαχείρισης Αιτημάτων Ανάκλησης (Revocation Management Service) η οποία υποδέχεται, ελέγχει (σε συνεργασία με την Υπηρεσία Εγγραφής) και διεκπεραιώνει τα αιτήματα σε 24ωρη βάση 7 ημέρες την εβδομάδα για ανάκληση, παύση ή επανενεργοποίηση των πιστοποιητικών, συνεργαζόμενη με την «υπηρεσία έκδοσης πιστοποιητικών» για την κατάλληλη ψηφιακή υπογραφή των σχετικών εκδιδόμενων ‘Λιστών ανακληθέντων πιστοποιητικών’ (Certificate Revocation Lists).

-Υπηρεσία δημοσίευσης (Dissemination and Revocation Status Service) η οποία αναλαμβάνει τη δημοσίευση των κειμένων τεκμηρίωσης των υπηρεσιών του Παρόχου Υπηρεσιών Πιστοποίησης, τη δημοσίευση των καταλόγων και των λιστών ανακληθέντων πιστοποιητικών, καθώς και τις σχετικές ενημερώσεις ή κοινοποιήσεις προς τους συνδρομητές του Παρόχου Υπηρεσιών Πιστοποίησης.

Εκτός από τις παραπάνω υποχρεωτικές υπηρεσίες, ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορεί επίσης να παρέχει προαιρετικά και υπηρεσίες ‘προμήθειας- προετοιμασίας φορέα’ πχ (έξυπνη κάρτα ή usb token) για τους συνδρομητές (subject device Provision Service), Υπηρεσίες χρονοσήμανσης ηλεκτρονικών εγγράφων (time stamping Authority), υπηρεσίες ‘ασφαλούς αρχειοθέτησης’ εγγράφων Notary Services κλπ.

Για ένα πάροχο υπηρεσιών πιστοποίησης είναι επιτρεπτό να εκχωρίσει σε τρίτους (outsourcing) τη διεκπεραίωση μέρους ή ακόμη και του συνόλου των παραπάνω παρεχόμενων υπηρεσιών του.

Εφόσον όμως ο πάροχος εξακολουθεί να αναγράφεται στα εκδιδόμενα πιστοποιητικά ως εκδότης, τότε διατηρείται ακέραια η ευθύνη του έναντι των

τρίτων, οποιαδήποτε πράξη ή παράλειψη που αναφέρεται στην οδηγία και προξενεί ζημιά σε συνδρομητές ή τρίτους.

Σύμφωνα με πληροφορίες που προέρχονται από το ICRI (Interdisciplinary centre for low and Information Technology) ηγέτης στο χώρο της παροχής πιστοποιητικών στην ελληνική αγορά φαίνεται να είναι η εταιρία VeriSign η οποία δραστηριοποιείται μέσω της ελληνικής εταιρίας Adacom.

7.2.Νομικό πλαίσιο για τις ψηφιακές υπογραφές.

Η νομική αναγνώριση των ψηφιακών υπογραφών σε διεθνές επίπεδο, ξεκίνησε από τα μέσα της προηγούμενης δεκαετίας με την θέσπιση σχετικών νόμων σε διάφορα κράτη.

Μπορούμε να διακρίνουμε δύο διαφορετικές νομικές προσεγγίσεις:

- Την αναλυτική προσέγγιση με την οποία μόνο συγκεκριμένες τεχνολογικές μέθοδοι, οι οποίες ικανοποιούν συγκεκριμένα κριτήρια ασφάλειας και αξιοπιστίας, αναγνωρίζονται ως νομικά ισότιμες με τις ιδιόχειρες υπογραφές.
- Την μινιμαλιστική προσέγγιση όπου κάθε αξιόπιστη τεχνολογική μέθοδος απόδειξης της προέλευσης και της αυθεντικότητας των ψηφιακών δεδομένων πρέπει να γίνεται νομικώς αποδεκτή.

Οι ηλεκτρονικές υπογραφές αποτελούν σημαντικό τμήμα της δημιουργίας ενός περιβάλλοντος εμπιστοσύνης στο οποίο το ηλεκτρονικό εμπόριο ενθαρρύνεται και προωθείται. Επίσης παρέχουν στους πολίτες νέες και αποτελεσματικές μεθόδους για επικοινωνία με τους κυβερνητικούς φορείς.

