



ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

Δ.Π.Μ.Σ: ΜΑΘΗΜΑΤΙΚΑ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΤΩΝ ΑΠΟΦΑΣΕΩΝ

Αλγόριθμοι Κρυπτογράφησης Διαμοιραζόμενου Κλειδιού: Θεωρία και Εφαρμογές

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Ανδρεοπούλου Αικατερίνης

Επιβλέπων:

Πετρόπουλος Κωνσταντίνος (Επίκουρος Καθηγητής)

Πάτρα, Μάιος 2018

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την

.....

Κ.Πετρόπουλος
Επ.Καθηγητής
Τμήμα Μαθηματικών

Πανεπιστήμιο Πατρών

.....

Ι.Σταματίου
Αν.Καθηγητής
Τμήμα Διοίκησης
Επιχειρήσεων

Πανεπιστήμιο Πατρών

.....

Μ.Βραχάτης
Καθηγητής
Τμήμα Μαθηματικών

Πανεπιστήμιο Πατρών

Πάτρα, Μάιος 2018

.....
Αικατερίνη Ανδρεοπούλου, 2018
Πτυχιούχος Μαθηματικός Πανεπιστημίου Πατρών

Copyright Αικατερίνη Ανδρεοπούλου, 2018
Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξόλοκληρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευτεί ότι εκφράζουν τις επίσημες θέσεις του Πανεπιστημίου Πατρών.

ΕΥΧΑΡΙΣΤΙΕΣ

Η συγγραφή μίας διπλωματικής εργασίας σημαίνει το τέλος μίας δύσκολης αλλά συνάμα ε-
ποικοδομητικής περιόδου μέσα στην οποία πραγματοποιήθηκε με επιτυχία η παρακολούθηση των
μεταπτυχιακών σπουδών. Πρόκειται για μία επίπονη διανοητική εργασία, η οποία για να φτάσει
στο πέρας της είναι απαραίτητη η συνδρομή κάποιων ανθρώπων που παρέχουν είτε ψυχολογική
υποκίνηση, είτε συνδράμουν με τις γνώσεις και το ερευνητικό τους έργο. Η παρούσα εργασία εκ-
πονήθηκε στα πλαίσια του Διατμηματικού Προγράμματος Μεταπτυχιακών Σπουδών «Μαθηματικά
των Υπολογιστών και των Αποφάσεων» του Τμήματος Μαθηματικών και του Τμήματος Μηχανι-
κών Η/Υ και Πληροφορικής. Θα ήθελα αρχικά να ευχαριστήσω τον επιβλέποντα καθηγητή μου
και Επίκουρο Καθηγητή κ. Κωνσταντίνο Πετρόπουλο για την άριστη συνεργασία που είχαμε όλο
αυτό το διάστημα της προσπάθειάς μου προς την επίτευξη του στόχου μου.

Επίσης, θα ήθελα να ευχαριστήσω ιδιαίτερα τον Αναπληρωτή Καθηγητή κ.Ιωάννη Σταματίου
,με τον οποίο και συνεργάστηκα εκτενώς, για τη συνεχή καθοδήγηση και ενθάρρυνση με σκοπό την
επίτευξη του βέλτιστου δυνατού αποτελέσματος, τη συμπαράστασή του, τη συνεχή του υποστήριξη,
το αμείωτο ενδιαφέρον που έδειξε από την αρχή μέχρι το τέλος, καθώς και για το χρόνο που
μου αφιέρωσε. Επίσης τον Καθηγητή κ.Μιχαήλ Βραχάτη, εξαιρετικό καθηγητή με βαρύνουσα
άποψη και κύρος, για την τιμή που μου έκανε να αποτελέσει μέλος της Τριμελούς Εξεταστικής
Επιτροπής. Επιπρόσθετα νιώθω την ανάγκη να ευχαριστήσω θερμά όλους τους διδάσκοντες του
Διατμηματικού Προγράμματος Μεταπτυχιακών Σπουδών για τις γνώσεις και τα εφόδια που μου
μετέδωσαν καθώς και για την άριστη συνεργασία κατά τη διάρκεια των μαθημάτων.

Θα ήθελα να ευχαριστήσω θερμά όλους τους φίλους μου που πίστεψαν σε μένα και με ενθάρ-
ρυναν σε κάθε στάδιο των σπουδών μου. Ιδιαίτερος ευχαριστώ τη συμφοιτήτριά μου και φίλη μου
Ξένια Καραμέτου για τις στιγμές και τις αγωνίες που μοιραστήκαμε, καθώς και για την έμπρακτη
υποστήριξή της και τις επίμονες παροτρύνσεις της συμβάλλοντας έτσι με το δικό της ξεχωριστό
τρόπο στην ολοκλήρωση της συγγραφής.

Κλείνοντας, ευχαριστώ ειλικρινά τους γονείς μου για την ηθική τους στήριξη και τους ευγνω-
μονώ που στέκονται πάντα δίπλα μου τόσο στις επιτυχίες όσο και στις αποτυχίες, δίνοντάς μου
την ελπίδα και τη δύναμη να συνεχίσω να προσπαθώ για το καλύτερο.

Εισαγωγή

Ο σκοπός της κρυπτογραφίας είναι να παραλάβει ένα μήνυμα ή αρχείο, που ονομάζεται απλό κείμενο (plain text), και να το αποκρυπτογραφήσει παράγοντας το κρυπτοκείμενο (ciphertext), με τέτοιο τρόπο ώστε μόνο εξουσιοδοτημένα άτομα να γνωρίζουν πως θα το μετατρέψουν αντίστροφα σε απλό κείμενο. Για όλους τους υπόλοιπους, το κρυπτοκείμενο είναι απλούστατα μια ακατονόητη σειρά από bits. Οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης πρέπει πάντα να είναι δημόσιοι. Οι προσπάθειες απόκρυψής τους δε βοηθούν ποτέ και δίνουν στους ανθρώπους που προσπαθούν να κρύψουν τα δεδομένα μια απατηλή αίσθηση ασφάλειας.

Η μυστικότητα εξαρτάται από παραμέτρους στους αλγόριθμους, οι οποίες ονομάζονται κλειδιά (keys). Τα συστήματα κρυπτογράφησης τα συναντούμε στην καθημερινή μας ζωή σε μεγάλο πλήθος εφαρμογών. Μερικές από τις χρήσεις τους είναι η ασφαλής επικοινωνία, η αναγνώριση- η πιστοποίηση- η εξουσιοδότηση (δηλαδή η ικανότητά ενός δικτύου να αναγνωρίζει αξιόπιστα τους χρήστες), ο διαμοιρασμός μυστικού (secret sharing), το ηλεκτρονικό εμπόριο (οι εμπορικές συναλλαγές μέσω του διαδικτύου), πιστοποίηση/έκδοση βεβαίωσης, η ανάκτηση κλειδιού, η ασφαλής απομακρυσμένη πρόσβαση κλπ.

Καθ' όλη τη διάρκεια της ιστορίας, τα σημαντικά μηνύματα που στέλνονται από τις κυβερνήσεις, τους στρατούς και τις επιχειρήσεις έχουν στηριχθεί σε κώδικες που κρυπτογραφούνται από τη μία πλευρά και συγχρόνως αποκρυπτογραφούνται από τον παραλήπτη. Αλλά για να το κάνουν αυτό, η πληροφορία για τον κώδικα πρέπει να κοινοποιηθεί σε τουλάχιστον δύο ανθρώπους μέσω του αγγελιοφόρου, ή όπως γίνεται πιο συχνά στην σύγχρονη εποχή, μέσω ενός δικτύου επικοινωνιών. Όμως, στο δίκτυο μπορεί να εισέλθει κάποιος και να γίνει κλοπή του κώδικα κρυπτογράφησης.

Οι περισσότερες ασφαλείς ψηφιακές επικοινωνίες δεδομένων σήμερα βασίζονται στη χρήση πολύ μεγάλων αριθμών, τα λεγόμενα κλειδιά. Δύο κλειδιά περιέχονται σε κάθε κρυπτογράφηση, ένα ιδιωτικό κλειδί, στο οποίο μόνο ο πομπός του μηνύματος έχει την πρόσβαση, και ένα δημόσιο κλειδί, που είναι διαθέσιμο στον καθένα. Τα δύο κλειδιά λειτουργούν μαζί, έτσι ένα μήνυμα που αναμειγνύεται με ένα δημόσιο κλειδί μπορεί να ξεκαθαριστεί και να αναγνωστεί μόνο με το ιδιωτικό κλειδί. Τα δημόσια συστήματα με κλειδιά απαιτούν να ξέρει ο πομπός το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει ένα μήνυμα. Έτσι απαιτείται να υπάρχει μια παγκόσμια βιβλιοθήκη των δημόσιων κλειδιών. Μια αδυναμία αυτού του συστήματος είναι ότι, με έναν αρκετά ισχυρό υπολογιστή, είναι πιθανό να υπολογιστεί το ιδιωτικό κλειδί από το δημόσιο κλειδί.

Περίληψη

Αντικείμενο της διπλωματικής εργασίας είναι κυρίως οι Αλγόριθμοι Κρυπτογράφησης Διαμοιραζόμενου Κλειδιού, καθώς και οι εφαρμογές τους. Η κρυπτογραφία ξεκίνησε από αρχαιοτάτων χρόνων, με την ιστορική της διαδρομή να χωρίζεται σε τρεις περιόδους: από το 1900 π.Χ. έως το 1900 μ.Χ. που είναι η πρώτη της περίοδος, από το 1900 μ.Χ. έως το 1950 μ.Χ. που είναι η δεύτερή της περίοδος με την αλματώδη ανάπτυξη που είχε ιδιαίτερα τις περιόδους των δύο παγκοσμίων πολέμων και τέλος από το 1950 μ.Χ. μέχρι και σήμερα. Στην συνέχεια παρουσιάζονται οι βασικές αρχές της κρυπτογραφίας και τα είδη της, που είναι κυρίως η συμμετρική, η ασύμμετρη και η υβριδική, καθώς επίσης και τα πλεονεκτήματα – μειονεκτήματα που έχει το κάθε είδος. Αμέσως μετά γίνεται αναφορά στους διάφορους μηχανισμούς, οι οποίοι χρησιμοποιούνται για να εφαρμοστεί η κρυπτογραφία και αυτό επιτυγχάνεται με κάποιους κρυπταλγόριθμους τμημάτων, οι οποίοι είναι οι Stream Ciphers, οι Block Ciphers και βασίζονται βασικά στις δομές Feistel, και τις συναρτήσεις κατακερματισμού. Τέλος στην ενότητα αυτή αναφέρονται ορισμένα για την τεχνική Message Authentication Code (MAC), που είναι ο Κώδικας Αυθεντικοποίησης Μηνυμάτων.

Στις δύο ενότητες που ακολουθούν αναφέρονται περιπτώσεις αλγορίθμων συμμετρικής και ασύμμετρης κρυπτογραφίας, οι μέθοδοι λειτουργίας τους, η δομή τους, η αρχιτεκτονική τους, τα πιθανά πλεονεκτήματα – μειονεκτήματα, καθώς και οι πιθανές επιθέσεις εναντίον τους από κακόβουλους, οι οποίοι θέλουν να υποκλέψουν τα μηνύματα ή κάποια δεδομένα, που ανταλλάσσουν μεταξύ τους οντότητες που επικοινωνούν μέσω ενός δικτύου. Συνεχίζεται η εργασία με τέσσερις ενότητες που αναφέρονται στα πρωτόκολλα, Secure Socket Layer (SSL) και Privacy Enhanced Mail (PEM), που σκοπό έχουν την ασφαλή επικοινωνία στο Internet, όπου διακινούνται ευαίσθητες πληροφορίες, προσωπικά δεδομένα και εμπορικές συναλλαγές με πιστωτικές κάρτες. Γίνεται αναφορά στις αρχές αυτών των πρωτοκόλλων, τις υπηρεσίες που προσφέρουν, τα χαρακτηριστικά τους, την αρχιτεκτονική τους, την αντοχή τους σε γνωστές επιθέσεις και τέλος τις αδυναμίες τις οποίες έχουν. Υπάρχει η ενότητα η οποία αναφέρεται στο σύστημα κρυπτογράφησης Pretty Good Privacy (PGP) και ιδιαίτερα στα στοιχεία του, τη λειτουργία το, τα χαρακτηριστικά του καθώς και τις αλυσίδες κλειδιών. Επίσης γίνεται εκτενής αναφορά στις αρχές πιστοποίησης, οι οποίες είναι απαραίτητες, ώστε να είναι δυνατή η δημιουργία και η διανομή ψηφιακών πιστοποιητικών, στην υποδομή δημόσιου κλειδιού, τα είδη των πιστοποιητικών, καθώς και τις ψηφιακές υπογραφές. Ακολουθούν αρκετές εφαρμογές της κρυπτογραφίας, οι οποίες αναφέρονται συνοπτικά.

Τέλος γίνεται αναφορά στο Cloud Computing και το IoT, και αναλυτικά στην αρχιτεκτονική τους, τα χαρακτηριστικά τους, τα μοντέλα εφαρμογής τους, τους τρόπους χρήσης τους, τα πλεονεκτήματα – μειονεκτήματά τους, τις υπηρεσίες τους, τα πιθανά οφέλη από την χρήση τους και τις εφαρμογές τους.

Abstract

The subject of the dissertation is mainly Cipher (Encryption) Algorithms of Shared Key. Cryptography has begun from ancient times, with its historical path divided into three periods: from 1900 b.c. to 1900 a.c., which is the first period, from 1900 a.c. to 1950 a.c., that signifies the second period with the leapward growth of cryptography, especially during the two world wars, and the third period from 1950 a.c. until today.

Continuing, there are presented the basic principles of cryptography and its types of symmetrical, asymmetric and hybrid as well as the advantages and disadvantages of each kind. Next, reference is made to the various mechanisms used to implement cryptography and how this is accomplished with some ciphers of segments, like Stream Ciphers, Block Ciphers, and it is based on the Feistel structures and functions of fragmentation. Finally, into this unit are mentioned some elements about the technique known as Message Authentication Code (MAC).

In the two following units, there is reference to some algorithm cases of symmetrical and asymmetric cryptography, their function methods, their structure and architecture, the advantages and disadvantages they may have, as well as possible attacks by malicious people who want to shed messages or some data, which are exchanged between entities that communicate through a network.

The next four units of the dissertation deal with the two protocols named Secure Socket Layer (SSL) and Privacy Enhanced Mail (PEM), which are used for the secure communication through internet, where sensitive information and personal data are being exchanged and also commercial transactions with credit cards are being made. There is reference to the principles of these protocols, the services they offer, their characteristics, their structure, their ability to resist to malicious attacks and last but not least, their weaknesses. Another unit is dedicated to the cryptography system called Pretty Good Privacy (PGP) and especially to its elements, function, characteristics and its key chains. There is also a thorough reference to the principles of certification which are essential for the creation and distribution of digital certificates, the infrastructure of a public key, the types of certificates as well as the digital signatures. Several other applications of cryptography are mentioned briefly in the dissertation.

Finally, another subject examined here is Cloud Computing and IoT, specifically their structure, characteristics, their application models, their ways of use, their assets and flaws, their services, the benefits that may derive from their use and applications.

Περιεχόμενα

1	Κρυπτογραφία	15
1.1	Εισαγωγή	15
1.2	Ιστορική αναδρομή και χρονικές περίοδοι κρυπτογραφίας	16
1.3	Βασικές αρχές κρυπτογραφίας	21
1.4	Τεχνικοί όροι και έννοιες	23
1.5	Είδη κρυπτογραφίας	25
1.5.1	Συμμετρική Κρυπτογραφία	25
1.5.2	Ασύμμετρη Κρυπτογραφία ή Κρυπτογραφία Δημοσίου Κλειδιού	26
1.5.3	Υβριδική Κρυπτογραφία Ψηφιακού Φακέλου	28
1.5.4	Μειονεκτήματα και Πλεονεκτήματα την Συμμετρικής και Ασύμμετρης Κρυπτογραφίας	29
1.5.5	Κβαντική κρυπτογραφία	29
2	Μηχανισμοί Εφαρμογής της Κρυπτογραφίας	31
2.1	Κρυπταλγόριθμος Στοιχειοσειράς (Stream Cipher)	31
2.2	Κρυπταλγόριθμος τμημάτων (Block Cipher)	32
2.2.1	Substitution Ciphers	33
2.2.2	Transposition Systems	35
2.2.3	Product Systems	36
2.2.4	Δομές Feistel	36
2.3	Συναρτήσεις Κατακερματισμού (Hash Functions)	39
2.4	Κώδικας Αυθεντικοποίησης Μηνυμάτων Message Authentication Code - (MAC)	42
3	Αλγόριθμοι Μυστικού ή Συμμετρικού Κλειδιού	45
3.1	Γενικά	45
3.2	Μέθοδοι Λειτουργίας των Κρυπταλγορίθμων Τμημάτων (Modes of operation)	45
3.3	Ασφάλεια μυστικού κλειδιού του κρυπταλγορίθμου τμημάτων	47
3.3.1	Ταξινόμηση των επιθέσεων	47
3.3.2	Πρακτικές Απορρήτου	49
3.3.3	Brute Force Attacks	49
3.4	Σχεδιασμός των κρυπταλγορίθμων τμημάτων	51
3.5	Επιθέσεις στους Αλγορίθμους Μυστικού Κλειδιού	51
3.5.1	Διαφορική Κρυπτανάλυση (Differential Cryptanalysis)	51
3.5.2	Γραμμική Κρυπτανάλυση Linear Cryptanalysis	52
3.5.3	Επίθεση στα Αδύναμα Κλειδιά	53
3.5.4	Αλγεβρικές Επιθέσεις	53
3.6	Block and Key Size	53
3.7	Ευρέως Χρησιμοποιούμενοι Συμμετρικοί Αλγόριθμοι Κρυπτογράφησης	54

3.7.1	DES (Data Encryption Standard)	54
3.7.2	TDES (Triple Data Encryption Standard)	56
3.7.3	CAST-128	57
3.7.4	MARS	58
3.7.5	RC2	58
3.7.6	RC4	59
3.7.7	RC5	60
3.7.8	RC6	62
3.7.9	SERPENT	63
3.7.10	International Data Encryption Algorithm (IDEA)	63
3.7.11	Towfish	64
3.7.12	Blowfish	64
3.7.13	Safer K-64	66
3.7.14	RIJNDAEL	66
3.7.15	Advanced Encryption Standard (AES)	67
3.7.16	Κουτιά Αντικατάστασης (S-boxes)	71
4	Αλγόριθμοι Δημόσιου ή Ασύμμετρου Κλειδιού	73
4.1	Δομή Κρυπτοσυστημάτων Δημοσίου Κλειδιού	73
4.2	Μέθοδος Λειτουργίας	74
4.3	Ο Αλγόριθμος RSA	75
4.3.1	Λειτουργία του Αλγορίθμου RSA	77
4.3.2	Πλεονεκτήματα του Αλγορίθμου RSA	78
4.3.3	Ασφάλεια του Αλγορίθμου RSA	78
4.3.4	Πιθανές Επιθέσεις του Αλγορίθμου RSA	79
4.4	Ο Αλγόριθμος Diffie and Hellman	79
4.5	Ο Αλγόριθμος El Gamal	80
4.6	Ο Αλγόριθμος DSA	80
4.7	Αλγόριθμος Ελλειπτικών Καμπυλών	80
4.8	Αλγόριθμοι MD2, MD4 και MD5	81
4.9	Αλγόριθμοι SHA και SHA-1	81
4.10	Ripemd-160	82
4.11	Επιθέσεις στους Αλγορίθμους Δημόσιου Κλειδιού	83
4.11.1	Επιθέσεις παραγοντοποίησης (factoring attacks)	83
4.11.2	Επιθέσεις αλγοριθμικές	83
4.12	Στεγανογραφία	83
5	Πρωτόκολλο SSL (Secure Socket Layer)	85
5.1	Γενικά	85
5.2	Υπηρεσίες που προσφέρει το SSL	85
5.3	Χαρακτηριστικά του SSL	86
5.4	SSL και Μοντέλο OSI	87
5.5	Η Αρχιτεκτονική του SSL	87
5.6	Πρωτόκολλο SSLRP	89
5.7	Εκδόσεις του SSL	89
5.8	SSL Ψηφιακά Πιστοποιητικά	90
5.9	Αντοχή του SSL σε γνωστές επιθέσεις	90
5.10	Αδυναμίες του SSL	91

6	Αρχές Πιστοποίησης και Πιστοποιητικά Server	93
6.1	Αρχές Πιστοποίησης CA (Certification Authorities)	93
6.2	Ιεραρχίες Πιστοποίησης	94
6.3	Υποδομή Δημόσιου Κλειδιού (PKI)	96
6.3.1	Συστατικά Μέρη της Υποδομής Δημόσιου Κλειδιού	96
6.3.2	Υπηρεσίες Υποδομής Δημόσιου Κλειδιού	98
6.4	Ψηφιακά Πιστοποιητικά	98
6.4.1	Γενικά	98
6.4.2	Είδη Πιστοποιητικών	99
6.4.3	Απόκτηση Πιστοποιητικών για έναν Server	99
6.4.4	Ψηφιακά πιστοποιητικά από την μεριά του χρήστη	100
6.4.5	Ψηφιακές Υπογραφές	101
7	PGP (Pretty Good Privacy)	103
7.1	Εισαγωγή	103
7.2	Συστατικά στοιχεία του PGP	103
7.3	Η γεννήτρια Τυχαίων Αριθμών	104
7.4	Η Λειτουργία του PGP	104
7.5	Τα χαρακτηριστικά του PGP	105
7.6	Αλυσίδες κλειδιών (Key Rings)	106
7.7	Προστασία Δημόσιου Κλειδιού	106
7.8	Διαδικασία αναγνώρισης έγκυρων κλειδιών	107
7.9	Προστασία του μυστικού κλειδιού	108
7.10	Δουλεύοντας με το PGP	109
8	Πρωτόκολλο PEM (Privacy Enhanced Mail)	111
8.1	Εισαγωγή	111
8.2	Οι αρχές του PEM	111
8.3	Είδη κλειδιών και διαχείριση αυτών για το πρωτόκολλο PEM	112
8.4	Περιληπτική Διαχείριση Μηνυμάτων	112
8.5	Μηχανισμός Ενθυλάκωσης	113
8.6	Τύποι μηνυμάτων των PEM	113
8.7	Ταχυδρομικές Λίστες	114
8.8	Περίληψη Ενθυλακωμένων Επικεφαλίδων	114
8.9	Υποστηριζόμενοι Αλγόριθμοι	115
9	Εφαρμογές της Κρυπτογραφίας	117
9.1	Γενικά	117
9.2	Πρωτόκολλα	118
9.2.1	PEM (Privacy Enhanced Mail)	118
9.2.2	S/MIME (Secure/Multipurpose Internet Mail Extensions)	118
9.2.3	S-HTTP(Secure Hyper –Text-Transfer-Protocol)	118
9.2.4	IP Sec (IP Security Protocol)	119
9.2.5	SET (Secure Electronic Transactions)	119
9.2.6	SSH (Secure Shell)	119
9.2.7	Το πρωτόκολλο ανταλλαγής κλειδιών (IKE-Internet Key Exchange)	119
9.3	Συστήματα ψηφιακών πληρωμών	120
9.3.1	First Virtual	120
9.3.2	Cyber Cash	120

9.3.3	Digicash	120
9.3.4	Millicent	120
9.3.5	Μαγνητικές Κάρτες	121
9.3.6	Έξυπνες Κάρτες (Smart Card)	121
9.4	Σύστημα Κέρβερος	121
9.5	Συστήματα βάσης βιομετρήσεων	121
9.6	Ιδιωτικά δίκτυα VPN (Virtual Private Network)	122
9.7	Ηλεκτρονική ψηφοφορία	122
9.8	Ηλεκτρονική δημοπρασία	122
9.9	Ηλεκτρονικό γραμματοκιβώτιο (Mail Box)	123
9.10	Τηλεδιάσκεψη	123
9.11	Τηλεφωνία μέσω VOIP	123
9.12	Ασφάλεια τραπεζικών συναλλαγών	123
9.13	Δίκτυα ATM	123
10		125
10.1	Η Έννοια Της Ιδιωτικότητας(Privacy)	125
10.2	ABC 4 Trust	126
10.2.1	Attribute Based Διαπιστευτήρια	126
10.2.2	Περιγραφή του έργου ABC4Trust	127
10.2.3	Στόχοι του έργου ABC4Trust	128
10.3	Υπολογιστικό Νέφος (cloud computing)	129
10.3.1	Εισαγωγή στο 'νέφος'	129
10.3.2	Ιστορική αναδρομή για το Cloud Computing	130
10.3.3	Γενικά για το Cloud Computing	131
10.3.4	Αρχιτεκτονική του Cloud Computing	132
10.3.5	Τι είναι το cloud computing	134
10.3.6	Σημαντικές Έννοιες	136
10.3.7	Εναλλακτικοί και χρήσιμοι τρόποι χρήσης των cloud υπηρεσιών	137
10.3.8	Πλεονεκτήματα της χρήσης της τεχνολογίας cloud	137
10.3.9	Πάροχοι υπηρεσιών cloud	138
10.3.10	Υπηρεσίες cloud της Google	138
10.3.11	Πιθανά οφέλη από τη χρήση του cloud και ζητήματα προς επίλυση	139
10.3.12	Η υπηρεσία Pithos	142
10.3.13	Το Chromebook	143
10.4	Internet of Things	143
10.4.1	Εισαγωγή	143
10.4.2	Κύρια Χαρακτηριστικά του IoT	144
10.4.3	Κατηγορίες Εφαρμογών του IoT	145
10.4.4	Συγκεκριμένα παραδείγματα εφαρμογών	145
10.4.5	Ιδιότητες των αυτόνομων IoT συστημάτων	149
10.4.6	Πηγές κινδύνου	150

Κατάλογος Σχημάτων

1.1	Σύστημα Κρυπτογράφησης Αποκρυπτογράφησης	23
1.2	Διαδικασία Συμμετρικής Κρυπτογραφίας	26
1.3	Διαδικασία Κρυπτογράφησης Δημόσιου Κλειδιού	27
2.1	Διαδικασία Κρυπτογράφησης Στοιχειοσειράς	32
2.2	Κρυπταλγόριθμος τμημάτων	32
2.3	Κλασικό δίκτυο Feistel	37
2.4	Κρυπτογράφηση μηνύματος με hash function	40
2.5	Ταξινόμηση των κρυπτογραφικών συναρτήσεων κατακερματισμού	41
2.6	Η επαναληπτική δομή Damgard-Merkle για συναρτήσεις κατακερματισμού. (f είναι μια συνάρτηση συμπίεσης)	42
2.7	Αυθεντικοποίηση μηνύματος με χρήση MAC	43
3.1	Το μοντέλο του Shannon ενός γενικού συστήματος απορρήτου	47
3.2	Γενική περιγραφή του αλγορίθμου κρυπτογράφησης DES	55
3.3	Γενική περιγραφή του αλγορίθμου κρυπτογράφησης TDES	56
3.4	Αλγόριθμος CAST-128	58
3.5	Αλγόριθμος RC2	59
3.6	Αλγόριθμος RC4	60
3.7	Αλγόριθμος RC5	61
3.8	Αλγόριθμος RC6	62
3.9	Αλγόριθμος SERPENT	63
3.10	Αλγόριθμος IDEA	64
3.11	Αλγόριθμος BLOWFISH	65
3.12	Συμμετρικοί Αλγόριθμοι Κρυπτογράφησης	70
4.1	Παράδειγμα Αλγορίθμου RSA	76
4.2	Αλγόριθμος RSA	77
4.3	Ελλειπτική Καμπύλη	81
4.4	Συγκριτική παρουσίαση των αλγορίθμων MD5, SHA-1, RIPEMD-160	82
4.5	Μια εικόνα που περιέχει το κρυμμένο μήνυμα (110, 010, 111, 010, 010, 010, 100, 101, 011, 001)	84
6.1	Γενική ιεραρχία πιστοποίησης	94
6.2	Κατερχόμενη ιεραρχία πιστοποίησης	95
10.1	Επαλήθευση ενός attribute-based διαπιστευτηρίου	127
10.2	Ένα απλό μοντέλο επιπέδων του «cloud»	133
10.3	Μοντέλα υπηρεσιών του «cloud»	136
10.4	Συγκεντρωτικός πίνακας παρόχων υπηρεσιών «νέφους»	138

10.5	Οφέλη από την χρήση του cloud	140
10.6	Ζητήματα προς επίλυση του cloud	141

Κεφάλαιο 1

Κρυπτογραφία

1.1 Εισαγωγή

Η κρυπτογραφία αναφέρεται στην υλοποίηση μεθόδων τροποποίησης των μεταδιδόμενων πληροφοριών, έτσι ώστε να γίνονται κατανοητά μόνο από τον προβλεπόμενο παραλήπτη. Είναι μια διαδικασία που μπορεί να εκτελεστεί τόσο σε υλικό (hardware), όσο και σε λογισμικό (software).

Οι χρήστες δεν γνωρίζουν ούτε αντιλαμβάνονται την παρουσία της και πραγματοποιούν ανενόχλητοι τις εργασίες τους. Το γεγονός ότι ο χρήστης δεν ανακατεύεται καθόλου στις διαδικασίες της κρυπτογράφησης, αυξάνει την αποτελεσματικότητα του εργαλείου στην παρεχόμενη ασφάλεια. Παρ' όλα αυτά, δεν έχει καθιερωθεί η κρυπτογραφία σε υλικό λόγω του υψηλού κόστους, το οποίο είναι απαγορευτικό για την αγορά και την διατήρηση των ειδικών μηχανημάτων που χρειάζονται για την εφαρμογή της και τα οποία βρίσκονται τοποθετημένα σε στρατηγικά σημεία κάθε δικτύου.

Η λογισμική κρυπτογράφηση είναι πιο φθηνή, γι' αυτό είναι ευρέως αποδεκτή και εύκολα πραγματοποιήσιμη. Βέβαια δεν είναι το ίδιο γρήγορη με την εκτέλεση σε υλικό, αλλά η συνεχώς αυξανόμενη ανάγκη για την διασφάλιση των επικοινωνιών έχει εδραιώσει την χρήση της.

Ως κρυπτογραφία μπορεί να ορισθεί ο επιστημονικός κλάδος ο οποίος ασχολείται με την μετατροπή των πληροφοριών, με σκοπό την διαφύλαξη του απορρήτου τους. Σκοπός της είναι να διασφαλίσει την ιδιωτικότητα ενός μηνύματος με το να κρατά την πληροφορία κρυφή από οποιονδήποτε, ο οποίος δεν έχει οριστεί σαν αποδέκτης του μηνύματος, ακόμα και εάν έχει πρόσβαση στα κρυπτογραφημένα δεδομένα.

Εκτός από την κρυπτογραφία, που έχει στόχο την διατήρηση της μυστικότητας των μηνυμάτων, υπάρχει και η κρυπτανάλυση, η οποία ορίζεται σαν η τεχνική της παραβίασης του κρυπτογραφημένου μηνύματος, χωρίς να είναι γνωστό το κλειδί της αποκρυπτογράφησης. Η τεχνική της επινόησης κρυπτογραφημάτων και της παραβίασης αυτών είναι συνολικά γνωστή σαν κρυπτολογία.

Παλαιότερα χρησιμοποιούσαν την κρυπτογράφηση αποκλειστικά για στρατιωτικούς σκοπούς. Σήμερα όμως στην κοινωνία της πληροφορίας, η κρυπτογράφηση είναι ένα από τα βασικά εργαλεία διατήρησης των μηνυμάτων με όλα τα προφανή πλεονεκτήματα. Γενικά η κρυπτογράφηση μπορεί να χρησιμοποιηθεί σε πολλές εφαρμογές όπως:

- Προστασία δεδομένων, αποθηκευμένων στον υπολογιστή, από μη εξουσιοδοτημένη πρόσβαση.
- Προστασία δεδομένων κατά την μεταφορά τους ανάμεσα σε δύο υπολογιστικά συστήματα.
- Ανίχνευση τυχαίας ή εσκεμμένης αλλαγής σε δεδομένα.
- Πιστοποίηση της ταυτότητας του συντάκτη/εκδότη ενός κειμένου ή μηνύματος.

Βέβαια η κρυπτογράφηση έχει και μειονεκτήματα, όπως:

- Το γεγονός ότι δε μπορεί να αποτρέψει την διαγραφή δεδομένων από έναν εισβολέα του συστήματος.
- Επίσης κατά την διάρκεια μιας επίθεσης μπορεί να μεταβληθεί το πρόγραμμα κρυπτογράφησης, ώστε να χρησιμοποιεί διαφορετικό κλειδί από αυτό που έχει καθοριστεί από τον νόμιμο χρήστη ή να καταγραφούν όλα τα κλειδιά για μελλοντική χρήση.
- Επιπλέον μπορεί να βρεθεί ένας εύκολος τρόπος για την αποκωδικοποίηση μηνυμάτων.
- Τέλος μπορεί ένα αρχείο να προσπελασθεί πριν από την κωδικοποίησή του ή μετά από την αποκωδικοποίησή του.

1.2 Ιστορική αναδρομή και χρονικές περίοδοι κρυπτογραφίας

Η κρυπτογραφία ξεκινάει περίπου το 4000 π.Χ. στην αρχαία Αίγυπτο, μετά περνάει στην Αρχαία Ελλάδα και συνεχίζεται στην εποχή του Ιουλίου Καίσαρα.

Η ιστορία της κρυπτογραφίας χωρίζεται βασικά σε τρεις μεγάλες χρονικές περιόδους: την 1η περίοδο από το 1900 π.Χ. μέχρι το 1900 μ.Χ., την 2η περίοδο από το 1900 μ.Χ. μέχρι το 1950 μ.Χ. και τέλος την σύγχρονη περίοδο από το 1950 μ.Χ. μέχρι και σήμερα.

1η Περίοδος κρυπτογραφίας 1900 π.Χ. έως 1900 μ.Χ.

Την περίοδο αυτή αναπτύχθηκε ένας μεγάλος αριθμός μεθόδων και αλγορίθμων κρυπτογράφησης, οι οποίες βασίζονταν κυρίως σε απλή αντικατάσταση γραμμάτων. Σε αυτές δεν απαιτούνταν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές, αλλά στηρίζονταν στην ευφυΐα και την εφευρετικότητα των δημιουργών τους. Στις όχθες του ποταμού Τίγρη, στην Μεσοποταμία βρέθηκε μια σφηνοειδής επιγραφή η οποία περιγράφει μία μέθοδο κατασκευής σμάλτων για αγγειοπλαστική και θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο (με βάση τον Kahn). Έτσι προκύπτει ότι οι πολιτισμοί της περιοχής, είχαν ασχοληθεί 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 32 έως 35, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καλθένα σφηνοειδή σύμβολα.

Μία από τις παλαιότερες αναφορές στην κρυπτογραφία υπάρχει στην Ιλιάδα του Ομήρου, όπου αναφέρεται η αποστολή ενός κρυπτογραφημένου μηνύματος από τον Βελλεροφόντη. Επίσης στον δίσκο της Φαιστού του 17ου αιώνα π.Χ είναι γραμμένο ένα κείμενο το οποίο δεν έχει αποκρυπτογραφηθεί μέχρι σήμερα. Ο Ηρόδοτος ακόμη περιγράφει πώς μεταφέρονταν κρυπτογραφημένα μηνύματα από τους αγγελιοφόρους. Οι αρχαίοι εβραίοι κρυπτογραφούσαν κάποιες λέξεις στις περιγραφές τους. Ο Πολύβιος ήταν ο πρώτος που χρησιμοποίησε αριθμούς σε μορφή πίνακα για την κωδικοποίηση γραμμάτων.

Όταν η κρυπτογραφία άρχισε να χρησιμοποιείται για στρατιωτικούς σκοπούς, ώστε να αποκρύπτει ζωτικής σημασίας πληροφορίες, έτυχε μελέτης τόσο απ' αυτούς που ήθελαν να κωδικοποιούν μυστικά, όσο και απ' αυτούς που ήθελαν να βρουν τρόπους ώστε να μπορέσουν να αποκωδικοποιήσουν αυτά τα μυστικά. Έτσι η κρυπτογραφία εξελίχθηκε σε επιστήμη.

Η πρώτη στρατιωτική χρήση της ιστορικά, όπως αναφέρει ο Πλούταρχος, αποδίδεται στους Σπαρτιάτες, οι οποίοι τον 5ο περίπου αιώνα π.Χ., εφηύραν την σκυτάλη, που αποτελεί την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποιείται η μέθοδος της μετάθεσης. Σε αυτή, το κείμενο ήταν γραμμένο σε μια λωρίδα περγαμηνής, τυλιγμένη ελικοειδώς, σε μια ξύλινη ράβδο, ορισμένης διαμέτρου. Το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα της σκυτάλης, όταν δε ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της ανάμειξης των γραμμάτων. Το κλειδί αποκρυπτογράφησης ήταν η διάμετρος της σκυτάλης αφού ο παραλήπτης θα έπρεπε να τυλίξει την περγαμηνή σε έναν κύλινδρο ίδιας διαμέτρου με αυτή στην οποία γράφτηκε το μήνυμα. Οι Αιγύπτιοι ιερείς χρησιμοποιούσαν μέθοδο αντίστοιχη με την σκυτάλη των Σπαρτιατών, την οποία χρησιμοποίησε και ο Ιούλιος Καίσαρας. Επίσης μεθόδους κρυπτογράφησης είχαν αναπτύξει και οι Αριστοτέλης, Πυθαγόρας και Νέρωνας.

Τα συστήματα γραπτής αντικατάστασης γραμμάτων, τα βρίσκουμε στην εποχή των Ρωμαίων και κυρίως την εποχή του Ιουλίου Καίσαρα (100-44 π.Χ.). Ο Ιούλιος Καίσαρας έγραφε επιστολές στον Κικέρωνα και σε άλλους φίλους του, αντικαθιστώντας τα γράμματα του κειμένου με γράμματα που βρίσκονται 3 θέσεις μετά, στο Λατινικό Αλφάβητο. Το σύστημα του Καίσαρα χρησιμοποιήθηκε ευρέως και στους επόμενους αιώνες.

Στην διάρκεια του Μεσαίωνα, καθυστέρησε η εξέλιξη της κρυπτογραφίας, επειδή θεωρήθηκε μια μορφή αποκρυφισμού και μαύρης μαγείας.

Οι Άραβες ήταν οι πρώτοι που επινόησαν και χρησιμοποίησαν μεθόδους κρυπτανάλυσης, γύρω στον 14ο αιώνα μ.Χ., με την χρήση της συχνότητας των γραμμάτων του κειμένου, σε συνδυασμό με τις συχνότητες εμφάνισης, στο κείμενο, των γραμμάτων της γλώσσας. Οι Άραβες λοιπόν χρησιμοποίησαν αλγορίθμους αντικατάστασης και μετατόπισης. Το 1412 μ.Χ. ο Al-Kalka-Shandi συμπεριέλαβε την περιγραφή πολλών κρυπτογραφικών συστημάτων στην εγκυκλοπαίδεια Subh al-a'sha και έδωσε σαφείς οδηγίες και παραδείγματα για την κρυπτανάλυση κρυπτογραφημένων κειμένων χρησιμοποιώντας την συχνότητα των χαρακτήρων.

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

Ο Sir Francis Bacon το 1563 μ.Χ. περιέγραψε έναν αλγόριθμο που σήμερα φέρει το όνομά του. Ήταν ένας αλγόριθμος που χρησιμοποιούσε κωδικοποίηση 5 bits. Τον αλγόριθμο αυτόν τον εξέλιξε σαν μια μέθοδο στεγανογραφίας, χρησιμοποιώντας μια μεταβολή στην μορφή των χαρακτήρων μεταφέροντας κάθε bit της κωδικοποίησης. Τα μυστικά της κρυπτολογίας φυλάσσονταν στα μοναστήρια ή στα μυστικά αρχεία των βασιλιάδων, με αποτέλεσμα λίγες μέθοδοι να γίνονται ευρέως γνωστές. Κατά την Αναγέννηση η κρυπτολογία έγινε χωριστή επιστήμη και ταυτόχρονα οι εφαρμογές της αναζητούσαν μια γενική γλώσσα.