Πληροφορίες για τα νομικά ζητήματα των ηλεκτρονικών υπογραφών παρέχονται από την Τράπεζα Νομικών Πληροφοριών Ηλεκτρονικού Εμπορίου του Εμπορικού και Βιομηχανικού Επιμελητηρίου Αθηνών.

Η Ευρωπαϊκή Ένωση με την οδηγία 99/93/ΕΚ του Ευρωπαϊκού κοινοβουλίου και του συμβουλίου της 13^{ης} Δεκεμβρίου 1999 « Σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές» ακολούθησε μια μικτή προσέγγιση δύο επιπέδων η οποία συνδυάζει και τις δύο παραπάνω κατευθύνσεις.

Έτσι η συγκεκριμένη Ευρωπαϊκή Οδηγία αναγνωρίζει ως ηλεκτρονικές υπογραφές όλα τα δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε ή λογικά συσχετιζόμενα με άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως απόδειξη της γνησιότητας. Ο ορισμός αυτός καλύπτει κάθε ηλεκτρονική μέθοδο απόδειξης της προέλευσης των δεδομένων από τις πιο απλές (π.χ. απλή αναγραφή του ονόματος του συντάξαντα στο τέλος μιας ηλεκτρονικής επιστολής) ως τις πιο σύνθετες

(π.χ. προηγμένες μέθοδοι κρυπτογράφησης δεδομένων, χρήση βιομετρικών στοιχείων κ.λ.π.) ανεξάρτητα δηλαδή από τον βαθμό τεχνικής ασφάλειας που παρέχουν.

Από την κανονιστική πλευρά η Οδηγία διακρίνει μια κατηγορία ηλεκτρονικών υπογραφών αποκαλούμενες ως « αναγνωρισμένες ηλεκτρονικές υπογραφές» - στην οποία κατηγορία αποδίδει πλήρη και άμεση νομική ισοδυναμία με τις ιδιόχειρες υπογραφές.

Στην κατηγορία ανήκουν όλες οι: «προηγμένες ηλεκτρονικές υπογραφές» που βασίζονται σε «αναγνωρισμένο ποιστοποιητικό» και δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής.

Οι νομικές προεκτάσεις της εφαρμογής της παρούσας Οδηγίας καθώς και οι πρακτικές εφαρμογές των ηλεκτρονικών στα κράτη- μέλη παρουσιάζονται αναλυτικά σε μελέτη για την αντίστοιχη Ευρωπαϊκή Επιτροπή το 2003.

Ως προηγμένες ηλεκτρονικές υπογραφές η Οδηγία προσδιορίζει τις ηλεκτρονικές υπογραφές που ικανοποιούν τις εξής απαιτήσεις:

1) συνδέονται μονοσήματα με τον υπογράφοντα
2) δημιουργούνται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπο τον αποκλειστικό του έλεγχο.
3) είναι ικανές να ταυτοποιήσουν τον υπογράφοντα.
4) συνδέονται με τα δεδομένα στα οποία αναφέρονται κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε αλλοίωση στα εν λόγω δεδομένα.

Οι συγκεκριμένες απαιτήσεις μπορούν να ικανοποιηθούν σήμερα μόνο με τη χρήση της τεχνολογίας της ασύμμετρης κρυπτογραφίας η οποία κάνει χρήση ιδιωτικών και δημοσίων κρυπτογραφικών κλειδιών που χρησιμοποιούνται συμπληρωματικά το ένα προς το άλλο για την παραγωγή και την επαλήθευση της ηλεκτρονικής υπογραφής.

Ως αναγνωρισμένο πιστοποιητικό ορίζεται από την Οδηγία η ηλεκτρονική βεβαίωση που εκδίδεται από κάποιο Πάροχο Υπηρεσιών Πιστοποίησης και η οποία συνδέει μονοσήμαντα τα δεδομένα επαλήθευσης μιας υπογραφής με συγκεκριμένο φυσικό πρόσωπο τηρώντας κάποιους βασικούς όρους.