Το 1600 ο καρδινάλιος Ρισελιέ χρησιμοποίησε μια κάρτα με τρύπες για τα μηνύματά του. Έτσι όταν τελείωνε γέμιζε τα κενά με λέξεις ώστε να μοιάζει με ένα κανονικό γράμμα. Για την αποκωδικοποίηση χρειαζόταν η κάρτα με την οποία είχε γραφτεί το γράμμα.

Το 1776 ο Αμερικανός Arthur Lee ανέπτυξε έναν κώδικα με βιβλίο, τον οποίο σύντομα υιοθέτησε ο στρατός.

Ο Ιταλός Giovanni Batista Porta, το 1563 μ.Χ., δημοσίευσε το βιβλίο για την κρυπτολογία, "De furtivis literaum notis", με το οποίο έγιναν γνωστά τα πολλαλφαβητικά συστήματα κρυπτογράφησης

καθώς και τα διγραφικά κρυπτογραφήματα, στα οποία, δύο γράμματα αντικαθίστανται με ένα.

Ένας μηχανικός αλγόριθμος κρυπτογράφησης είναι ο κύλινδρος του Jefferson, ο οποίος την δεκαετία του 1790 ανέπτυξε μια συσκευή, για να εφαρμόσει την πολυαλφαβητική αντικατάσταση. Η συσκευή αυτή αποτελείτο από 36 δίσκους, που ο καθένας έφερε και ένα αλφάβητο με διαφορετική διάταξη των γραμμάτων στην περιφέρειά του. Οι δίσκοι αυτοί μπορούσαν να μπου, στον άξονά τους, με οποιαδήποτε σειρά από τις 36 δυνατές διατάξεις. Ο κάθε δίσκος είχε έναν αριθμό και η σειρά τους αποτελούσε κάθε φορά το κλειδί, το οποίο όμως είχε συμφωνηθεί από πριν, από τον αποστολέα και τον παραλήπτη του μηνύματος. Κατά την κρυπτογράφηση ενός μηνύματος, οι δίσκοι περιστρέφονται κατάλληλα ώστε να σχηματιστούν τα γράμματα αυτού σε μια σειρά, κατά μήκος του άξονα. Το κρυπτόγραμμα του μηνύματος αποτελούσε οποιαδήποτε από τις υπόλοιπες 25 γραμμές της συσκευής (από το σύνολο των 26 γραμμών, όσα δηλαδή και τα γράμματα του αγγλικού αλφαβήτου). Από την πλευρά του ο παραλήπτης, αφού διατάξει τους δίσκους στη σειρά που υπαγορεύεται από το κλειδί, περιστρέφει αυτούς κατάλληλα ώστε να σχηματίσει σε μια από τις γραμμές το κρυπτόγραμμα, που έχει λάβει. Τότε σε κάποια από τις υπόλοιπες γραμμές έχει σχηματιστεί το καθαρό μήνυμα. Ο μηχανισμός αυτός χρησιμοποιήθηκε συστηματικά από το 1920, περίπου για μερικές δεκαετίες από το πολεμικό ναυτικό των ΗΠΑ.

Την ίδια εποχή ήταν και ο Γάλλος Vigenere, ο οποίος δημιούργησε τον πίνακα της πολυαλφαβητικής αντικατάστασης, που χρησιμοποιείται ακόμα και σήμερα.

Πρόκειται για έναν κωδικοποιητή πολυαλφαβητικής αντικατάστασης. Σε αυτόν υπήρχαν δύο ομόκεντροι δίσκοι που φέρουν τα γράμματα του αλφαβήτου στις περιφέρειές τους. Ο εξωτερικός δίσκος είχε τα 26 γράμματα σε αλφαβητική σειρά και ένα κενό, ενώ ο εσωτερικός δίσκος είχε απλώς τα 26 γράμματα σε τυχαία σειρά. Επίσης υπήρχαν και δύο δείκτες, (ένας εξωτερικός και ένας εσωτερικός), όταν ο εξωτερικός δείκτης περνούσε από τα 26 γράμματα και το κενό, ο εσωτερικός δείκτης έκανε το ίδιο για τα 26 γράμματα της περιφέρειας του δίσκου του. Κατά την κρυπτογράφηση, ο εξωτερικός δείκτης μετακινείται διαδοχικά στα γράμματα του καθαρού κειμένου, πάντα κατά την φορά των δεικτών του ρολογιού, συμπεριλαμβάνοντας το κενό σαν χαρακτήρα, ενώ τα γράμματα του κρυπτογραφήματος προσδιορίζονταν από τον εσωτερικό δείκτη. Αντίστοιχα προέβαινε ο παραλήπτης κατά την αποκρυπτογράφηση. Σε κάθε λέξη αντιστοιχούσε και ένα διαφορετικό αλφάβητο, λόγω του κενού, αλλά και η ίδια λέξη μπορούσε να κωδικοποιηθεί με διαφορετικά αλφάβητα αν υπήρχαν διαδοχικά γράμματα με αντίστροφη αλφαβητική σειρά ή επαναλαμβανόμενα. Ο C.Wheatstone (1802-1872 μ.Χ.), το 1860 παρουσίασε την πρώτη μηχανική κρυπτοσυσκευή, γνωστή σαν δίσκος του Wheatstone, που ουσιαστικά είναι ένας μηχανικός αλγόριθμος που αποτέλεσε την βάση για την ανάπτυξη των κρυπτομηχανών της 2ης περιόδου της κρυπτογραφίας.

Την μεγαλύτερη αποκρυπτογράφηση αποτελεί, η ανάγνωση των ιερογλυφικών. Το 1652 μ.Χ. ο Γερμανός Ιησουίτης Αθανάσιος Κίρχερ, εξέδωσε ένα λεξικό ερμηνείας των ιερογλυφικών, με τίτλο 'Oedipus Aegyptiacus'. Με βάση αυτό προσπάθησε να ερμηνεύσει τις αιγυπτιακές γραφές, αλλά χωρίς επιτυχία.

Η ερμηνεία των ιερογλυφικών έγινε αργότερα με την "Στήλη της Ροζέτας", που ήταν μία πέτρινη στήλη με το ίδιο κείμενο τρεις φορές γραμμένο, ιερογλυφικά, ελληνικά και ιερατικά. Η στήλη βρέθηκε από τα στρατεύματα του Ναπολέοντα στην Αίγυπτο.

Τέλος δύο μεγάλοι αποκρυπτογράφοι, ο Γιανγκ και ο Σαμπολιάν, ήταν αυτοί που μοιράστηκαν την δόξα της ερμηνείας των ιερογλυφικών. Ένας διάσημος κώδικας είναι ο κώδικας Μορς που αναπτύχθηκε από τον Samuel Mors το 1832 και περιγράφει τον τρόπο κωδικοποίησης του αλφαβήτου σε μακρύς και σύντομους ήχους. Με την ταυτόχρονη ανακάλυψη του τηλέγραφου, ο κώδικας Μορς βοήθησε στην επικοινωνία των ανθρώπων σε μεγάλες αποστάσεις.

Το 1860 οι μεγάλοι κώδικες χρησιμοποιούνταν συχνά στις διπλωματικές επικοινωνίες. Στην διπλωματία και κατά τις περιόδους πολέμου, υπήρχε αυξημένη χρήση της κρυπτογραφίας με χαρακτηριστικό παράδειγμα τα one-time pads, τα οποία χρησιμοποιούνταν ευρέως.

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

2η Περίοδος κρυπτογραφίας 1900 μ.Χ. έως 1950 μ.Χ.

Η περίοδος αυτή καλύπτει χρονικά τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων η κρυπτογραφία αναπτύχθηκε ραγδαία. Τα κρυπτοσυστήματα άρχισαν να γίνονται πολύπλοκα και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές που ονομάζονται κρυπτομηχανές. Το κρυπτόγραμμα υπολογιζόταν ως εξής: $y = b + 1 - x(mod26)$, όπου x είναι η αλφαβητική θέση του γράμματος του καθαρού κειμένου, π.χ. του "a" είναι το 1 του "b" είναι το 2 κτλ. Το b είναι η γραμμή του τετραγώνου του Beaufort που υπαγορεύεται από το κλειδί και το Y η αλφαβητική θέση του κώδικα. Αυτό επαναλαμβανόταν για όλα τα γράμματα του μηνύματος.

Στον 20ο αιώνα υπάρχουν πολλά παραδείγματα για εκτεταμένη χρήση διάφορων κρυπτογραφικών τεχνικών. Από όλες τις ιστορικές προσωπικότητες που συνέβαλαν στην ανάπτυξη της κρυπτογραφίας ο William Frederick Friedman, ιδρυτής των Riverbank Laboratories, κρυπτολόγος της Αμερικάνικης κρυπτανάλυσης, το 1918 έγραψε το βιβλίο "The Index of Coincidence and Its Application in Cryptography", που ακόμα και σήμερα θεωρείται από πολλούς σαν το σημαντικότερο σύγγραμμά πάνω στην κρυπτογραφία κατά τον 20ο αιώνα. Στα τέλη της δεκαετίας του 1920 και στις αρχές της δεκαετίας του 1930, το FBI ίδρυσε ένα γραφείο με σκοπό την αντιμετώπιση της χρήσης της κρυπτογραφίας από τους εγκληματίες. Το πρόβλημα εκείνης της εποχής ήταν το λαθραίο εμπόριο οινόπνευματων ποτών, που σύμφωνα με μια αναφορά, η πολυπλοκότητα της κρυπτογραφίας που χρησιμοποιούσαν οι λαθρέμποροι, ήταν πιο πολύπλοκη από κάθε άλλη που είχε χρησιμοποιηθεί, ακόμα και από κυβερνήσεις ή και κατά την διάρκεια του 1ου Παγκοσμίου Πολέμου.

Το πιο σημαντικό όμως παράδειγμα είναι η χρήση της κρυπτογραφίας στον Β' Παγκόσμιο πόλεμο, του οποίου η έκβαση, υπέρ των συμμάχων και κατά των Γερμανών, κρίθηκε σε ένα πολύ μεγάλο βαθμό στην ικανότητα των συμμάχων, να αποκρυπτογραφούν τα γερμανικά μηνύματα, που στέλνονταν στα γερμανικά υποβρύχια σε Μεσόγειο και Ατλαντικό, υποκλέποντάς τα, πράγμα βέβαια το οποίο δεν μπορούσαν να κάνουν στον ίδιο βαθμό οι Γερμανοί.

Ένας μηχανικός αλγόριθμος είναι και η μηχανή του Hagelin ο οποίος ήταν Σουηδός και την δεκαετία του 1930, ανακάλυψε αυτήν τη μηχανή που ήταν βασισμένη στην πολyalφαβητική αντικατάσταση. Έκανε χρήση ενός συνόλου αλφαβήτων, του ονομαζόμενου τετραγώνου του Beaufort, που συγκρίνεται με τον πίνακα του Vigenere, αλλά με τα γράμματα των αλφαβήτων σε αντίστροφη σειρά.

Μια άλλη περίπτωση είναι οι μηχανές ρότορα, που αποτελούνταν από πολλούς περιστρεφόμενους κύλινδρους. Κάθε κύλινδρος έχει 26 εισόδους και εξόδους, με κάθε είσοδο να συνδέεται με μία έξοδο. Κάθε γράμμα του μηνύματος κωδικοποιείται στον πρώτο κύλινδρο, στην συνέχεια στον δεύτερο κτλ. Ο πιο απομακρυσμένος από τον χειριστή κύλινδρος, περιστρέφεται με την εισαγωγή κάθε γράμματος του μηνύματος, με αποτέλεσμα μια διαφορετική σύνδεση μεταξύ εισόδων και εξόδων αυτού, δηλαδή διαφορετικό αλφάβητο αντικατάστασης. Όταν αυτός συμπληρώνει 26 περιστροφές και επανέρχεται στην αρχική κατάσταση, τότε ο γειτονικός του κύλινδρος περιστρέφεται κατά μία θέση, με αποτέλεσμα ένα άλλο αλφάβητο. Αυτό συνεχίζεται για όλους τους κύλινδρους. Αν έχουμε δηλαδή μια μηχανή με τρεις κύλινδρους έχουμε $26 \times 26 \times 26$ συνδυασμούς αλφαβήτων και έτσι σε ένα μήνυμα με λιγότερα από $26 \times 26 \times 26$ γράμματα, κάθε γράμμα θα κωδικοποιείται από διαφορετικό συνδυασμό αλφαβήτων.

Παραδείγματα μηχανών ρότορα είναι η μηχανή Enigma που αναπτύχθηκε από τον Arthur Sherbius και χρησιμοποιήθηκε από τους Γερμανούς στον 2ο Παγκόσμιο Πόλεμο, καθώς και η μηχανή Purple που αναπτύχθηκε χρησιμοποιώντας τεχνικές που ανακαλύφθηκαν από τον Harbat O. Yardley και χρησιμοποιήθηκε από τους Ιάπωνες.

Η κρυπτανάλυση την περίοδο του 20ου αιώνα απαιτούσε μεγάλο αριθμό προσωπικού. Παραδείγματα τέτοιων μηχανών έχουμε από τους Γερμανούς, π.χ. με την κρυπτομηχανή Enigma. Το σύστημα αυτό των Γερμανών, παραβίασε ο Πολωνός Marian Rajewski, το 1932, χρησιμοποιώντας τα θεωρητικά μαθηματικά. Το 1939 όμως οι Γερμανοί έκαναν κάποιες αλλαγές στην Enigma που οι Πολωνοί δεν μπόρεσαν να παρακολουθήσουν, γι' αυτό συνεργάστηκαν με Γάλλους και Βρετανούς. Αυτό οδήγησε σε συνεχείς αποκρυπτογραφήσεις, που έγιναν στο Κέντρο της Βρετανικής Υπηρεσίας Αποκρυπτογράφησης, παρά τις συνεχείς παραλλαγές εκ μέρους των Γερμανών.

Μετά το 1940 οι Αμερικανοί έσπασαν αρκετά κρυπτογραφήματα των Ιαπώνων, όπως το JN-25, που οδήγησε τους Αμερικανούς στην νίκη στην ναυμαχία του Μίντγουεϊ, την μηχανή Purple, την μηχανή M και την μηχανή Red.

Συμμαχικές κρυπτομηχανές κατά τον Β' Παγκόσμιο Πόλεμο ήταν, η Βρετανική Typex και η Αμερικανική Sigaba.

3η Περίοδος κρυπτογραφίας 1950 μ.Χ. μέχρι και σήμερα

Αυτή η περίοδος χαρακτηρίζεται από την έξαρση της ανάπτυξης στους κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων.

Η σύγχρονη κρυπτογραφία ξεκινάει με τον Claude Shannon, που θεωρείται ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας, όπου το 1949 εισήγαγε την ιδέα των δικτύων αντικατάστασης - μετάθεσης (substitution-permutation (S-P) networks ή ΔΑΜ).

Από την δεκαετία του 60 και μετά, η κρυπτογραφία αναπτύχθηκε ραγδαία, σε αυτό βοήθησε η εξέλιξη των υπολογιστών και των τηλεπικοινωνιών. Άρχισε με την εργασία του Feistel της IBM το 70 και κατέληξε στα μέσα της δεκαετίας του 1970 και συγκεκριμένα στις 17 Μαρτίου του 1975, όταν και έγινε η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES (Data Encryption Standard), το οποίο είναι ένα τυποποιημένο μέσο για την ασφάλεια του ηλεκτρονικού εμπορίου σε πολλά οικονομικά ιδρύματα στον κόσμο.

Αυτό μαζί με τις παραλλαγές του 3DES ή TDES, χρησιμοποιούνται μέχρι και σήμερα. Όμως ο DES, το 2001 αντικαταστάθηκε από τον AES.

Το 1976 οι Diffie και Hellman εισήγαγαν την έννοια της κρυπτογραφίας δημόσιου κλειδιού, το οποίο έφερε μια επανάσταση στην επιστήμη της κρυπτογραφίας.

Το 1978 οι Rivest, Shamir και Adleman ανακάλυψαν την πρακτική εφαρμογή RSA, (από τα αρχικά των ονομάτων τους), ή μέθοδος του προταθέντος σχήματος. Αυτή βασίζεται στην παραγοντοποίηση μεγάλων ακεραίων που ήταν ένα πολύ δύσκολο και σύνθετο πρόβλημα. Το RSA παρά τις μεγάλες προόδους που έγιναν, ιδιαίτερα την δεκαετία του 80, παραμένει και σήμερα μια από τις πιο ασφαλείς μεθόδους κρυπτογράφησης.

Στα μέσα της δεκαετίας του 1980 ο αλγόριθμος ROT 13 χρησιμοποιήθηκε από χρήστες του USENET για να μην μπορούν να δουν τα μηνύματα με επιλήψιμο περιεχόμενο χρήστες που δεν πρέπει. Λίγο αργότερα, το 1990, μια ανακάλυψη από τους Xuejia Lai και James Masey οδήγησε σε ένα δυνατότερο, 128-bit key cipher με σκοπό την αντικατάσταση του γερασμένου DESstandard. Ο αλγόριθμος IDEA που σχεδιάστηκε από αυτούς τους δύο με σκοπό να είναι πιο αποδοτικός με γενικής χρήσης υπολογιστές, όπως αυτούς που χρησιμοποιούνται από τις επιχειρήσεις και τα νοικοκυριά.

Το 1991 ο Phil Zimmerman εξέδωσε την πρώτη έκδοση του Pretty Good Privacy (PGP), σαν ένα προϊόν ελεύθερα διαθέσιμο, το οποίο χρησιμοποιεί τον αλγόριθμο IDEA. Το PGP, ένα δωρεάν πρόγραμμά του, παρέχει στρατιωτικού επιπέδου αλγορίθμους ασφαλείας στην κοινότητα του

Internet, έχει εξελιχθεί σε πρότυπο κρυπτογραφίας, λόγω της ευρείας διάδοσής του. Το 1994 ο καθηγητής Ron Rivest, ο οποίος βοήθησε στην ανάπτυξη του RSA, δημοσίευσε έναν νέο αλγόριθμο τον RC5. Τέλος μια από τις πιο σημαντικές προσφορές της κρυπτογραφίας δημόσιου κλειδιού ήταν η ψηφιακή υπογραφή.

1.3 Βασικές αρχές κρυπτογραφίας

Από την απαρχή του ανθρώπινου πολιτισμού μέχρι τις υψηλά δικτυωμένες κοινωνίες στις οποίες ζούμε σήμερα, η επικοινωνία αποτελούσε πάντοτε ένα αναπόσπαστο κομμάτι της ύπαρξής μας. Η επικοινωνία αυτή σήμερα έχει πάρει διάφορες μορφές, λόγω της τεχνολογικής εξέλιξης, με πιο σημαντική το διαδίκτυο.