Τέλος ως ασφαλής διάταξη δημιουργίας της υπογραφής ορίζεται διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή του ιδιωτικού κλειδιού από τον υπογράφοντα και το οποίο ν διασφαλίζει την αξιοπιστία της δημιουργίας της υπογραφής στο παράρτημα 3 της οδηγίας.

Η οδηγία προβλέπει την ελεύθερη παροχή υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής απαγορεύοντας οποιοδήποτε σύστημα αδειοδότησης της λειτουργίας των Παρόχων Υπηρεσιών πιστοποίησης προσδιορίζοντας όμως τις προϋποθέσεις λειτουργίας και την ευθύνη των παρόχων Υπηρεσιών

Πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά προς το κοινό. Παράλληλα προβλέπει τη δυνατότητα «εθελοντικής διαπίστευσης» των Παρόχων Υπηρεσιών Πιστοποίησης καθώς και τη διαδικασία «διαπίστωσης» της συμφόρησης των «προϊόντων ηλεκτρονικών υπογραφών» με τις απαιτήσεις ασφάλειας και αξιοπιστίας της οδηγίας από αρμόδιους φορείς.

Στην Ελλάδα η πρώτη νομοθετική πρόβλεψη για «ψηφιακές υπογραφές» γίνεται από το άρθρο 14 του νόμου 2672 /98 όπου παρέχεται μια αρχική αλλά περιορισμένη αναγνώρισή τους σε διαδικασίες δημοσίου τομέα. Συγκεκριμένα το άρθρο 14 του νόμου 2672/98 προβλέπει τη χρήση της ηλεκτρονικής υπογραφής και κατά τη διακίνηση εγγράφων μεταξύ υπηρεσιών του δημοσίου των Ν.Π.ΔΔ και των Ο.Τ.Α. ή μεταξύ αυτών και των ενδιαφερόμενων φυσικών προσώπων, νομικών προσώπων ιδιωτικού δικαίου και ενώσεων προσώπων με τηλεομοιοτυπία και ηλεκτρονικό ταχυδρομείο.

Ακολούθησε το πλαίσιο δικαίου 150/2001 το οποίο εναρμόνησε το εθνικό μας δίκαιο με την παραπάνω οδηγία και καθόρισε την Εθνική επιτροπή Τηλεπικοινωνιών και Δικτύων ΕΕΤΤ ως αρμόδια αρχή για την εποπτεία των εγκατεστημένων στη Ελλάδα Παρόχων Υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής καθώς και για τη λειτουργία μηχανισμών «εθελοντικής διαπίστευσης» των παρόχων υπηρεσιών πιστοποίησης και «διαπίστωσης» της συμμόρφωσης των «προϊόντων ηλεκτρονικής υπογραφής».

Τον Οκτώβριο του 2002 κατ' εξουσιοδότηση του νόμου 2672/98 εκδόθηκε το πλαίσιο δικαίου 342/02 το οποίο προσδιορίζει περαιτέρω κάποιους όρους για τη διακίνηση ψηφιακά υπογεγραμμένων «μηνυμάτων ηλεκτρονικού ταχυδρομείου» στις επικοινωνίες δημοσίου τομέα.

Τέλος, στο πλαίσιο άσκησης των σχετικών αρμοδιοτήτων της, η ΕΕΤΤ έχει εκδώσει έναν γενικό «Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής», καθώς και τρεις Κανονισμούς σχετικά με την Εθελοντική Διαπίστευση των ΠΥΠ, την Διαπίστωση (της συμμόρφωσης με τις απαιτήσεις της Οδηγίας) βασικών προϊόντων ηλεκτρονικής υπογραφής και τον ορισμό των φορέων που θα προβαίνουν σε σχετικούς ελέγχους και διαπιστεύσεις για λογαριασμό της ΕΕΤΤ.

7.3.Εφαρμογές ηλεκτρονικών υπογραφών και πιστοποιητικών.