Τα δίκτυα υπολογιστών, στα πρώτα χρόνια της δημιουργίας τους, χρησιμοποιήθηκαν από ερευνητές με αποκλειστικό σκοπό την αποστολή ηλεκτρονικού ταχυδρομείου, χωρίς να δίνουν μεγάλη σημασία στην ασφάλεια και την προστασία αυτών τα οποία έγραφαν. Σήμερα όμως που εκατομμύρια χρηστών χρησιμοποιούν τα δίκτυα για διεκπεραίωση τραπεζικών συναλλαγών, αγορές ή ακόμα και για αποπληρωμή των φόρων τους, η ασφάλεια δικτύων ανακύπτει ως ένα σοβαρό, μαζικό πρόβλημα. Για να αντιμετωπιστεί αυτό το πρόβλημα, αναπτύχθηκαν τα τελευταία χρόνια πολλά διαφορετικά μέτρα και υπηρεσίες, τα οποία πάρα τη διαφορετικότητά τους, θα πρέπει να ικανοποιούν 4 σημαντικές προϋποθέσεις ασφαλείας: [1]

- **Απόρρητο(εμπιστευτικότητα):** αφορά στο να κρατούνται οι πληροφορίες ιδιωτικές και μυστικές έτσι ώστε μόνο ο εξουσιοδοτημένος παραλήπτης να μπορεί να τις καταλαβαίνει. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και κωδικοποιώντας τα δεδομένα κατά την αποστολή τους. Η εμπιστευτικότητά μπορεί να εφαρμοστεί σε όλο το μήνυμα ή σε ένα τμήμα του. Για την εξασφάλιση της εμπιστευτικότητας μπορεί να χρησιμοποιηθεί, ανάλογα με την περίπτωση σε:
 - κρυπτογράφηση end to end, όπου τα δεδομένα αποστέλλονται κρυπτογραφημένα και αποκρυπτογραφούνται όταν τα παραλάβει ο χρήστης, για τον οποίο προορίζονται. Έτσι τα δεδομένα δεν είναι δυνατόν να αναγνωστούν από τους ενδιάμεσους κόμβους του δικτύου, στον βαθμό βέβαια που η κρυπτογραφική τεχνική είναι ασφαλής.
 - κρυπτογράφηση link to link, όπου τα δεδομένα αποστέλλονται κρυπτογραφημένα και αποκρυπτογραφούνται, όχι μόνο από τον τελικό χρήστη, αλλά και από τους ενδιάμεσους κόμβους του δικτύου. Έτσι αποστέλλονται κρυπτογραφημένα δεδομένα από έναν κόμβο σε άλλον και ταυτόχρονα κοινοποιούνται σε όλους τους ενδιάμεσους κόμβους.
- **Πιστοποίηση αυθεντικότητας:** αφορά στην απόδειξη της ταυτότητας του αποστολέα στον παραλήπτη, έτσι ώστε ο παραλήπτης να μπορεί να είναι σίγουρος ότι ο αποστολέας είναι πράγματι αυτός που ισχυρίζεται ότι είναι. Με την διαδικασία της αυθεντικοποίησης μπορεί να εξασφαλιστεί η γνησιότητα ενός μηνύματος. Η πιστοποίηση μπορεί να πραγματοποιηθεί με τρεις βασικές μεθόδους:
 - Με κάτι που γνωρίζουμε, όπως π.χ. το PIN μιας τραπεζικής κάρτας ή τον κωδικό ενός λογαριασμού (password).
 - Με κάτι που βρίσκεται στην ιδιοκτησία μας, όπως π.χ. το κλειδί μιας πόρτας ή μια τραπεζική κάρτα.

- Με κάτι που έχουμε εκ γενετής, π.χ. φωνή, ίριδα του ματιού, δακτυλικά αποτυπώματα κτλ.

Με την διαδικασία της αυθεντικοποίησης μπορεί να εξασφαλιστεί η γνησιότητα ενός μηνύματος. Γενικά, είναι η πιο βασική υπηρεσία ασφάλειας που μπορεί να προσφέρει ένα δίκτυο υπολογιστών, καθώς παρέχει:

- προστασία απέναντι σε μη εξουσιοδοτημένους δοσοληψίες
- εξασφαλίζει την γνησιότητα ενός μηνύματος
- εξασφαλίζει την νομιμότητα ενός χρήστη ή αποστολέα
- εξασφαλίζει την εγκυρότητα ενός τερματικού υπολογιστή

Η αυθεντικοποίηση σε ένα περιβάλλον δικτύου υπολογιστών, όπου εμπλέκεται μεγάλος αριθμός χρηστών, επιβάλλεται η δημιουργία ενός κέντρου ελέγχου (που ονομάζεται κέντρο αυθεντικοποίησης), το οποίο διευκολύνει την διαδικασία της αυθεντικοποίησης, με την παροχή αναγκαίων πληροφοριών για κάθε εμπλεκόμενο χρήστη. Απαραίτητη προϋπόθεση για την ύπαρξη ενός τέτοιου κέντρου, είναι η αποδοχή του από όλα τα εμπλεκόμενα μέρη, καθώς το κέντρο κατέχει και διαχειρίζεται πληροφορίες, η αποκάλυψη και τροποποίηση των οποίων, σημαίνει την υπονόμηση του συστήματος ασφάλειας.

Επειδή στην λειτουργία του κέντρου αυθεντικοποίησης εμπλέκεται και ο ανθρώπινος παράγοντας, ο οποίος μπορεί να συντελέσει στην εξασθένηση της ασφάλειας του συστήματος, προτάθηκε τελευταία, κάποιες από τις αρμοδιότητες του κέντρου να μεταφερθούν στους χρήστες. Η υλοποίηση ενός τέτοιου συστήματος μπορεί να επιτευχθεί με την βοήθεια έξυπνων καρτών (smart cards), στις οποίες καταχωρούνται μυστικά κλειδιά, αλγόριθμοι και χαρακτηριστικά των χρηστών.

- Έλεγχος ακεραιότητας: αφορά στο να διασφαλίσει ότι η πληροφορία του μηνύματος δεν έχει αλλοιωθεί κατά τη διάρκεια της μεταφοράς της ή της αποθήκευσής της στο δίκτυο. Οποιοδήποτε μη εξουσιοδοτημένο άτομο δε θα πρέπει να είναι σε θέση να αλλάξει την πληροφορία κατά τη μεταφορά της. Η υπηρεσία παρέχεται από μηχανισμούς κρυπτογραφίας όπως η ψηφιακή υπογραφή και μπορεί να εφαρμοστεί σε ολόκληρο το μήνυμα ή σε επιλεγμένα τμήματα αυτού.
- Μη αποκήρυξη: αφορά στο να διασφαλίσει ότι ο αποστολέας του μηνύματος δε θα αρνηθεί ότι πράγματι έστειλε την πληροφορία. Σ' αυτήν την υπηρεσία συνδυάζονται οι υπηρεσίες της πιστοποίησης και της ακεραιότητας. Στην ασύμμετρη κρυπτογραφία παρέχονται ψηφιακές υπογραφές, τέτοιες ώστε μόνο ο αποστολέας του μηνύματος θα μπορούσε να έχει στην κατοχή του. Αυτό έχει ως αποτέλεσμα, ο οποιοσδήποτε, και συνεπώς και ο παραλήπτης, να βρίσκεται σε θέση να επιβεβαιώσει την ψηφιακή υπογραφή του αποστολέα. Ένας άλλος μηχανισμός, (πέρα από την ψηφιακή υπογραφή), είναι η ύπαρξη ενός έμπιστου κέντρου ελέγχου.

1.4 Τεχνικοί όροι και έννοιες

Κρυπτογράφηση (encryption) ονομάζεται η διαδικασία κατά την οποία ένα μήνυμα μετασχηματίζεται με τη βοήθεια ενός κρυπτογραφικού αλγορίθμου σε μια ακατανόητη μορφή ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν πέραν του εξουσιοδοτημένου παραλήπτη. Η αντίστροφη διαδικασία κατά την οποία από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται **αποκρυπτογράφηση** (decryption).

Κρυπτογραφικός Αλγόριθμος (cipher) είναι η μέθοδος μετασχηματισμού δεδομένων σε τέτοια μορφή η οποία δεν επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη.

Αρχικό κείμενο (plaintext) είναι το μη κρυπτογραφημένο μήνυμα ή δεδομένα τα οποία είναι σε μορφή που μπορούν να διαβαστούν και τα οποία παίρνει ο αλγόριθμος ως είσοδο.

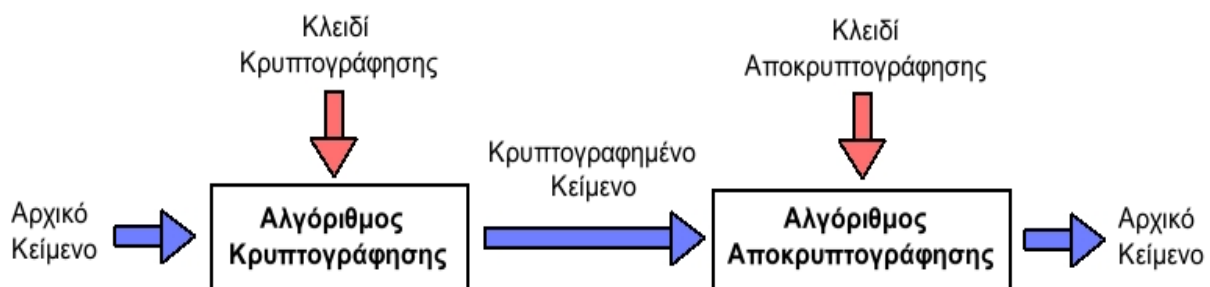
Κλειδί (key) είναι ένας αριθμός bit που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.

Κρυπτογραφημένο κείμενο (ciphertext) είναι το αποτέλεσμα που προκύπτει μετά την εφαρμογή ενός κρυπτογραφικού αλγορίθμου πάνω στο αρχικό κείμενο.

Κρυπτανάλυση (cryptanalysis) είναι η επιστήμη που ασχολείται με το 'σπάσιμο' κάποιας κρυπτογραφικής τεχνικής έτσι ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.

Η διαδικασία των δύο μεθόδων, δηλαδή κρυπτογράφηση – αποκρυπτογράφηση, εφαρμοζόμενη σε ένα μήνυμα ή σε κάποια δεδομένα τα οποία είναι προς μετάδοση, γίνεται αφ' ενός με έναν αλγόριθμο κρυπτογράφησης (cipher) και αφ' ετέρου με ένα κλειδί κρυπτογράφησης (key). Τις πιο πολλές φορές ο εν λόγω αλγόριθμος είναι γνωστός, όμως για να διατηρείται η εμπιστευτικότητα του μεταδιδόμενου μηνύματος θα πρέπει το κλειδί με το οποίο γίνεται η κρυπτογράφηση να κρατιέται μυστικό. Η μονάδα μέτρησης για το μέγεθος του κλειδιού κρυπτογράφησης είναι τα bits. Έτσι το γενικό συμπέρασμα είναι ότι όσο μεγαλύτερο, δηλαδή περισσότερα bits, είναι το κλειδί κρυπτογράφησης, τόσο πιο δύσκολο είναι να γίνει αποκρυπτογράφηση στο μεταδιδόμενο μήνυμα ή δεδομένα, από οποιονδήποτε τρίτο που δεν είναι εξουσιοδοτημένος να το κάνει.

Η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης παρουσιάζεται στο παρακάτω σχήμα:



Σχήμα 1.1: Σύστημα Κρυπτογράφησης Αποκρυπτογράφησης

Ο κύριος στόχος της κρυπτογραφίας είναι να δοθεί η δυνατότητα, σε δύο πρόσωπα να επικοινωνούν μεταξύ τους με ασφάλεια, όταν το κανάλι επικοινωνίας τους δεν είναι ασφαλές. Έτσι δεν μπορεί ένα τρίτο μη εξουσιοδοτημένο άτομο να καταλάβει το τι λέει ένα μήνυμα που στέλνει κάποιο άτομο σε ένα άλλο.

Ένα κρυπτόςυστημα (σύνολο διαδικασιών κρυπτογράφησης - αποκρυπτογράφησης) αποτελείται από μία πεντάδα (P, C, k, E, D) :

- Το P είναι ο χώρος όλων των δυνατών μηνυμάτων ή αλλιώς ανοικτών κειμένων
- Το C είναι ο χώρος όλων των δυνατών κρυπτογραφημένων μηνυμάτων ή αλλιώς κρυπτοκειμένων
- Το k είναι ο χώρος όλων των δυνατών κλειδιών ή αλλιώς κλειδοχώρος
- Η E είναι ο κρυπτογραφικός μετασχηματισμός ή κρυπτογραφική συνάρτηση
- Η D είναι η αντίστροφη συνάρτηση ή μετασχηματισμός αποκρυπτογράφησης

Η συνάρτηση κρυπτογράφησης E δέχεται δύο παραμέτρους, μία από τον χώρο P και μία από τον χώρο k και παράγει μία ακολουθία η οποία ανήκει στον χώρο C .

Η συνάρτηση αποκρυπτογράφησης D δέχεται 2 παραμέτρους, τον χώρο C και τον χώρο k και παράγει μια ακολουθία που ανήκει στον χώρο P .

Πρώτα ο αποστολέας του μηνύματος διαλέγει τυχαία ένα κλειδί, το οποίο έχει μήκος n , από τον χώρο κλειδιών k , και στέλνει το κλειδί μέσα από ένα κανάλι που είναι ασφαλές. Ακολούθως ο αποστολέας δημιουργεί ένα μήνυμα από τον χώρο μηνυμάτων C . Έτσι η συνάρτηση κρυπτογράφησης λαμβάνει το κλειδί και το μήνυμα παράγοντας έναν γρίφο ο οποίος στέλνεται μέσα από ένα μη ασφαλές κανάλι επικοινωνίας. Τελικά η συνάρτηση αποκρυπτογράφησης λαμβάνει το κλειδί και τον γρίφο και έτσι παράγει την ισοδύναμη ακολουθία μηνύματος.

Αν τώρα κάποιο τρίτο άτομο παρακολουθεί μεν την επικοινωνία μεταξύ δύο ατόμων αλλά δεν έχει στην κατοχή του το κλειδί με το οποίο έγινε η κρυπτογράφηση, δεν μπορεί να δημιουργήσει το αρχικό μήνυμα. Διακρίνουμε εδώ δύο περιπτώσεις, στην πρώτη το τρίτο άτομο παρακολουθεί όλη την επικοινωνία (τα μηνύματα) οπότε θα προσπαθήσει να βρει το κλειδί αποκρυπτογράφησης, ενώ στην δεύτερη περίπτωση (το τρίτο άτομο) ενδιαφέρεται μόνο για το υπάρχον μήνυμα και θα έχει μια εκτίμηση για τις πληροφορίες που περιέχει το μήνυμα.

1.5 Είδη κρυπτογραφίας

1.5.1 Συμμετρική Κρυπτογραφία

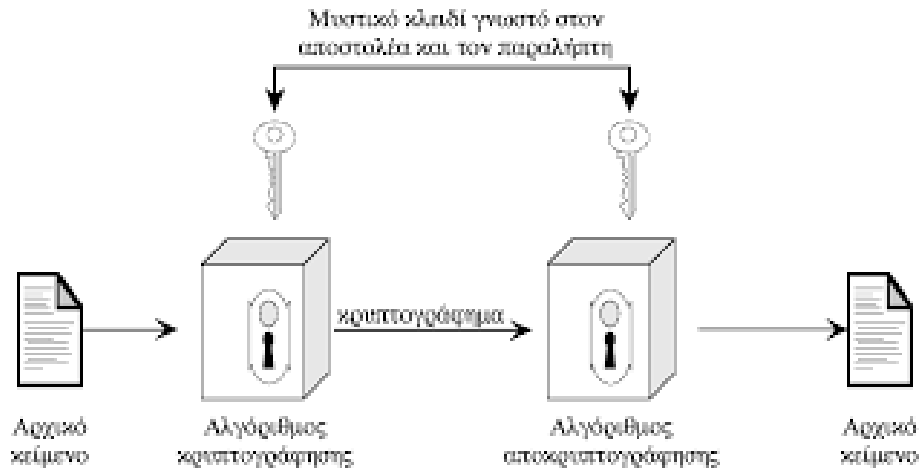
Η συμμετρική κρυπτογραφία βασίζεται στην ύπαρξη ενός μοναδικού κλειδιού, γνωστό ως μυστικό ή συμμετρικό κλειδί (secret key), με το οποίο γίνεται η κρυπτογράφηση και η αποκρυπτογράφηση της πληροφορίας. Ο αποστολέας και ο παραλήπτης είναι οι μοναδικές οντότητες που γνωρίζουν και χρησιμοποιούν το μυστικό κλειδί. Τα μηνύματα προς κρυπτογράφηση, γνωστά ως το αρχικό κείμενο (plaintext), κρυπτογραφούνται με χρήση του συμμετρικού (ή μυστικού) κλειδιού. Η διαδικασία της κρυπτογράφησης έχει ως έξοδο ένα κείμενο σε ακατανόητη μορφή, γνωστό ως κρυπτογράφημα (ciphertext). Η ασφάλεια της μεταδιδόμενης πληροφορίας επιτυγχάνεται ακριβώς επειδή το κρυπτογράφημα μεταδίδεται σε ακατανόητη μορφή. Η διαδικασία της ανάκτησης της αρχικής πληροφορίας με τη χρήση του ίδιου συμμετρικού κλειδιού ονομάζεται αποκρυπτογράφηση. Υπάρχουν δύο απαιτήσεις για την ασφαλή χρήση της συμμετρικής κρυπτογράφησης:

- Χρειαζόμαστε έναν ισχυρό αλγόριθμο κρυπτογράφησης. Κατ' ελάχιστο, θα θέλαμε ο αλγόριθμος να είναι τέτοιος ώστε ένας αντίπαλος, ο οποίος γνωρίζει τον αλγόριθμο και έχει πρόσβαση σε ένα ή περισσότερα κρυπτογραφημένα κείμενα, να μην είναι ικανός να αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο ή να ανακαλύψει το κλειδί.
- Ο αποστολέας και ο παραλήπτης πρέπει να έχουν προμηθευτεί αντίγραφα του μυστικού κλειδιού με ασφαλή τρόπο και πρέπει να κρατούν το κλειδί ασφαλές. Εάν κάποιος μπορεί να ανακαλύψει το κλειδί και γνωρίζει τον αλγόριθμο, κάθε επικοινωνία που χρησιμοποιεί αυτό το κλειδί είναι αναγνώσιμη.

Ένα σχήμα συμμετρικής κρυπτογραφίας έχει πέντε στοιχεία:

- **Το αρχικό κείμενο:** είναι το αρχικό μήνυμα ή δεδομένα που τροφοδοτούνται σαν είσοδος στον αλγόριθμο.
- **Τον αλγόριθμο κρυπτογράφησης:** εκτελεί διάφορες αντικαταστάσεις και μετασχηματισμούς στο καθαρό κείμενο.
- **Το μυστικό κλειδί:** είναι επίσης μια είσοδος στον αλγόριθμο κρυπτογράφησης. Οι ακριβείς αντικαταστάσεις και οι μετασχηματισμοί που εκτελούνται από τον αλγόριθμο εξαρτώνται από το κλειδί.
- **Το κρυπτογραφημένο κείμενο:** είναι το περιπλεγμένο κείμενο που παράγεται σαν έξοδος. Εξαρτάται από το καθαρό κείμενο και το μυστικό κλειδί. Για ένα συγκεκριμένο μήνυμα, δύο διαφορετικά κλειδιά θα παράγουν δύο διαφορετικά κρυπτογραφημένα κείμενα.
- **Τον αλγόριθμο αποκρυπτογράφησης:** είναι απαραίτητα ο αλγόριθμος κρυπτογράφησης εκτελεσμένος αντίστροφα. Παίρνει το κρυπτογραφημένο κείμενο και το μυστικό κλειδί και παράγει το αρχικό καθαρό κείμενο.

Στο Σχήμα 1.2 περιγράφεται η διαδικασία της συμμετρικής κρυπτογραφίας.



Σχήμα 1.2: Διαδικασία Συμμετρικής Κρυπτογραφίας

Η συμμετρική κρυπτογραφία χρησιμοποιείται εδώ και χιλιάδες χρόνια. Ένας από τους παλιότερους γνωστούς κώδικες κρυπτογραφίας είναι ο αλγόριθμος του Καίσαρα, που αποτελεί έναν απλό κώδικα αντικατάστασης. Άλλοι γνωστοί και πιο σύγχρονοι αλγόριθμοι είναι οι αλγόριθμοι DES, IDEA, RC5, και AES.