Σε διεθνές επίπεδο η χρήση των ηλεκτρονικών υπογραφών και των ηλεκτρονικών πιστοποιητικών ήδη πλαισιώνει και παρέχει υψηλότερα επίπεδα ασφαλείας σε συναλλαγές διαφόρων τύπων όπως:

- Τυποποιημένες εφαρμογές ηλεκτρονικών συναλλαγών, όπως η ηλεκτρονική ανταλλαγή δεδομένων (electronic data interchange – EDI)
- Ηλεκτρονικά τιμολόγια που ανταλλάσσονται σε μορφή άλλη από EDI
- Ηλεκτρονική ψηφοφορία
- Ηλεκτρονικές δημόσιες προμήθειες
- Συστήματα ηλεκτρονικών πληρωμών (π.χ. πιστωτικές κάρτες mastercard, visa)
- Ηλεκτρονικά διαβατήρια και ηλεκτρονικές ταυτότητες που συνήθως φέρουν ενσωματωμένα βιομετρικά στοιχεία (π.χ. φωτογραφία, δακτυλικά αποτυπώματα κ.λ.π.) του κατόχου τους.
- Υπηρεσία ασφαλούς ηλεκτρονικού ταχυδρομείου
- Συστήματα υπογραφής αυθεντικότητας διακινούμενου λογαριασμού (microsoft authenticode)
- Πιστοποίηση ταυτότητας εξυπηρετητών διαδικτύου (web servers)

Στην Ευρωπαϊκή Ένωση, εκτός από το πλήθος άτυπων εφαρμογών στις τηλεπικοινωνίες, τραπεζικές εφαρμογές, εμπόριο κ.λ.π. έχουν θεσμοθετηθεί και βρίσκονται ήδη σε λειτουργία τυπικές υπογραφές ηλεκτρονικών υπογραφών, οι προϋποθέσεις των οποίων πηγάζουν από το νόμο. Τα ηλεκτρονικά δελτία ταυτότητας σε χώρες όπως η Ιταλία, η Φιλανδία κ.λ.π. τα οποία χρησιμοποιούν την τεχνολογία σε συνδυασμό με τις έξυπνες κάρτες, αποτελούν παράδειγμα τέτοιων εφαρμογών.

Άλλος ένας τομέας εφαρμογής ηλεκτρονικών υπογραφών στην Ευρωπαϊκή ένωση είναι τα ηλεκτρονικά τιμολόγια, τα οποία σύμφωνα με την Ευρωπαϊκή οδηγία 01/115, εφ-όσων φέρουν ηλεκτρονική υπογραφή μπορούν να γίνονται αποδεκτά από τις αρμόδιες αρχές των κρατών μελών.

Άλλη εφαρμογή αποτελούν οι ηλεκτρονικές δημόσιες προμήθειες στο πλαίσιο των σχετικών οδηγιών της Ευρωπαϊκής ένωσης. Επίσης θεσμικά όργανα της Ευρωπαϊκής ένωσης, όπως η υπηρεσία δημοσιεύσεων σχεδιάζουν τη χρήση των ηλεκτρονικών υπογραφών για τα έγγραφα που εκδίδουν σε ηλεκτρονική μορφή (π.χ. την εφημερίδα ευρωπαϊκών Κοινοτήτων, τα περιεχόμενα των νομικών βάσεων δεδομένων CELEX, EUR-Lex & OEIL).

Στην Ελλάδα μια από τις πρώτες εφαρμογές έγκυρης ηλεκτρονικής υπογραφής επίσημων εγγράφων η οποία λειτουργεί ήδη από το 2002 είναι το σύστημα ασφαλούς ηλεκτρονικής επικοινωνίας του Χρηματιστηρίου Αθηνών με τις εισηγμένες σε αυτό εταιρίες. Το σύστημα αυτό ονομάζεται ΕΡΜΗΣ ή HERMES (Hellenic Exchange Remote Messaging Services) και βασίζεται στις ψηφιακές υπογραφές εξουσιοδοτημένων φυσικών προσώπων, δηλαδή εκπροσώπων των

εισηγμένων, στα οποία παρέχονται δύο διαφορετικά ζεύγη κλειδιών και πιστοποιητικών (ένα για την ταυτοποίηση τους στο σύστημα και ένα για την αναγνωρισμένη ηλεκτρονική υπογραφή τους στις υποβαλλόμενες ηλεκτρονικά δηλώσεις τους)τοποθετημένα σε μια προσωποποιημένη έξυπνη κάρτα.