1.5.2 Ασύμμετρη Κρυπτογραφία ή Κρυπτογραφία Δημοσίου Κλειδιού

Στο τέλος της δεκαετίας του 1970 οι Whitfield Diffie και Martin Hellman βρήκαν έναν διαφορετικό τρόπο στην διαχείριση των κλειδιών κρυπτογράφησης, σε σχέση με την κρυπτογράφηση συμμετρικού κλειδιού, ώστε να περιοριστούν τα προβλήματα που παρουσιάζονται με αυτήν την μέθοδο. Ο τρόπος αυτός είναι η κρυπτογράφηση με Δημόσιο Κλειδί ή ασύμμετρη κρυπτογραφία.

Στην ασύμμετρη κρυπτογραφία χρησιμοποιείται άλλο κλειδί για την κρυπτογράφηση και άλλο για την αποκρυπτογράφηση. Για την κρυπτογράφηση χρησιμοποιείται το λεγόμενο δημόσιο κλειδί (public key), ενώ για την αποκρυπτογράφηση το ιδιωτικό κλειδί (private key). Η αποκρυπτογράφηση μπορεί να γίνει μόνο με το ιδιωτικό κλειδί. Επίσης τα δύο αυτά κλειδιά έχουν κάποια μαθηματική σχέση μεταξύ τους, τέτοια η οποία αποτρέπει τον υπολογισμό του ενός από το άλλο.

Ένα σχήμα κρυπτογράφησης δημόσιου κλειδιού έχει τα εξής συστατικά:

- **Το αρχικό κείμενο:** είναι το αρχικό μήνυμα ή δεδομένα που τροφοδοτούνται σαν είσοδος στον αλγόριθμο.
- **Τον αλγόριθμο κρυπτογράφησης:** εκτελεί διάφορες αντικαταστάσεις και μετασχηματισμούς στο καθαρό κείμενο.
- **Το δημόσιο και το ιδιωτικό κλειδί:** είναι ένα ζεύγος κλειδιών που έχουν επιλεγεί, έτσι ώστε αν το ένα χρησιμοποιείται για την κρυπτογράφηση το άλλο χρησιμοποιείται για την αποκρυπτογράφηση. Οι ακριβείς μετασχηματισμοί, που εκτελούνται από τον αλγόριθμο κρυπτογράφησης, εξαρτώνται από το δημόσιο ή το ιδιωτικό κλειδί που παρέχεται σαν είσοδος.
- **Τον αλγόριθμο αποκρυπτογράφησης:** ο αλγόριθμος αυτός δέχεται το κωδικοποιημένο κείμενο και το ταιριαστό κλειδί και στην συνέχεια παράγει το αρχικό καθαρό κείμενο.

Για τα δύο αυτά κλειδιά, όπως υποδηλώνεται και από το όνομά τους, το μεν πρώτο (το δημόσιο) κοινοποιείται και μπορεί να χρησιμοποιηθεί από όλους τους χρήστες, ενώ το δεύτερο (το ιδιωτικό) το γνωρίζει μόνο ο κάτοχός του.

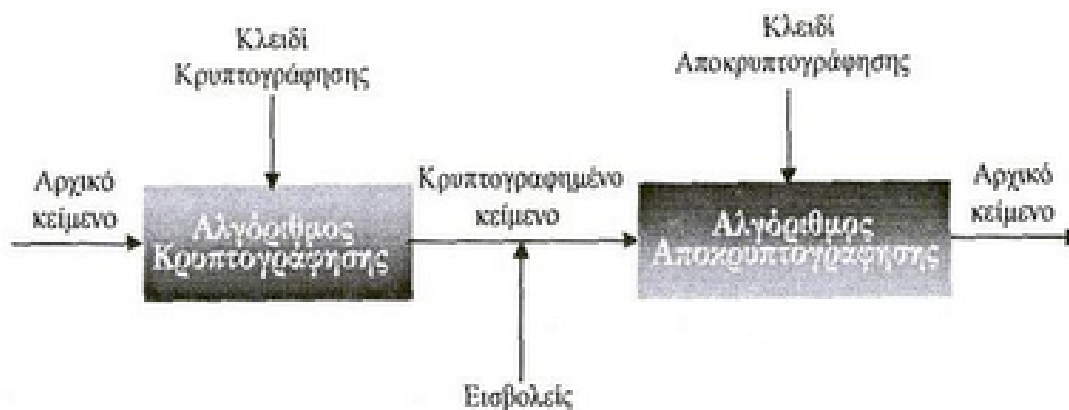
Οι αλγόριθμοι κρυπτογράφησης έχουν τα παρακάτω χαρακτηριστικά:

- Είναι υπολογιστικά ανέφικτο να προσδιοριστεί το κλειδί αποκρυπτογράφησης με δεδομένη μόνο την γνώση του κρυπτογραφικού αλγορίθμου και του κλειδιού αποκρυπτογράφησης.
- Για τα περισσότερα σχήματα δημόσιου κλειδιού, μπορεί να χρησιμοποιηθεί για κρυπτογράφηση οποιοδήποτε από τα δύο σχετικά κλειδιά, με το άλλο να χρησιμοποιείται για αποκρυπτογράφηση.

Προσεγγίζοντας λοιπόν το θέμα με αυτόν τον τρόπο, όλοι οι χρήστες οι οποίοι συμμετέχουν, έχουν πρόσβαση μόνο στα δημόσια κλειδιά, ενώ τα ιδιωτικά παράγονται σε τοπικό επίπεδο από τον καθένα που συμμετέχει, έτσι δεν υπάρχει καμία αιτία για να διανεμηθούν. Αν ο κάθε χρήστης προστατεύει το ιδιωτικό του κλειδί, δεν υπάρχει ποτέ περίπτωση να αποκαλυφθεί και άρα η επικοινωνία του είναι ασφαλής.

Βέβαια ο κάθε χρήστης έχει την δυνατότητα οποιαδήποτε στιγμή να αλλάξει το ιδιωτικό του κλειδί και να κάνει γνωστό το αντίστοιχο δημόσιο κλειδί ώστε να αντικατασταθεί το παλιό (δημόσιο κλειδί). Γίνεται γνωστό ότι τους αλγορίθμους κρυπτογράφησης δημόσιου κλειδιού, δεν τους χρησιμοποιούμε μόνο για την διαδικασία της κρυπτογράφησης, αλλά και για την εξακρίβωση γνησιότητας, δηλαδή για τις ηλεκτρονικές υπογραφές.

Το σχήμα 1.3 περιγράφει τη διαδικασία κρυπτογράφησης δημοσίου κλειδιού. Ο αποστολέας κρυπτογραφεί με το δημόσιο κλειδί του παραλήπτη, το οποίο είναι ελεύθερα διαθέσιμο, το μήνυμα που θέλει να του στείλει. Το κρυπτογραφημένο μήνυμα φτάνει στον παραλήπτη ο οποίος το αποκρυπτογραφεί με το ιδιωτικό κλειδί του.



Σχήμα 1.3: Διαδικασία Κρυπτογράφησης Δημόσιου Κλειδιού

Η κρυπτογραφία δημόσιου κλειδιού χρησιμοποιείται σε δύο περιπτώσεις αφενός για την κρυπτογράφηση και αφετέρου για την αποκρυπτογράφηση μηνυμάτων ή δεδομένων και για την ψηφιακή υπογραφή. Στο είδος αυτής της κρυπτογράφησης η ασφάλεια της επικοινωνίας βασίζεται στο ότι είναι αδύνατον να παραχθεί το ιδιωτικό κλειδί από το δημόσιο. Θεωρητικά βέβαια αυτό μπορεί να γίνει, αλλά το κόστος, ο χρόνος για να επιτευχθεί, η μνήμη και η υπολογιστική ισχύς είναι παράγοντες οι οποίοι το καθιστούν σχεδόν αδύνατο.

Τα βασικά χαρακτηριστικά του δημόσιου και του ιδιωτικού κλειδιού είναι:

- κάθε κλειδί είναι ένα δυαδικό αλφαριθμητικό
- τα κλειδιά, δημόσια και ιδιωτικά, παράγονται ταυτόχρονα από ένα ειδικό λογισμικό πρόγραμμα
- τα δύο κλειδιά δημόσιο και ιδιωτικό δεν ταυτίζονται, έχουν όμως μια σχέση μεταξύ τους η οποία είναι μοναδική, ώστε να μπορούν να χρησιμοποιηθούν και για την κρυπτογράφηση, αλλά και για την αποκρυπτογράφηση μηνυμάτων ή δεδομένων. Η διαδικασία για την παραγωγή τους εξασφαλίζει ότι από την μια μεριά το κάθε κλειδί έχει μοναδική σχέση με το ταίρι του και από την άλλη δεν μπορεί να παραχθεί το ένα από το άλλο.
- το ένα κλειδί συμπληρώνει το άλλο, δηλαδή οι πληροφορίες που κρυπτογραφούνται με το ένα κλειδί, αποκρυπτογραφούνται με το άλλο και αντίστροφα.
- ο κάθε χρήστης ο οποίος συμμετέχει σε μια επικοινωνία δημόσιου κλειδιού, έχει το δικό του ζευγάρι κλειδιών.
- το ιδιωτικό κλειδί προστατεύεται από τον ιδιοκτήτη του και χρησιμοποιείται για την ψηφιακή υπογραφή μηνυμάτων
- το δημόσιο κλειδί μπορεί να διανέμεται ελεύθερα και γι' αυτό είναι προσβάσιμο από τον καθένα. Χρησιμοποιείται για να πιστοποιούνται οι ψηφιακές υπογραφές των χρηστών, να κρυπτογραφούνται μηνύματα ή δεδομένα καθώς και για να αποθηκεύεται μέσα σε ψηφιακά πιστοποιητικά, τα οποία παρέχουν φυσικά ακεραιότητα και αυθεντικότητα όσο αφορά τον κάτοχο του συγκεκριμένου κλειδιού.
- τα δημόσια κλειδιά μπορούν να διανέμονται ελεύθερα, ενώ τα ιδιωτικά δεν θα πρέπει να γίνονται γνωστά σε άτομα τα οποία δεν είναι εξουσιοδοτημένα

1.5.3 Υβριδική Κρυπτογραφία Ψηφιακού Φακέλου

Ένας από τους τρόπους για να μπορέσει να υπάρξει μια ασφαλής επικοινωνία μεταξύ χρηστών, είναι η χρήση της υβριδικής κρυπτογραφίας ή όπως είναι γνωστότερη σαν κρυπτογραφία ψηφιακού φακέλου (digital envelope). Αυτό το είδος της κρυπτογράφησης χρησιμοποιεί συγχρόνως τις τεχνικές της συμμετρικής αλλά και της ασύμμετρης κρυπτογραφίας, επιπλέον μπορεί να χρησιμοποιηθεί για πολλούς παραλήπτες ταυτόχρονα.

Τα βήματα τα οποία θα ακολουθηθούν ώστε να δημιουργηθεί ένας ψηφιακός φάκελος είναι τα ακόλουθα:

- δημιουργείται ένα συμμετρικό κλειδί με την χρήση ενός αλγορίθμου συμμετρικής κρυπτογραφίας (π.χ το DES).
- η αρχική πληροφορία κρυπτογραφείται με το συμμετρικό κλειδί που έχει δημιουργηθεί
- το συμμετρικό κλειδί κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη
- τα δύο κρυπτογραφημένα κείμενα αποτελούν τον ψηφιακό φάκελο του παραλήπτη

Ο παραλήπτης λοιπόν προβαίνει στο άνοιγμα του ψηφιακού φακέλου, κάνοντας αποκρυπτογράφηση με το ιδιωτικό κλειδί το αρχικό κείμενο. Όταν τελειώσει η επικοινωνία μεταξύ των επικοινωνούντων μερών, το συμμετρικό κλειδί καταστρέφεται.

1.5.4 Μειονεκτήματα και Πλεονεκτήματα την Συμμετρικής και Ασύμμετρης Κρυπτογραφίας

Στα πλεονεκτήματα τα οποία έχει η συμμετρική κρυπτογραφία συμπεριλαμβάνονται και οι πολύ υψηλές ταχύτητες για την κρυπτογράφηση αλλά και την αποκρυπτογράφηση, οι οποίες μπορούν να ξεπεράσουν ακόμα και τα 100 Mbps καθώς και οι μικρές απαιτήσεις που έχει για την μνήμη και την υπολογιστική ισχύ. Ένα άλλο πλεονέκτημα είναι το αρκετά πιο μικρό μέγεθος του κρυπτοκειμένου σε σχέση με το αρχικό κείμενο. Εδώ θα πρέπει να σημειωθεί ότι μπορεί να εφαρμοστεί σε περιβάλλον όπως είναι ένα κινητό τηλέφωνο ή μια έξυπνη κάρτα.

Υπάρχει όμως ένα μεγάλο πρόβλημα στην συμμετρική κρυπτογραφία, που παρουσιάζεται στην συνεννόηση μεταξύ χρηστών, καθώς και στην ανταλλαγή κλειδιών χωρίς κάποιος τρίτος μη εξουσιοδοτημένος να μάθει για αυτά. Αυτό γίνεται επειδή η μετάδοση μέσα από το διαδίκτυο δεν είναι ασφαλής, αφού ο καθένας μπορεί να γνωρίζει για την συγκεκριμένη συναλλαγή και επιπλέον υπάρχουν τα κατάλληλα μέσα για την καταγραφή όλης της επικοινωνίας ανάμεσα στον αποστολέα και τον παραλήπτη, με αποτέλεσμα να είναι δυνατή η απόκτηση του κλειδιού. Ο κάθε τρίτος λοιπόν μη εξουσιοδοτημένος θα μπορεί να διαβάζει, να τροποποιεί και να πλαστογραφεί τα μηνύματα ή τα δεδομένα τα οποία ανταλλάσσουν δύο ανυποψίαστοι χρήστες. Για να πιστοποιηθεί η ταυτότητα κάποιου, μέσα από την συμμετρική κρυπτογράφηση απαιτείται η κοινή χρήση του ιδίου κλειδιού, που τις πιο πολλές φορές αποθηκεύονται σε υπολογιστές οι οποίοι κινδυνεύουν από εξωτερικές επιθέσεις κάποιων κακόβουλων. Σαν αποτέλεσμα αυτού είναι ότι ο αποστολέας έχει την δυνατότητα να αποκηρύξει ένα υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι υπάρχει αποκάλυψη του μυστικού κλειδιού.

Στο πρόβλημα της παρεμβολής τρίτου προσώπου στο να διαβάζει, να τροποποιεί και να πλαστογραφεί μηνύματα ή δεδομένα τα οποία ανταλλάσσουν δύο ανυποψίαστοι χρήστες, δίνει λύση η ασύμμετρη κρυπτογραφία, αφού σε ουδεμία περίπτωση δεν διακινούνται μέσω του διαδικτύου ευαίσθητα δεδομένα επειδή δεν χρειάζεται ανταλλαγή μυστικού κλειδιού το οποίο είναι γνωστό μόνο στον ιδιοκτήτη του, με αποτέλεσμα να καθίσταται δύσκολη η παραποίησης του.

Ένα άλλο πλεονέκτημα της κρυπτογραφίας δημόσιου κλειδιού είναι ότι δίνει την δυνατότητα να υλοποιηθεί μια από τις πιο σημαντικές διαδικασίες της κρυπτογραφικής λειτουργίας που είναι η ψηφιακή υπογραφή των δεδομένων. Στην ασύμμετρη κρυπτογράφηση δε μπορεί ο αποστολέας να αποκηρύξει ένα υπογεγραμμένο μήνυμα, αφού ο κάθε χρήστης έχει την αποκλειστική γνώση σε ότι αφορά το ιδιωτικό κλειδί, καθώς και την αποκλειστική ευθύνη για την φύλαξη του εν λόγω κλειδιού. Όμως η κρυπτογραφία δημόσιου κλειδιού έχει μεγάλες απαιτήσεις οι οποίες αφορούν την υπολογιστική ισχύ, η οποία φτάνει ακόμα και τις 100 φορές περισσότερο σε σχέση με την συμμετρική κρυπτογραφία.

1.5.5 Κβαντική κρυπτογραφία

Η κβαντική κρυπτογραφία έχει μεγάλες διαφορές σε σχέση με τα συστήματα ασφάλειας τα οποία χρησιμοποιούν τα σημερινά συστήματα, παρά το ότι υπάρχουν πολύπλοκες διαδικασίες πάνω στις οποίες βασίζονται, γιατί είναι δυνατόν να υπάρχει παραβίαση από οποιονδήποτε, που έχει χρόνο, χρήμα και μεγάλο μέγεθος υπολογιστικής ισχύος.

Η κρυπτογραφία αυτή χρησιμοποιεί τους νόμους που διέπουν την κβαντική φυσική και οι οποίοι θεωρούνται απαραβίαστοι. Η αρχική ιδέα αυτής της κρυπτογραφίας ξεκίνησε πριν από 25 χρόνια από τον Τσαρλς Μπένετ, της IBM και τον Ζιλ Μπρασάρ του πανεπιστημίου του Μόντρεαλ. Αυτή η ιδέα βασίστηκε στην γνωστή κβαντική αρχή της απροσδιοριστίας του Χάιζενμπεργκ, που είναι το ότι κάποιος παρατηρητής δεν μπορεί να μετρήσει την κβαντική πληροφορία, χωρίς να υπάρξει αλλοίωση.

Αυτή η νέα σχετικά τεχνολογία λειτουργεί στέλνοντας δέσμες φωτονίων, οι οποίες διαταράσσονται όταν κάποιος προσπαθήσει να υποκλέψει μήνυμα ή δεδομένα. Το εν λόγω σύστημα χρειάζεται κλειδιά τα οποία δημιουργούνται και διανέμονται μέσα από διαδικασίες και τεχνολογίες της κβαντικής κρυπτογράφησης. Κάθε φωτόνιο που μεταδίδεται μεταφέρει και ένα μυστικό κλειδί, που κωδικοποιεί τα μηνύματα ή τα δεδομένα που μεταφέρονται, όπως ακριβώς συμβαίνει και στα γνωστά συστήματα ηλεκτρονικών υπολογιστών. Το πλεονέκτημά της είναι ότι κανένας εκτός από τα επικοινωνούντα άτομα δεν μπορεί να υποκλέψει το κλειδί κρυπτογράφησης χωρίς να γίνει αντιληπτός.

Κεφάλαιο 2

Μηχανισμοί Εφαρμογής της Κρυπτογραφίας

2.1 Κρυπταλγόριθμος Στοιχειοσειράς (Stream Cipher)

Τα stream ciphers αποτελούν μία σημαντική κλάση τεχνικών συμμετρικής κρυπτογραφίας. Λειτουργούν σε μικρές μονάδες, συνήθως bits, του αρχικού κειμένου και ο μετασχηματισμός αυτών των bits εξαρτάται από το χρόνο. Από τα πιο σημαντικά χαρακτηριστικά των stream ciphers είναι η ταχύτητα και η απλότητα.

Ένας κρυπταλγόριθμος στοιχειοσειράς λειτουργεί ως εξής:

- Τα δεδομένα που πρόκειται να κρυπτογραφηθούν παρίστανται ως μία ακολουθία από δυαδικά ψηφία (bits). Κατόπιν, ελέγχεται μια γεννήτρια κλειδοροής (key stream generator) που δέχεται ως είσοδο ένα μυστικό κλειδί k και παράγει στην έξοδο μια ψευδοτυχαία ακολουθία από bits που ονομάζεται κλειδοροή (key stream). Η γεννήτρια κλειδοροής είναι ένας ειδικός τύπος γεννήτριας ψευδοτυχαίων αριθμών.
- Στη συνέχεια, το αρχικό κείμενο κρυπτογραφείται με modulo 2 (XOR), δηλαδή προσθέτοντας την κλειδοροή στο αρχικό κείμενο. Η ακολουθία από bits που παράγεται με αυτόν τον τρόπο αποτελεί το κρυπτοκείμενο (ciphertext).