Παράλληλα η υποστήριξη και η χρήση ηλεκτρονικών συναλλαγών υπογραφών και πιστοποιητικών προβλέπεται στις προδιαγραφές των περισσοτέρων έργων που προκηρύχθηκαν ή προκηρύσσονται στα πλαίσια προγράμματος για την κοινωνία της πληροφορίας και των σχετικών Υπηρεσιακών προγραμμάτων των φορέων του ευρύτερου δημόσιου τομέα. Χαρακτηριστικά παραδείγματα αποτελούν οι σχεδιαζόμενες εφαρμογές για την ηλεκτρονική κατάθεση εμπορικών σημάτων καθώς και το σύστημα ηλεκτρονικών δημόσιων προκηρύξεων και προμηθειών στο υπουργείο Ανάπτυξης, τα σχέδια για ηλεκτρονικές υπογραφές των ηλεκτρονικών φύλλων της εφημερίδας της κυβερνήσεως του Εθνικού Τυπογραφείου, η πλήρης ηλεκτρονική λειτουργία των ΚΕΠ.

Σημαντική εξέλιξη προς τη γενικευμένη χρήση ηλεκτρονικών υπογραφών στην ελληνική Δημόσια Διοίκηση αποτελεί η υλοποίηση και η ολοκλήρωση του έργου Σύζευξις, που προβλεύθηκε η χρήση Υποδομής Δημόσιου Κλειδιού PKI και η πιστοποίηση ψηφιακών υπογραφών για ένα μεγάλο αριθμό δημοσίων υπαλλήλων, οι οποίοι θα μπορούν να εκδίδουν, να υπογράφουν και να διακινούν επίσημα ηλεκτρονικά δημόσια έγγραφα.

Η δυνατότητα ενός υποκειμένου να μην μπορεί να χρησιμοποιήσει τα ίδια μέσα πχ κρυπτογραφικά κλειδιά, πιστοποιητικά, για τη δημιουργία των δικών του ηλεκτρονικών υπογραφών και την επαλήθευση των ηλεκτρονικών υπογραφών τρίτων σε περισσότερους από έναν συναλλακτικούς κύκλους, δηλαδή η διαλειτουργικότητα όλων των σχετικών εφαρμογών αποτελεί ένα σημαντικό ζητούμενο αφού:

α) θα μειώσει το συνολικό κόστος

β) θα απλοποιήσει τις λειτουργίες του χρήστη

γ) θα περιορίσει τις πολλαπλές διαδικασίες ταυτοποίησης του υποκειμένου

δ) θα συμβάλει στη δημιουργία της κρίσιμης μάζας των χρηστών με δυνατότητα ηλεκτρονικής υπογραφής η οποία

ε) θα οδηγήσει στην ανάπτυξη και παροχή περισσότερων σχετικών υπηρεσιών προς τους χρήστες

Παράλληλα όμως η διαλειτουργικότητα και η χρήση της ίδιας ατομικής ψηφιακής υπογραφής σε πολλούς συναλλακτικούς κύκλους θέτει έντονα ζητήματα προστασίας των προσωπικών δεδομένων των χρηστών από πιθανές ανεπίτρεπτες διασταυρώσεις των συναλλαγών τους και τη δημιουργία έτσι αρχείων με ολοκληρωμένα ατομικά προφίλ των χρηστών.

Η τεχνική πολυπλοκότητα οι παραλλαγές των εφαρμογών προηγμένων ηλεκτρονικών υπογραφών και τα διάφορα επίπεδα αναγνώρισης τους, αναδεικνύουν ιδιαίτερες δυσκολίες ως προς την επίτευξη πλήρους διαλειτουργικότητας μεταξύ των υφιστάμενων εφαρμογών ηλεκτρονικής υπογραφής σε διεθνές και ευρωπαϊκό επίπεδο. Έχει παρατηρηθεί ότι η διαλειτουργικότητα επιτυγχάνεται ευκολότερα σε κλειστές εφαρμογές οι οποίες επιβάλλουν οι ίδιες συγκεκριμένες αναλυτικές προδιαγραφές πχ πρότυπα EMV για πιστωτικές κάρτες, συντονισμένες εφαρμογές διακυβέρνησης ενός κράτους κλπ . Στα πλαίσια της ευρωπαϊκής ένωσης, παρά τα τέσσερα και πλέον χρόνια από την έκδοση της σχετικής Ευρωπαϊκής οδηγίας που είχε ως στόχο την εναρμόνιση του σχετικού θεσμικού πλαισίου μεταξύ των κρατών- μελών, η παροχή πανευρωπαϊκώς αναγνωρισμένων και διαλειτουργικών μεταξύ τους υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, εξακολουθεί να εμφανίζει ακόμα αρκετές δυσχέρειες. Το γεγονός αυτό οφείλεται σε κάποιους ανασταλτικούς παράγοντες μεταξύ των οποίων περιλαμβάνονται:

- Ορισμένες ασάφειες του ευρωπαϊκού κανονιστικού πλαισίου, το οποίο προσπαθώντας να εξισορροπίσει μεταξύ τεχνολογικής ουδετερότητας και ασφάλειας δικαίου, καταλήγει σε ορισμένες αοριστίες.
- Η ανάπτυξη αυτόνομών εθνικών κανονιστικών πλαισίων σε ορισμένα κράτη – μέλη πριν την έκδοση της οδηγίας, και η διαφορετική ερμηνευτική προσέγγιση της οδηγίας από αυτά τα κράτη – μέλη, ώστε να διατηρηθεί απαράλλακτη η υφιστάμενη υποδομή τους.
- Οι αργοί ρυθμοί ανάπτυξης της προβλεπόμενης σχετικής τροποποίησης από τους ευρωπαϊκούς οργανισμούς, δεδομένου ότι επιχειρείται η όσο το δυνατόν μεγαλύτερη συμβατότητα με τις υφιστάμενες υποδομές και τα εφαρμοζόμενα συστήματα στα διάφορα κράτη - μέλη.

Με εξαίρεση ορισμένα κράτη μέλη πχ Γερμανία, Φιλανδία, Ιταλία που έχουν προβεί εγκαίρως σε αναλυτικές ρυθμίσεις για την παροχή υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, διαλειτουργικότητας υπάρχουν ακόμη και στις σχετικές υπηρεσίες που παρέχονται από τους παρόχους υπηρεσιών πιστοποίησης που λειτουργούν στο ίδιο κράτος, όπως παρατηρήθηκε – στο πλαίσιο της λειτουργίας της ομάδας Ε2 του e business forum – ότι συμβαίνει στην Ελλάδα.

Τα σημαντικότερα προβλήματα διαλειτουργικότητας μεταξύ των υπηρεσιών πιστοποίησης ηλεκτρονικών υπογραφών που παρατηρούνται, αναφέρονται κυρίως στην περιγραφή των στοιχείων του υποκειμένου των πιστοποιητικών (naming policy) στον τρόπο προσδιορισμού των επιτρεπόμενων χρήσεων των σχετικών κρυπτογραφικών κλειδιών και στα μέσα που χρησιμοποιούνται για την ενημέρωση των κατόχων και των αποδεκτών των ηλεκτρονικών πιστοποιητικών ως προς τους λοιπούς όρους έκδοσης που θέτονται από την εφαρμοζόμενη πολιτική των εκδιδόμενων πιστοποιητικών. Επίσης σημαντικά ζητήματα υφίστανται και με άλλα σχετιζόμενα θέματα, όπως η χρονοσήμανση των υπογραφών, η πιστοποίηση των ιδιοτήτων του υποκειμένου, οι υπηρεσίες ενημέρωσης για την ανάκληση των πιστοποιητικών, η αλληλο – διαπίστευση των παρόχων. Όλα αυτά έχουν ως πρόσθετο αρνητικό αποτέλεσμα την έλλειψη κοινώς αποδεκτών εφαρμογών λογισμικού για τη δημιουργία και την επαλήθευση ηλεκτρονικών υπογραφών, οι οποίες να εφαρμόζουν και να ερμηνεύουν και να ερμηνεύουν σωστά όλες τις παραπάνω παραμέτρους, ανεξάρτητα από τον εκδότη, το υποκείμενο ή τον αποδέκτη των σχετικών πιστοποιητικών.