Επομένως ένας συμβολισμός του κρυπταλγορίθμου στοιχειοσειράς θα μπορούσε να είναι :

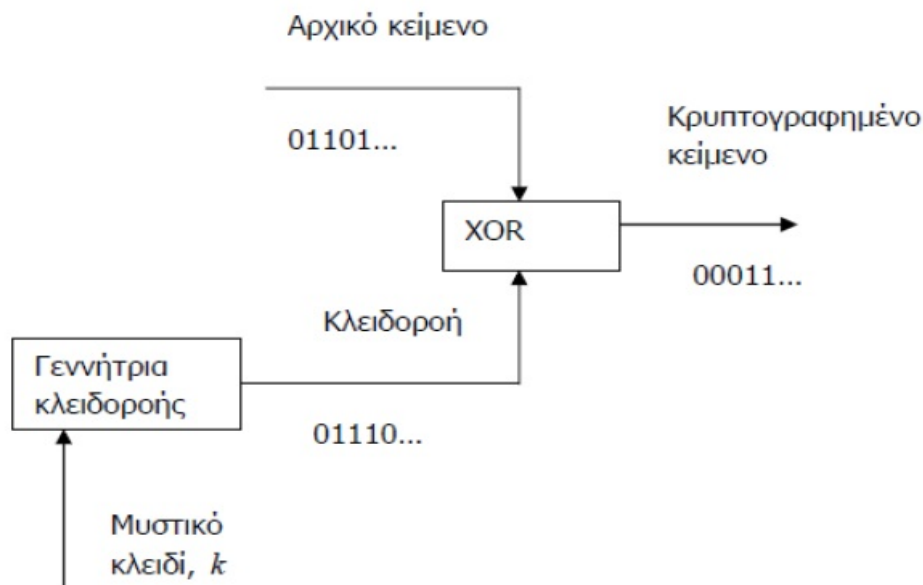
$$c_i = m_i \oplus s_i, \forall i \geq 0$$

όπου $m_0, m_1, \dots$ είναι τα bits του αρχικού κειμένου, $s_0, s_1, \dots$ είναι τα bits της κλειδοροής και $c_0, c_1, \dots$ είναι τα bits του κρυπτοκειμένου.

Αντίστοιχα, για την αποκρυπτογράφηση ισχύει:

$$m_i = c_i \oplus s_i, \forall i \geq 0$$

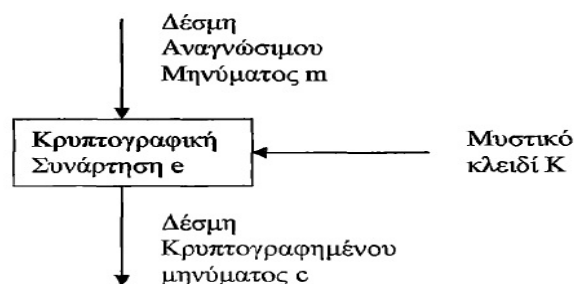
Δηλαδή η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο που γίνεται και η κρυπτογράφηση στοιχειοσειράς.



Σχήμα 2.1: Διαδικασία Κρυπτογράφησης Στοιχειοσειράς

2.2 Κρυπταλγόριθμος τμημάτων (Block Cipher)

Ο αλγόριθμος τμημάτων είναι ένας αλγόριθμος συμμετρικής κρυπτογράφησης, ο οποίος μετατρέπει μία ομάδα από το plaintext (αρχικό κείμενο), που έχει ένα συγκεκριμένο και καθορισμένο μήκος, σε μια ομάδα του ciphertext (κρυπτογραφημένου κειμένου) ίδιου μήκους. Η μετατροπή αυτή γίνεται χρησιμοποιώντας ένα μυστικό κλειδί, που χορηγείται από τον χρήστη. Το plaintext (αρχικό κείμενο) χωρίζεται σε τμήματα τα οποία έχουν σταθερό μήκος, που ακολούθως κρυπτογραφούνται σε τμήματα του ciphertext (κρυπτογραφημένου κειμένου), με την χρήση όμως του ίδιου κλειδιού. Η αποκρυπτογράφηση γίνεται εκτελώντας ακριβώς την αντίστροφη διαδικασία μετατροπής στο κρυπτογραφημένο κείμενο με την χρήση του ίδιου μυστικού κλειδιού. Το συγκεκριμένο και καθορισμένο μήκος, ονομάζεται block size (μέγεθος τμημάτων), που για τους πιο πολλούς αλγορίθμους κρυπτογράφησης είναι 64 bits. Κάθε κείμενο στο οποίο εκτελείται κρυπτογράφηση τμημάτων δίνει διαφορετικό ciphertext (κρυπτογραφημένου κειμένου).



Σχήμα 2.2: Κρυπταλγόριθμος τμημάτων

Οι κρυπταλγόριθμοι τμημάτων (block ciphers) χωρίζονται σε τρεις ομάδες: στους αλγόριθμους κρυπτογράφησης υποκατάστασης (substitution ciphers), τους αλγόριθμους κρυπτογράφησης μεταφοράς (transposition ciphers) και τους αλγόριθμους κρυπτογράφησης γινομένου (product ciphers).

2.2.1 Substitution Ciphers

Όπως υποδεικνύεται και από τον τίτλο, κάθε χαρακτήρας του αρχικού κειμένου υποκαθίσταται από κάποιους χαρακτήρες του κρυπτοκειμένου. Υπάρχουν τέσσερα είδη αλγορίθμων κρυπτογράφησης υποκατάστασης:

- Απλή Αντικατάσταση (Simple substitution)
- Πολυαλφαβητική Αντικατάσταση (Polyalphabetic substitution)
- Ομοφωνική Αντικατάσταση (Homophonic substitution)
- Πολυγραμμική Αντικατάσταση (Polygram substitution)

Συμβολισμοί

Έστω A_M και A_C τα αλφάβητα του αρχικού κειμένου και κρυπτοκειμένου, αντίστοιχα. Έστω επίσης $M = m_0, m_1, \dots, m_{n-1}$ ένα αρχικό κείμενο με n χαρακτήρες $\forall i, m_i \in A_M$ και $C = c_0, c_1, \dots, c_{n-1}$ το κρυπτοκείμενο $\forall i, c_i \in A_C$.

Απλή Αντικατάσταση

Μια μέθοδος απλής αντικατάστασης είναι η μέθοδος του Καίσαρα, σύμφωνα με αυτή την μέθοδο κάθε γράμμα του απλού αλφαβήτου αντικαθίσταται από το γράμμα το οποίο βρίσκεται τρεις θέσεις δεξιά του στο αλφάβητο.

Δηλαδή το "Α" αντικαθίσταται από το "D", το "B" αντικαθίσταται από το "E", το "C" αντικαθίσταται από το "F" κλπ.

Θεωρούμε πως το αλφάβητο σχηματίζει κύκλο. Μπορούμε να εκφράσουμε την κρυπτογράφηση και την αποκρυπτογράφηση της μεθόδου του Καίσαρα με τις ακόλουθες σχέσεις:

Κρυπτογράφηση:

$$C = (M + 3) \bmod 26$$

Αποκρυπτογράφηση:

$$M = (C - 3) \bmod 26$$

Αν το αποτέλεσμα της αφαίρεσης $(C - 3)$ είναι αρνητικός αριθμός, προσθέτουμε σε αυτόν το 26, και έτσι παίρνουμε τον επιθυμητό μη αρνητικό αριθμό.

Με την γενίκευση της μεθόδου του Καίσαρα, θα προκύψει η μέθοδος της απλής ή μονοαλφαβητικής αντικατάστασης, όταν στην θέση του 3 (κλειδιού), χρησιμοποιήσουμε έναν οποιονδήποτε αριθμό k μικρότερο του 26 και μεγαλύτερο του μηδενός. Ωστόσο και αυτή η μέθοδος δεν είναι ασφαλής, αφού υπάρχουν μόνο 25 δυνατά κλειδιά. Έτσι η εξέταση όλων αυτών οδηγεί με βεβαιότητα στην εξακρίβωση του κώδικα, αν και είναι δυνατό να υποτεθεί η τιμή του k από την εξέταση της συχνότητας εμφάνισης των γραμμάτων στον κώδικα.

Σε ένα κρυπτογράφημα με απλή αντικατάσταση κάθε χαρακτήρας του αρχικού κειμένου μεταμορφώνεται σε χαρακτήρα κρυπτοκειμένου μέσω της ίδιας συνάρτησης f .

Συγκεκριμένα $\forall i : 0 \leq i < n$

$$\begin{aligned} f : A_M &\rightarrow A_C \\ c_i &= f(m_i) \end{aligned}$$

Πιστεύεται ότι ο Ιούλιος Καίσαρας κρυπτογραφούσε μηνύματα μετατοπίζοντας κάθε γράμμα του αρχικού κειμένου τρεις θέσεις δεξιά στο αλφάβητο. Αυτό το κρυπτογράφημα στηρίζεται σε μετατοπισμένα αλφάβητα, δηλαδή $A_M = A_C$, και γενικά ορίζεται ως εξής $f(m_i) = m_i + k \pmod{|A_M|}$. Για το κρυπτογράφημα του Καίσαρα το μυστικό κλειδί k είναι ο αριθμός 3. Γενικά το κρυπτογράφημα μπορεί εύκολα να "σπάσει" το πολύ σε $|A_M|$ δοκιμές.

Πολυαλφαβητική Αντικατάσταση

Σε αυτή επιτρέπεται το κλειδί να έχει περισσότερες της μιας τιμές, δηλαδή κρυπτογραφώντας το πρώτο γράμμα του μηνύματος με την πρώτη τιμή του κλειδιού, ακολούθως το δεύτερο γράμμα του μηνύματος με την δεύτερη τιμή του κλειδιού κτλ, ώστε έτσι να επιτυγχάνεται κάποια βελτίωση της ασφάλειας της τεχνικής της αντικατάστασης, συνδυάζονται πολλές μονοαλφαβητικές αντικαταστάσεις. Έτσι, στην γενική περίπτωση με κλειδί μήκους j , το πρώτο γράμμα του απλού κειμένου κωδικοποιείται σύμφωνα με την πρώτη μονοαλφαβητική αντικατάσταση, το δεύτερο γράμμα σύμφωνα με την δεύτερη μονοαλφαβητική αντικατάσταση κτλ, μέχρι το j -οστό γράμμα του απλού κειμένου. Το $(j+1)$ -οστό γράμμα του απλού κειμένου, χρησιμοποιεί και πάλι την πρώτη μονοαλφαβητική αντικατάσταση, το $(j+2)$ -οστό γράμμα του απλού κειμένου την δεύτερη μονοαλφαβητική αντικατάσταση κτλ.

Σε μία πολυαλφαβητική αντικατάσταση λοιπόν οι χαρακτήρες του αρχικού κειμένου μεταμορφώνονται σε χαρακτήρες κρυπτοκειμένου χρησιμοποιώντας ένα κλειδί j χαρακτήρων $K = k_0, k_1, \dots, k_{j-1}$ το οποίο ορίζει j διακριτές συναρτήσεις $f_{k_0}, \dots, f_{k_{j-1}}$.

Συγκεκριμένα $\forall i : 0 < i \leq n$

$$f_{k_i} : A_M \rightarrow A_C \quad \forall l : 0 \leq l < j$$

$$c_i = f_{k_{i \bmod j}}(m_i)$$

Το κρυπτογράφημα του Vigenère δημοσιεύθηκε αρχικά το 1586.[3] Ας υποθέσουμε πάλι ότι $A_M = A_C$. Τότε το κρυπτογράφημα του Vigenère ορίζεται ως εξής

$$c_i = f_{k_{i \bmod j}}(m_i) = m_i + k_{i \bmod j} \pmod{|A_M|}$$

Ομοφωνική αντικατάσταση

Είναι μια βελτιωμένη εκδοχή της μονοαλφαβητικής αντικατάστασης, στην οποία χρησιμοποιούνται περισσότερες από έναν κώδικα για κάθε γράμμα του αλφαβήτου. Η επιλογή του κώδικα, ο οποίος θα αντικαταστήσει ένα συγκεκριμένο γράμμα του μηνύματος, γίνεται είτε τυχαία είτε με την σειρά από το σύνολο των κωδίκων που χρησιμοποιούνται γι' αυτό το γράμμα. Ωστόσο αν και οι διαφορετικές σχετικές συχνότητες των γραμμάτων μπορεί να συγκαλυφθούν με την ομοφωνική αντικατάσταση, οι συχνότητες διγραμμάτων και τριγραμμάτων διατηρούνται ως ένα βαθμό. Για να αντιμετωπιστεί αυτό το πρόβλημα, μπορεί να χρησιμοποιηθεί η κρυπτογράφηση πολλαπλών γραμμάτων ή πολυαλφαβητική αντικατάσταση. Σύμφωνα με την κρυπτογράφηση πολλαπλών γραμμάτων (διγραμμάτων ή τριγραμμάτων), αντιμετωπίζονται σαν μονάδες και αντικαθίστανται από ίσου μήκους κώδικες, ώστε να προκύψει το κρυπτογραφημένο κείμενο.

Πολυγραμμική αντικατάσταση

Σε αυτό το είδος αντικατάστασης γίνεται αντικατάσταση σε ακολουθίες χαρακτήρων π.χ. το "ABA" αντικαθίσταται από το "QWE" κ.ο.κ.

Τεχνικές μετάθεσης

Εδώ θα αναφερθούν τεχνικές μετάθεσης, όπου οι χαρακτήρες παραμένουν ως έχουν, και το μόνο που αλλάζει είναι η σειρά τους.

Σε έναν απλό κωδικοποιητή μετάθεσης με στήλες, το απλό κείμενο γράφεται κάθετα σε στήλες και το κρυπτογραφημένο κείμενο διαβάζεται οριζόντια η μια γραμμή μετά την άλλη. Ο αριθμός των γραμμών είναι το κλειδί που συμφωνούν εκ των προτέρων αποστολέας και παραλήπτης. Η αποκρυπτογράφηση γίνεται χωρίζοντας το κωδικοποιημένο κείμενο σε τμήματα που αντιστοιχούν στις γραμμές, θέτοντας το ένα τμήμα κάτω από το άλλο και διαβάζοντας κατά στήλη, την μια μετά την άλλη.

Απλή και πολλαπλή μετάθεση

Η προηγούμενη μέθοδος μπορεί να γίνει πιο σύνθετη με τον ακόλουθο τρόπο:

Αφού γραφτεί το καθαρό κείμενο κατά στήλες, όπως προηγουμένως, αναδιατάσσουμε αυτές με τρόπο ο οποίος περιγράφεται από το κλειδί.

Στην συνέχεια σχηματίζουμε τον κώδικα.

Η απλή κωδικοποίηση μετάθεσης μπορεί εύκολα να παραβιαστεί, από την συχνότητα εμφάνισης των γραμμμάτων, ο οποίος διατηρείται, μπορεί να αναγνωριστεί αν η μέθοδος κρυπτογράφησης βασίζεται στην τεχνική της μετάθεσης. Σε αυτήν την περίπτωση ο κρυπταναλυτής χωρίζει το κρυπτογραφημένο κείμενο σε γραμμές, δημιουργεί εξ αυτών έναν πίνακα και επιχειρεί αναδιάταξη των στηλών, λαμβάνοντας υπόψη την συχνότητα εμφάνισης διγραμμάτων και τριγραμμάτων. Αυτό το δοκιμάζει για διαφορετικούς αριθμούς γραμμών, έως ότου μπορέσει να εξαγάγει ένα κατανοητό μήνυμα. Μπορούμε βέβαια να δυσκολέψουμε την προσπάθεια του κρυπταναλυτή, αν μετατεθούν οι στήλες περισσότερες φορές. Τότε μιλάμε για πολλαπλή μετάθεση και σε αυτή την περίπτωση ο κρυπταναλυτής μπορεί σχετικά εύκολα να συναγάγει ότι πρόκειται για τη ν τεχνική της μετάθεσης όμως πιο δύσκολα να δημιουργήσει τον πίνακα που θα του επιτρέψει να αποκρυπτογραφήσει το κείμενο.

2.2.2 Transposition Systems

Οι αλγόριθμοι κρυπτογράφησης μεταφοράς είναι στην ουσία μεταθέσεις των χαρακτήρων του αρχικού κειμένου. Επομένως $A_M = A_C$. Ένα κρυπτογράφημα μεταφοράς ορίζεται ως εξής $\forall i : 0 \leq i < n$

$$\begin{aligned} f : A_M &\rightarrow A_M \\ \eta : 0, \dots, (n-1) &\rightarrow 0, \dots, (n-1), \text{ μία μετάθεση} \\ c_i &= f(m_i) = m_{\eta(i)} \end{aligned}$$

Πολλοί αλγόριθμοι κρυπτογράφησης μεταφοράς μεταθέτουν χαρακτήρες με σταθερή περίοδο j . Σ' αυτή την περίπτωση

$$\begin{aligned} f : A_M &\rightarrow A_M \\ \eta : 0, \dots, (j-1) &\rightarrow 0, \dots, (j-1), \text{ μία μετάθεση} \\ c_i &= f(m_i) = m_{(i \text{ div } j) + \eta(i \text{ mod } j)} \end{aligned}$$

Σε έναν κωδικοποιητή μετάθεσης, οι χαρακτήρες παραμένουν ως έχουν και το μόνο που αλλάζει είναι η σειρά τους. Σε ένα απλό κωδικοποιητή μετάθεσης με στήλες, το απλό κείμενο γράφεται κάθετα σε στήλες και το κρυπτογραφημένο κείμενο διαβάζεται οριζόντια, η μία γραμμή μετά την άλλη. Ο αριθμός των γραμμών είναι το κλειδί που συμφωνείται πριν από αποστολέα και παραλήπτη.

Η αποκρυπτογράφηση γίνεται χωρίζοντας το κωδικοποιημένο κείμενο σε τμήματα που αντιστοιχούν στις γραμμές, βάζοντας το ένα τμήμα κάτω από το άλλο και διαβάζοντας κατά στήλη, την μια μετά την άλλη.

Διακρίνονται δύο κατηγορίες μετάθεσης, η απλή και η πολλαπλή. Η απλή μετάθεση μπορεί εύκολα να παραβιαστεί λόγω της συχνότητας εμφάνισης των γραμμάτων. Στην πολλαπλή μετάθεση, μετατίθενται οι στήλες περισσότερες φορές, οπότε γίνεται δυσκολότερο το έργο του κρυπταναλυτή. Όμως και αυτή η μέθοδος μπορεί εύκολα να αποκαλυφθεί.

2.2.3 Product Systems

Μια προσπάθεια για να δημιουργηθούν ισχυροί αλγόριθμοι, είναι να γίνει ένας συνδυασμός των αλγορίθμων κρυπτογράφησης substitution ciphers με τους αλγορίθμους κρυπτογράφησης transposition ciphers. Οι αλγόριθμοι που προκύπτουν λέγονται κρυπταλγόριθμοι γινομένου. Τέτοιοι αλγόριθμοι είναι οι περισσότεροι block ciphers που χρησιμοποιούνται σήμερα. Ένας αλγόριθμος γινομένου λέγεται επαναληπτικός (iterated) όταν το κρυπτογραφημένο κείμενο μπορεί να υπολογιστεί εφαρμόζοντας μια κυκλική συνάρτηση επαναληπτικά, πολλές φορές στο αρχικό κείμενο. Στον κάθε γύρο ένα κυκλικό κλειδί συνδυάζεται με την εισαγωγή κειμένου.

Ορισμός. Σε έναν r -γύρων επαναληπτικό κρυπταλγόριθμο τμημάτων, το κρυπτοκείμενο υπολογίζεται εφαρμόζοντας επαναληπτικά μία κυκλική συνάρτηση g στο αρχικό κείμενο, τέτοια ώστε

$$C_i = g(C_{i-1}, K_i), i = 1, \dots, r \quad (2.1)$$

όπου C_0 είναι το αρχικό κείμενο, K_i ένα κυκλικό κλειδί και C_r είναι το κρυπτοκείμενο. Η αποκρυπτογράφηση γίνεται αντιστρέφοντας την (2.1), οπότε για ένα σταθερό κλειδί K_i η g πρέπει να είναι αντιστρέψιμη.