8.Επίλογος

Η ανάγκη προστασίας του απαραβίαστου του απορρήτου, στο σύγχρονο ψηφιακό περιβάλλον προκύπτει περισσότερο καθοριστική από ποτέ. Ειδικότερα, καθώς το Διαδίκτυο αποτελεί σήμερα το σημαντικότερο εκφραστικό μέσο της ελευθερίας στην
επικοινωνία των ανθρώπων, θα πρέπει να αναπτυχθούν μηχανισμοί προστασίας και ασφάλειας, από εκείνους που επιβουλεύονται την ελευθερία αυτή.

Η δημιουργία των ψηφιακών υπογραφών, βασιζόμενη στη τεχνολογία της κρυπτογραφίας, αποτελεί μια διαδεδομένη μέθοδο, προστασίας και ασφαλείας στη διακίνηση των ηλεκτρονικών εγγράφων.

Κρίνεται σκόπιμο να αναφερθεί ότι η ψηφιακή υπογραφή, παρέχει εγγύηση της αυθεντικότητας, της ακεραιότητας, της μη αλλοίωσης το περιεχομένου των μηνυμάτων που διακινούνται ηλεκτρονικά.

Κατά συνέπεια, προκύπτει πως η ιδανικότερη λύση για την ασφαλή διακίνηση αλλά και χρήση των ψηφιακών αντικειμένων είναι ο συνδυασμός των αναπτυγμένων μεθόδων προστασίας. Η προσθήκη δηλαδή ψηφιακής υπογραφής στα διακινούμενα ηλεκτρονικά έγγραφα, αποτελεί ενδεδειγμένο τρόπο, για την προστασία του εγγράφου τόσο κατά την μεταφορά του, όσο και κατά τη χρήση του.

Βιβλιογραφία

Κάτος Β.-Στεφανίδης Γ. (2003), *Τεχνικές Κρυπτογραφίας και κρυπτανάλυσης.* Ζυγός

Stalings William μεταφραστής Λιμνιώτης Κωνσταντίνος <<Κρυπτογραφία και ασφάλεια δικτύων>> (2012) Εκδόσεις Ίων

Μαρτάκος Δ.- Κυρλόγλου Ν.- Μητράκας Α-Γιαννακάκη Μ.-Σιουλής Χ . Δεκάλογος για τις ηλεκτρονικές υπογραφές και τα ηλεκτρονικά πιστοποιητικά ταυτοποίησης. E-bussines forum.

FIPS 46-3: U.S. DEPARTMENT OF COMMERCE, William M. Daley, Secretary, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Raymond G. Kammer, Director, "DATA ENCRYPTION STANDARD (DES)", October 1999.

Public- key Infrastructure (x.509) (pkix) Internet Working group

Ευρωπαϊκή οδηγία 99/93/ΕΚ του Ευρωπαϊκού κοινοβουλίου και του συμβουλίου της 13ης Δεκεμβρίου 1999 «Σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές»

Wikipedia, The Free Encyclopedia, *History of Cryptography* http://en.wikipedia.org/wiki/History_of_cryptography,

Wikipedia, The Free Encyclopedia, *Digital Signature*, http://en.wikipedia.org/wiki/Digital_signature

Εισαγωγή στην κβαντική κρυπτογραφία: Ιστορική αναδρομή, http://www.geocities.com/kzerzel/history.htm

Υπηρεσία εκδόσεων Ευρωπαϊκής Ένωσης

https://publications.europa.eu/index_el.html

HERMES-Hellenic Exchanges MEsaging Services

https://hermesD-EXT/ase.gr/hermes/_el.htm

Νομικά Θέματα Ηλεκτρονικού Εμπορίου, ψηφιακές υπογραφές, τράπεζες νομικών πληροφοριών Ηλεκτρονικού εμπορίου.

https://www.acci.gr/ecomm/legal.index.html

Λεπτομέρειες λειτουργίας του αλγορίθμου Blowfish

http://pocketbrief.net/related/BlowfishEncryption

Λειτουργία του αλγορίθμου RC5
https://www.grc.com/r&d/rc5

Λειτουργία του αλγορίθμου IDEA
http://www.nku.edu