2.2.4 Δομές Feistel

Οι δομές Feistel είναι δομές που χρησιμοποιούνται από block ciphers. Η ιδέα του Feistel ήταν απλή και είχε βάση στην απόδειξη της ασφάλειας ενός αλγορίθμου μέσα από κάποιες μη αναστρέψιμες συναρτήσεις. Ακόμα έκανε την προσπάθεια ώστε τα μοντέλα των κρυπταλγορίθμων τμημάτων να είναι όσο γίνεται πιο απλά. Όταν προστίθενται μέρη που είναι ασφαλή, το καθένα όμως ανεξάρτητα από το άλλο, δεν σημαίνει ότι και το σύνολο θα είναι ασφαλές. Όταν πολλές φορές επιλέγονται τμήματα τα οποία είναι αντιστρέψιμα, τότε εισάγεται μια δομή στον αλγόριθμο που πιθανόν να είναι προς όφελος αυτού που εκτελεί την κρυπτανάλυση και όχι προς όφελος της ασφάλειας ή ακόμα και της ταχύτητας αποκρυπτογράφησης.

Ο Feistel λοιπόν εισήγαγε κάποιες δικές του δομές, οι οποίες σήμερα χρησιμοποιούνται από πάρα πολλούς σύγχρονους αλγορίθμους. Αρχικά μέσω μιας συνάρτησης g παράγονται τα κλειδιά του κάθε γύρου K_i από το αρχικό κλειδί K . Σε κάθε γύρο του αλγορίθμου τμημάτων, η είσοδός του χωρίζεται στη μέση, έχουμε έτσι το αριστερό και το δεξί τμήμα. Τα δύο αυτά τμήματα δεδομένων ακολουθούν n επαναληπτικά βήματα επεξεργασίας, και στη πορεία συνδυάζονται για να παράγουν το τμήμα του κρυπτογραφημένου κειμένου. Αν λοιπόν είμαστε στον i γύρο, έχουμε τα L_{i-1} και R_{i-1} , αριστερό και δεξί τμήμα αντίστοιχα, τα οποία έχουν n bits το κάθε ένα και παράγονται από τον προηγούμενο γύρο, καθώς επίσης και ένα υποκλειδί K_i (subkey) που παράγεται από το αρχικό κλειδί K . Γενικά, τα υποκλειδιά K_i είναι διαφορετικά από το K και διαφορετικά μεταξύ τους, ενώ παράγονται από το κλειδί και από έναν αλγόριθμο παραγωγής υποκλειδιών.

Τα επαναληπτικά βήματα ακολουθούν την ίδια δομή: Στα δεδομένα που βρίσκονται στην αριστερή πλευρά πραγματοποιείται μία αντικατάσταση. Η αντικατάσταση επιτυγχάνεται με την εφαρμογή

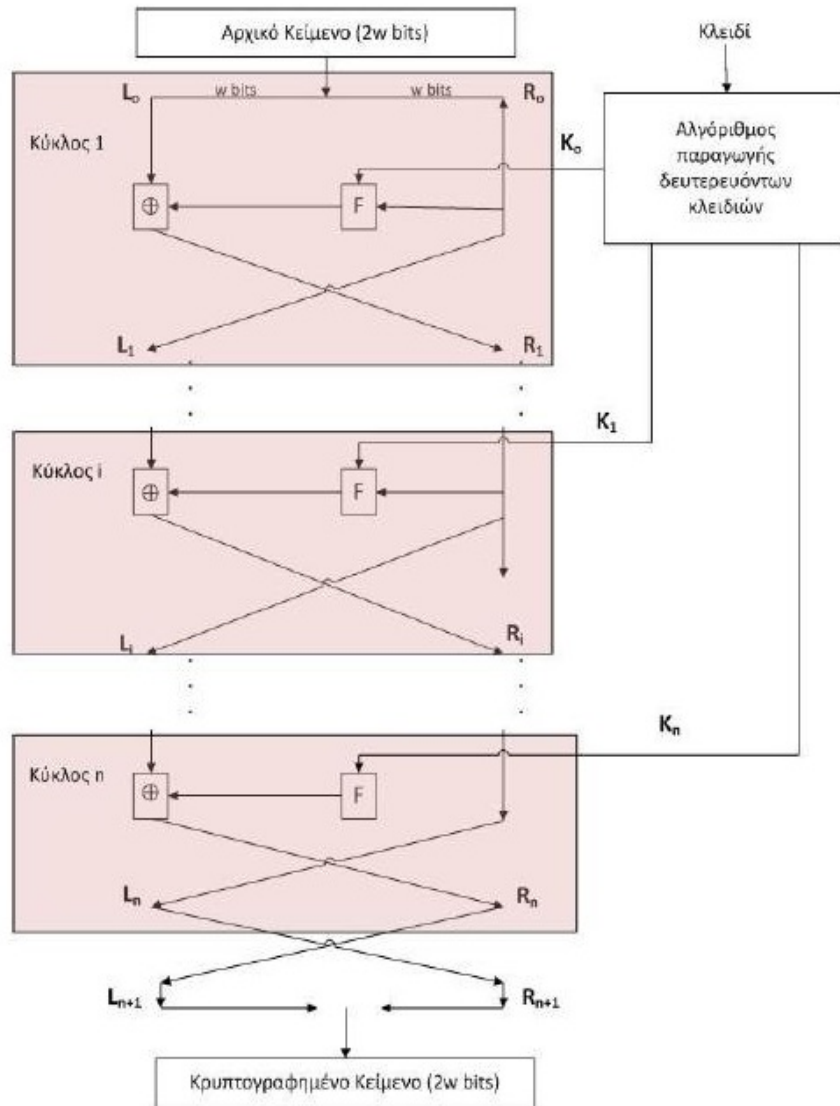
μιας συνάρτησης F (round function) στα δεδομένα της δεξιάς πλευράς και έπειτα συνδυάζοντας την έξοδο της συνάρτησης με τα δεδομένα της αριστερής πλευράς με τον τελεστή Exclusive-OR - XOR. Η συνάρτηση F έχει την ίδια γενική δομή για κάθε κύκλο, αλλά παραμετροποιείται από το υποκλειδί K_i του εκάστοτε κύκλου. Επίσης η συνάρτηση γύρου δε χρειάζεται να είναι αντιστρέψιμη και έχει ως είσοδο το κλειδί του γύρου και το R_{i-1} και ως έξοδο n bits. Μετά από αυτή την αντικατάσταση, εκτελείται μία αντιμετάθεση των πλευρών των δεδομένων.

Τότε ορίζουμε:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F_i(K_i, R_i)$$

Αν γνωρίζουμε το κλειδί και αντιστρέψουμε τα βήματα της δομής αυτής, θα προκύψει το αρχικό κείμενο από το κρυπτογράφημα. Άρα, καταλαβαίνουμε ότι η ασφάλεια του αλγόριθμου στηρίζεται στο να βρεθούν ασφαλείς οι συναρτήσεις γύρου F_i . Αν είναι αυτές ασφαλείς τότε και ο αλγόριθμος είναι εξίσου ασφαλής.



Σχήμα 2.3: Κλασικό δίκτυο Feistel

Η ακριβής υλοποίηση ενός δικτύου Feistel εξαρτάται από την επιλογή των ακόλουθων παραμέτρων και χαρακτηριστικών [4]:

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

Επιπλέον αναφέρονται δύο ακόμη παράμετροι οι οποίοι λαμβάνονται υπόψη κατά το σχεδιασμό μιας δομής δικτύου Feistel:

- **Λογισμικό ταχείας κρυπτογράφησης και αποκρυπτογράφησης (fast software encryption and decryption):** Σε αρκετές περιπτώσεις η κρυπτογράφηση ενσωματώνεται στις εφαρμογές ή σε βοηθητικές συναρτήσεις με τέτοιο τρόπο ώστε αποκλείεται η δυνατότητα υλοποίησης σε υλικό, κατά συνέπεια η ταχύτητα εκτέλεσης του αλγορίθμου θεωρείται σημαντικός παράγοντας.
- **Ευκολία ανάλυσης (ease of analysis):** Αν και είναι επιθυμητή η επίτευξη υψηλού βαθμού δυσκολίας κατά τη διαδικασία της κρυπτανάλυσης ενός αλγορίθμου, υπάρχει σημαντικό όφελος εάν επιτευχθεί εύκολη ανάλυση του αλγορίθμου. Εάν ο αλγόριθμος μπορεί να εξηγηθεί συνοπτικά και με σαφήνεια, τότε είναι πιο εύκολο να εξεταστεί για κρυπταναλυτικά σημεία ευπάθειας και επομένως να αναπτυχθεί υψηλότερο επίπεδο ασφάλειας.

Η κατά Feistel αποκρυπτογράφηση, είναι ίδια με την διαδικασία της κρυπτογράφησης, ακολουθώντας όμως τον κανόνα ότι οι είσοδοι χρησιμοποιούνται και στο κρυπτοκείμενο αλλά και στα υποκλειδιά, με αντίστροφη όμως σειρά. Το πιο σημαντικό της διαδικασίας είναι ότι δεν χρειάζεται να εφαρμοστούν δύο διαφορετικοί αλγόριθμοι, ένας για την κρυπτογράφηση και ένας άλλος για την αποκρυπτογράφηση.

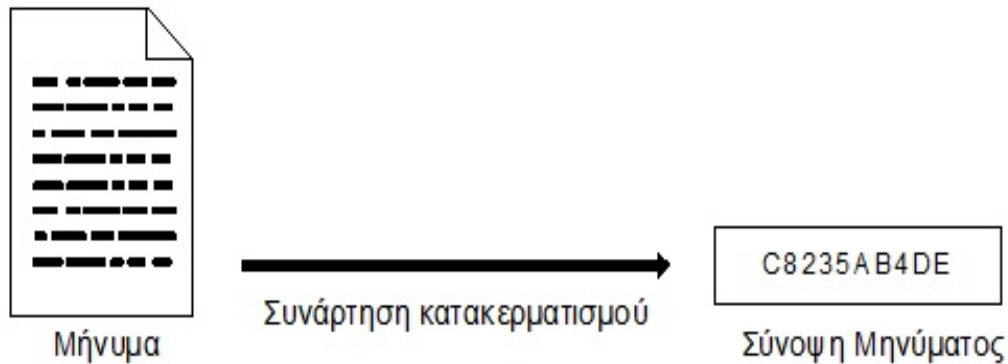
2.3 Συναρτήσεις Κατακερματισμού (Hash Functions)

Οι συναρτήσεις κατακερματισμού είναι πολύ βασικές στην κρυπτογραφία. Μία hash function είναι μια συνάρτηση η οποία παίρνει δεδομένα εισόδου μεταβλητού μήκους και στην συνέχεια παράγει δεδομένα εξόδου τα οποία είναι σταθερού μήκους. Αυτό σημαίνει ότι όταν οι τιμές κατακερματισμού δυο μηνυμάτων ταιριάζουν, η πιθανότητα να είναι ίδια τα μηνύματα γίνεται πολύ μεγάλη. Χρήσιμες κρυπτογραφικά συναρτήσεις κατακερματισμού είναι οι μη αντιστρέψιμες (one way), το οποίο σημαίνει ότι μπορούν να υπολογιστούν εύκολα, πρακτικά όμως είναι αδύνατον να αντιστραφούν. Μια καλή συνάρτηση κατακερματισμού θα πρέπει να αντέχει στις συγκρούσεις, δηλαδή να είναι δύσκολο να βρεθούν δυο διαφορετικές τιμές, ώστε η τιμή κατακερματισμού να είναι η ίδια.

Ο όρος συναρτήσεις κατακερματισμού υποδηλώνει έναν μετασχηματισμό που λαμβάνει ως είσοδο ένα μήνυμα m ανεξαρτήτου μήκους και επιστρέφει στην έξοδο μια ακολουθία χαρακτήρων h περιορισμένου μήκους που ονομάζεται hash value, δηλαδή ισχύει $h = H(m)$. Οι συναρτήσεις κατακερματισμού είναι συναρτήσεις της μορφής $H(x) = y$, και διαθέτουν τις παρακάτω ιδιότητες:

- η συνάρτηση H μπορεί να εφαρμοστεί σε ένα τμήμα δεδομένων οποιουδήποτε μεγέθους
- η συνάρτηση H παράγει μία έξοδο σταθερού μήκους ενώ η είσοδος μπορεί να είναι οποιουδήποτε μήκους
- η συνάρτηση $H(x)$ είναι σχετικά εύκολο να υπολογιστεί για κάθε δοσμένο x , κάνοντας πρακτικές τις υλοποιήσεις, υλικού και λογισμικού
- για κάθε δοσμένο κώδικα h , είναι υπολογιστικά ανέφικτο να βρεθεί x , τέτοιο ώστε $H(x) = h$
- για κάθε δοσμένο x , είναι υπολογιστικά ανέφικτο να βρεθεί $y \neq x$, με $H(y) = H(x)$
- είναι υπολογιστικά ανέφικτο να βρεθεί ένα ζεύγος (y, x) τέτοιο ώστε $H(y) = H(x)$
- η συνάρτηση $H(x)$ είναι μη αντιστρέψιμη και αμφιμονοσήμαντη

Λέγοντας ότι μια συνάρτηση H είναι μη αντιστρέψιμη εννοούμε πως δίνοντας μια τιμή κατακερματισμού h είναι υπολογιστικά αδύνατο να βρεθεί ένα μήνυμα τέτοιο ώστε $H(x) = h$, δηλαδή το αρχικό μήνυμα δεν μπορεί να ανακτηθεί από τη σύνοψή του. Όταν επιπλέον η συνάρτηση είναι αμφιμονοσήμαντη, τότε είναι πολύ δύσκολο να βρεθούν δύο διαφορετικά μηνύματα με την ίδια σύνοψη.

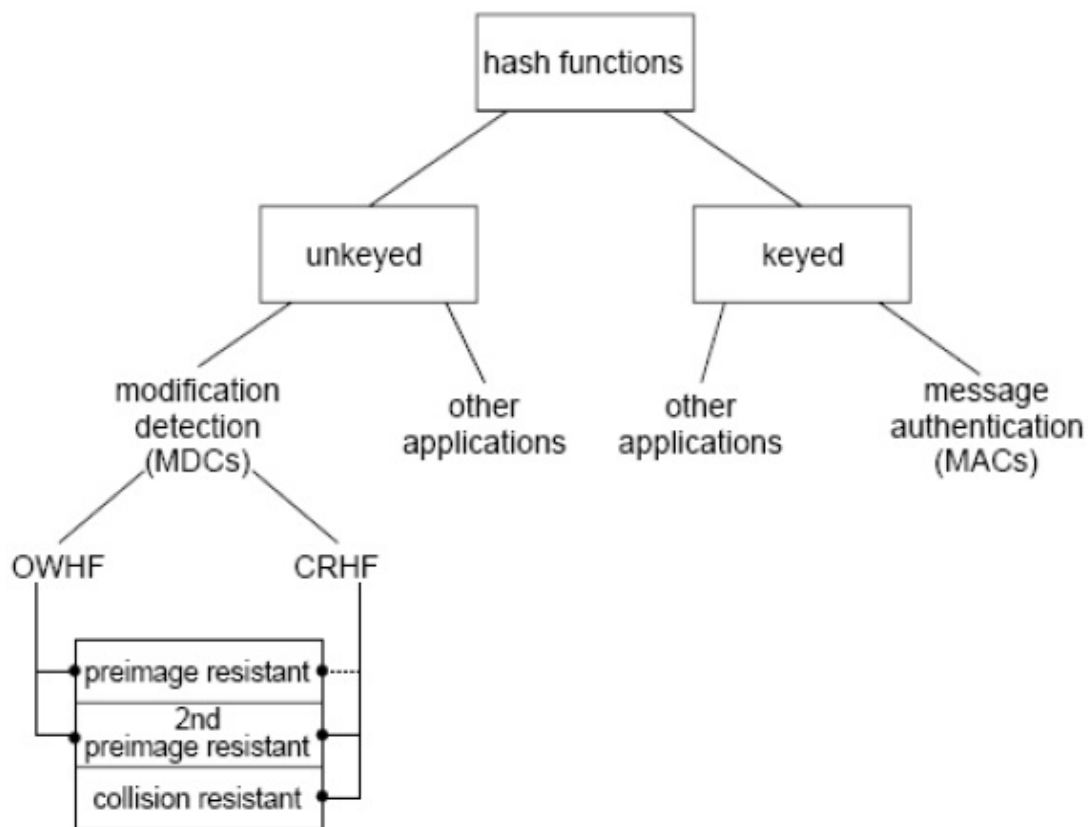


Σχήμα 2.4: Κρυπτογράφηση μηνύματος με hash function

Μία hash value παρουσιάζει συνοπτικά το μεγαλύτερο μήνυμα ή έγγραφο, και για τον λόγο αυτό λέγεται σύνοψη μηνύματος (message digest). Μπορούμε λοιπόν να την φανταστούμε σαν ένα ψηφιακό αποτύπωμα του εγγράφου. Οι πιο γνωστές συναρτήσεις κατακερματισμού είναι οι MD2, MD5, SHA.

Υπάρχουν δύο κατηγορίες συναρτήσεων κατακερματισμού:

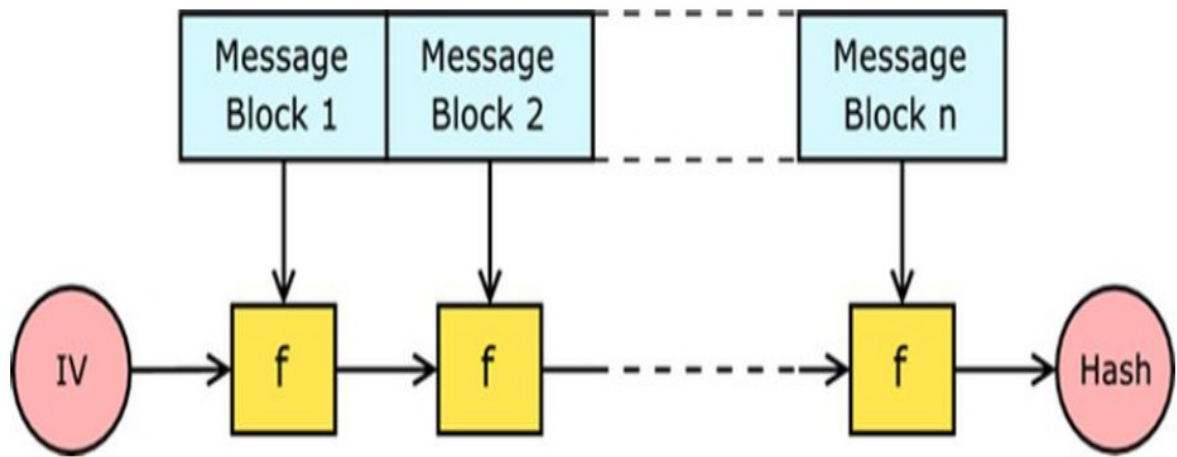
- κώδικες ανίχνευσης τροποποίησης (MDCs – modification detection codes): είναι γνωστοί σαν κώδικες ανίχνευσης χειρισμού, παρά σαν κώδικες ακεραιότητας μηνύματος (MICs). Ο σκοπός ενός τέτοιου κώδικα είναι να δίνει μια αντιπροσωπευτική εικόνα ή ένα κομμάτι ενός μηνύματος, ικανοποιώντας έτσι ορισμένες ιδιότητες. Οι MDCs είναι μια υποκατηγορία των unkeyded συναρτήσεων κατακερματισμού.
- κώδικες αυθεντικοποίησης μηνυμάτων (MACs – message authentication codes): είναι κώδικες οι οποίοι συνοδεύουν το μήνυμα και πιστοποιούν την ταυτότητα του αποστολέα αφενός και την ακεραιότητα του μηνύματος αφετέρου. Ο σκοπός ενός τέτοιου κώδικα είναι να προσφέρει διευκόλυνση, χωρίς να χρειάζονται επιπρόσθετοι μηχανισμοί διαβεβαίωσης, παίρνοντας υπόψη την πηγή του μηνύματος καθώς και την ακεραιότητά του. Οι MAC έχουν δύο διακριτές λειτουργικές παραμέτρους που είναι μια είσοδος μηνύματος και ένα μυστικό κλειδί. Σε αντίθεση με τις ψηφιακές υπογραφές οι κώδικες αυθεντικοποίησης υπολογίζονται και επαληθεύονται με το ίδιο κλειδί, με τέτοιο τρόπο ώστε να υπάρχει δυνατότητα επαλήθευσης από τον παραλήπτη. Τέλος οι κώδικες αυθεντικοποίησης μηνυμάτων είναι μια υποκατηγορία των keyed συναρτήσεων κατακερματισμού



Σχήμα 2.5: Ταξινόμηση των κρυπτογραφικών συναρτήσεων κατακερματισμού

Επειδή οι συναρτήσεις κατακερματισμού είναι ταχύτερες από τους αλγορίθμους κρυπτογράφησης καθώς επίσης και από τις ψηφιακές υπογραφές, η συνηθέστερη διαδικασία είναι η υπογραφή μηνυμάτων να παράγεται με εκτέλεση διαδικασιών κρυπτογράφησης στο message digest, το οποίο είναι πιο μικρό και πιο εύκολο στην διαχείριση. Το message digest μπορεί ακόμη να δημοσιοποιηθεί χωρίς μάλιστα να υπάρξει αποκάλυψη του αρχικού κειμένου.

Οι Damgard και Merkle είναι αυτοί οι οποίοι επηρέασαν κυρίως τον σχεδιασμό συναρτήσεων κρυπτογράφησης κατακερματισμού, χρησιμοποιώντας την συμπίεση. Μία συνάρτηση συμπίεσης (compression function) παίρνει σαν είσοδο κάποιο μήνυμα το οποίο έχει σταθερό μέγεθος και παράγει στην έξοδο μήνυμα το οποίο είναι σταθερού μεγέθους αλλά πιο μικρό. Σύμφωνα με τους Damgard και Merkle και έχοντας δώσει μια συνάρτηση συμπίεσης, τότε μια συνάρτηση κατακερματισμού μπορεί να οριστεί, αν εφαρμοστεί πολλές φορές η συνάρτηση της συμπίεσης, έως ότου γίνει επεξεργασία όλου του κειμένου. Με βάση αυτήν την διαδικασία, ένα μήνυμα αυθαίρετου μεγέθους, σπάει σε ομάδες, το μέγεθος των οποίων καθορίζεται από την συνάρτηση συμπίεσης που χρησιμοποιείται και συμπληρώνεται, ώστε το μέγεθος του μηνύματος να γίνει πολλαπλάσιο του μήκους της ομάδας. Κατόπιν οι ομάδες επεξεργάζονται σειριακά ή μια μετά την άλλη και παράγουν στο τέλος στην έξοδο την τιμή κατακερματισμού για το συγκεκριμένο μήνυμα.



Σχήμα 2.6: Η επαναληπτική δομή Damgard-Merkle για συναρτήσεις κατακερματισμού. (f είναι μια συνάρτηση συμπίεσης)

Βασικές Ιδιότητες των Συναρτήσεων Κατακερματισμού

Τρεις βασικές ιδιότητες για μια unkeyed συνάρτηση κατακερματισμού h , με εισόδους x, x^A και εξόδους y, y^A είναι:

- preimage resistance: είναι υπολογιστικά αδύνατο να βρεθεί οποιαδήποτε είσοδος που κατακερματίζεται σε αυτή την έξοδο. Δηλαδή να βρεθεί οποιαδήποτε preimage x^A τέτοια ώστε $h(x^A) = y$, δεδομένου κάποιας y , για την οποία η αντίστοιχη είσοδος δεν είναι γνωστή.
- 2nd preimage resistance: είναι υπολογιστικά αδύνατο να βρεθεί οποιαδήποτε δεύτερη είσοδος, η οποία έχει την ίδια έξοδο με κάποια συγκεκριμένη είσοδο. Δηλαδή δεδομένου του x , να βρεθεί μια 2nd preimage x^A τέτοια ώστε $h(x) = h(x^A)$
- collision resistance: είναι υπολογιστικά αδύνατο να βρεθούν δύο ξεχωριστές είσοδοι x, x^A , οι οποίες κατακερματίζονται στην ίδια έξοδο, δηλαδή τέτοια ώστε $h(x) = h(x^A)$

2.4 Κώδικας Αυθεντικοποίησης Μηνυμάτων Message Authentication Code - (MAC)

Στην τεχνική αυτή είναι απαραίτητη η χρήση ενός μυστικού κλειδιού, προκειμένου να παραχθεί ένα μικρό τμήμα δεδομένων, το οποίο στην συνέχεια θα προσαρτηθεί στο μήνυμα. Για παράδειγμα έστω ότι υπάρχουν δύο οντότητες Α και Β, οι οποίοι θέλουν να επικοινωνήσουν, να είναι γνώστες ενός μυστικού κλειδιού K_{AB} . Όταν ο Α θελήσει να στείλει ένα μήνυμα M στον Β, υπολογίζει το MAC σαν συνάρτηση του μηνύματος και του μυστικού κλειδιού: $MAC_M = f(K_{AB}, M)$. Το MAC προσαρτάται στο μήνυμα και αποστέλλεται στον Β, που ακολουθώντας τον ίδιο υπολογισμό στο μήνυμα που έλαβε, χρησιμοποιώντας το ίδιο μυστικό κλειδί, παράγει το νέο MAC.

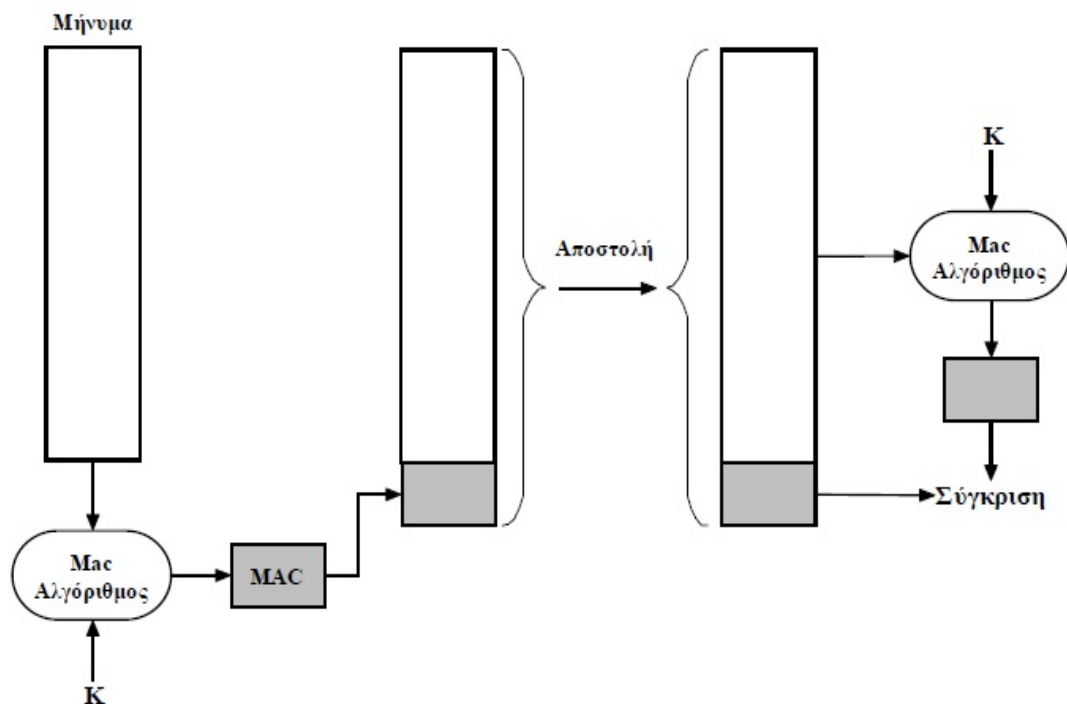
Υποθέτοντας τώρα ότι το μυστικό κλειδί είναι γνωστό μόνο στον αποστολέα και τον παραλήπτη και ότι τα MAC είναι ίσα, τότε συμπεραίνουμε τα παρακάτω:

- ο παραλήπτης επιβεβαιώνει ότι το μήνυμα δεν υπέστη κάποια αλλοίωση από έναν επιτιθέμενο, τότε κατά τον υπολογισμό του MAC από τον παραλήπτη θα προκύψει διαφορά με το αντίστοιχο MAC του αποστολέα. Επειδή ο επιτιθέμενος δεν γνωρίζει το μυστικό κλειδί, δεν μπορεί να αλλάξει το MAC, ώστε να ανταποκρίνεται στις αλλαγές του μηνύματος.

- ο παραλήπτης μπορεί να επιβεβαιώσει ότι το μήνυμα προέρχεται από τον συγκεκριμένο αποστολέα. Αυτή η διαβεβαίωση πηγάζει από το ότι κανείς, εκτός από τον αποστολέα και τον νόμιμα εξουσιοδοτημένο παραλήπτη, δεν γνωρίζει το μυστικό κλειδί, κατά συνέπεια κανένας άλλος δεν μπορεί να προετοιμάσει ένα μήνυμα με το κατάλληλο MAC.
- εάν το μήνυμα περιλαμβάνει αριθμό ακολουθίας, όπως αυτοί που χρησιμοποιούνται στα πρωτόκολλα X25, HDLC και TCP, τότε ο παραλήπτης είναι σε θέση να επιβεβαιώσει την ορθότητα της σωστής ακολουθίας, επειδή ο επιτιθέμενος δεν μπορεί να τροποποιήσει με επιτυχία έναν αριθμό ακολουθίας.

Στα σύγχρονα συστήματα, οι MAC παράγονται χρησιμοποιώντας αρκετούς αλγορίθμους. Από το US National Of Standards στο κείμενο με τίτλο DES Modes of Operation, προτείνεται η χρήση του DEA για την παραγωγή του MAC. Το DEA χρησιμοποιείται για την παραγωγή κρυπτογραφημένης έκδοσης του μηνύματος και τα τελευταία 16 ή 32 bits του κρυπτογραφημένου κειμένου χρησιμοποιούνται σαν MAC.

Η διαδικασία που περιγράφηκε προηγούμενα είναι αντίστοιχη με εκείνη της κρυπτογράφησης. Η βασική τους διαφορά είναι στο γεγονός ότι ένας αλγόριθμος αυθεντικοποίησης δεν πρέπει να είναι αντιστρέψιμος, ενώ αντίθετα η συνάρτηση κρυπτογράφησης θα πρέπει να μπορεί να αντιστραφεί στην πλευρά του παραλήπτη.



Σχήμα 2.7: Αυθεντικοποίηση μηνύματος με χρήση MAC

Κεφάλαιο 3

Αλγόριθμοι Μυστικού ή Συμμετρικού Κλειδιού

3.1 Γενικά

Η σύγχρονη κρυπτογραφία βασίζεται στις ίδιες βασικές ιδέες που χρησιμοποιούνται και στην παραδοσιακή κρυπτογραφία, με τη διαφορά ότι στη σύγχρονη κρυπτογραφία η έμφαση δίνεται σε διαφορετικό σημείο. Ο στόχος είναι ο αλγόριθμος να είναι αρκετά περίπλοκος και μπλεγμένος έτσι ώστε εάν ο κρυπταναλυτής αποκτήσει κομμάτι ενός κρυπτογραφημένου κειμένου, να μην είναι σε θέση να καταλάβει τίποτα από αυτό χωρίς να γνωρίζει το κλειδί.

Οι αλγόριθμοι συμμετρικού κλειδιού διακρίνονται σε δύο κατηγορίες: τους **αλγορίθμους τμημάτων** (block ciphers) και τους **αλγορίθμους στοιχειοσειράς** (stream ciphers). Στους αλγορίθμους τμημάτων, όταν ένα μήνυμα κρυπτογραφείται, ο αλγόριθμος δεν κρυπτογραφεί κάθε ένα bit (δυαδικά ψηφία) του μηνύματος ξεχωριστά αλλά ολόκληρες ομάδες από bits. Αντιθέτως, στους αλγορίθμους στοιχειοσειράς, ο αλγόριθμος εφαρμόζεται σε μια στοιχειοσειρά από bits.

3.2 Μέθοδοι Λειτουργίας των Κρυπταλγορίθμων Τμημάτων (Modes of operation)

Μία μέθοδος λειτουργίας είναι ένας προτεινόμενος τρόπος να χρησιμοποιηθεί ένας κρυπταλγόριθμος τμημάτων για να κρυπτογραφηθεί ένα αρχικό κείμενο και να παράγει το κρυπτοκείμενο. Μία τέτοια μέθοδος είναι απαραίτητη καθώς οι κρυπταλγόριθμοι τμημάτων προσφέρουν τρόπο να κρυπτογραφούμε ένα string n-bits και όχι αυθαίρετου μήκους. Ακόμα και όταν κρυπτογραφούμε string n-bits μία μέθοδος λειτουργίας θα αποτρέψει τη διαρροή πληροφορίας που προκύπτει από επαναλαμβανόμενα n-bit στο αρχικό κείμενο.

Τέσσερις μέθοδοι λειτουργίας ονόματι Electronic Codebook (ECB), Cipher Block Chaining (CBC), Output Feedback (OFB) και Cipher Feedback (CFB) έγιναν πρότυπες μέθοδοι στις Η.Π.Α. το 1980. Αυτές οι μέθοδοι περιγράφηκαν κυρίως για χρήση με το κρυπτοσύστημα DES αλλά αργότερα εφαρμόστηκαν και σε άλλους κρυπταλγόριθμους τμημάτων.

ECB: Electronic CodeBook

Στη μέθοδο αυτή, η κρυπτογράφηση ενός τμήματος κειμένου εξαρτάται αποκλειστικά από το κλειδί και από το τμήμα αυτό του κειμένου. Ο όρος "codebook" χρησιμοποιείται ακριβώς επειδή για δεδομένο κλειδί υπάρχει ένα μοναδικό κρυπτογράφημα για κάθε τμήμα αρχικού κειμένου των 64-

bit. Επομένως, κάποιος μπορεί να αναλογιστεί ένα μεγάλο μεγέθους ηλεκτρονικό βιβλίο στο οποίο υπάρχει μία εγγραφή για κάθε πιθανό πρότυπο αρχικού κειμένου των 64-bit, το οποίο καταγράφεται με το αντίστοιχο κρυπτογράφημα του. Με τη μέθοδο ECB, εάν ένα τμήμα αρχικού κειμένου των 64-bit εμφανίζεται περισσότερες από μία φορές στο μήνυμα, αυτό παράγει πάντοτε το ίδιο κρυπτογράφημα. Για το λόγο αυτό, σε μεγάλα μηνύματα ο τρόπος λειτουργίας ECB μπορεί να θεωρηθεί μη ασφαλής. Για παράδειγμα, εάν είναι γνωστό ότι το μήνυμα αρχίζει με κάποια προκαθορισμένα πεδία τότε ο κρυπταναλυτής μπορεί να διαθέτει έναν αριθμό από γνωστά ζεύγη αρχικού κειμένου – κρυπτογραφήματων για να τα αξιοποιήσει κρυπταναλυτικά. Εάν το μήνυμα έχει επαναλαμβανόμενα στοιχεία με περίοδο επανάληψης πολλαπλάσια των 64-bit τότε τα στοιχεία αυτά μπορούν να προσδιοριστούν από τον κρυπταναλυτή. Το γεγονός αυτό είτε μπορεί να συμβάλλει στην κρυπτανάλυση είτε μπορεί να παρέχει τη δυνατότητα ορθής αντικατάστασης ή αναδιάταξης των τμημάτων.

CBC: Cipher Block Chaining

Στη μέθοδο Αλυσιδωτής Κρυπτογράφησης Τμημάτων η είσοδος στον αλγόριθμο κρυπτογράφησης είναι το αποτέλεσμα της πύλης XOR του τρέχοντος τμήματος αρχικού κειμένου και του προηγούμενου τμήματος κρυπτογραφήματος. Το ίδιο κλειδί χρησιμοποιείται σε κάθε τμήμα. Στην πραγματικότητα υπάρχει λογική διασύνδεση κατά την επεξεργασία της ακολουθίας των επιμέρους τμημάτων του αρχικού κειμένου. Η είσοδος της συνάρτησης κρυπτογράφησης για κάθε τμήμα κειμένου δε σχετίζεται άμεσα με το τμήμα του κειμένου αυτού, επομένως δεν εκτίθενται με τον ίδιο τρόπο επαναλαμβανόμενα τμήματα των 64-bit. Για την αποκρυπτογράφηση, κάθε τμήμα επεξεργάζεται από τον αλγόριθμο αποκρυπτογράφησης και στο αποτέλεσμα που προκύπτει εφαρμόζεται η συνάρτηση XOR με το προηγούμενο τμήμα κρυπτογραφήματος, ώστε τελικά παράγεται το αντίστοιχο τμήμα του αρχικού κειμένου. Η μέθοδος CBC χρησιμοποιείται ευρύτατα σε πληθώρα εφαρμογών ασφάλειας.

OFB: Output Feedback

Η μέθοδος λειτουργίας OFB του DES είναι παρόμοια, γενικά, με τη μέθοδο λειτουργίας CFB. Η κύρια διαφορά τους έγκειται στο γεγονός ότι ο καταχωρητής ολίσθησης επανατροφοδοτείται από την έξοδο της λειτουργίας κρυπτογράφησης, ενώ στη μέθοδο CFB ο καταχωρητής ολίσθησης επανατροφοδοτείται από την κρυπτογραφημένη ακολουθία.

Το πιο βασικό πλεονέκτημα της OFB μεθόδου είναι η διασφάλιση ότι πιθανή εμφάνιση σφαλμάτων κατά τη μετάδοση έχει περιορισμένη επίδραση και μόνο στα αντίστοιχα bits του μηνύματος, συνεπώς επιτυγχάνεται ο περιορισμός διάδοσης σφαλμάτων. Άλλο πλεονέκτημα της μεθόδου OFB αποτελεί η εκ των προτέρων δυνατότητα υπολογισμού των ακολουθιών των κλειδιών, πριν την παραγωγή των ακολουθιών του καθαρού μηνύματος. Η δυνατότητα αυτή οδηγεί σε βελτίωση της επίδοσης του συστήματος.

Παρόλα αυτά, η μέθοδος λειτουργίας OFB διευκολύνει δυνητικούς επιτιθέμενους στην τροποποίηση μηνυμάτων: αφού η τροποποίηση ενός bit μιας ακολουθίας οδηγεί σε αλλαγή του αντίστοιχου bit που λαμβάνει ο παραλήπτης, αυτή την ιδιότητα μπορεί να εκμεταλλευθεί ο επιτιθέμενος ώστε να μη γίνεται αντιληπτή η αλλαγή που προκαλεί από τα αθροίσματα ελέγχου.

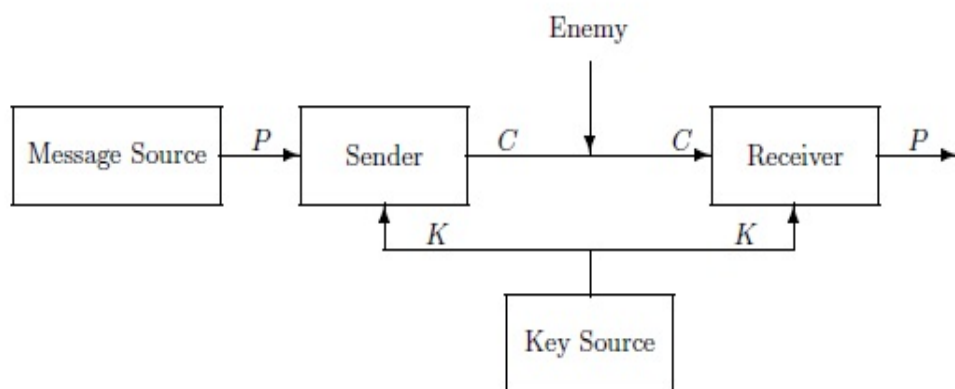
CFB: Cipher FeedBack

Το διάγραμμα DES αποτελεί ουσιαστικά μία τεχνική κρυπταλγορίθμων τμημάτων, η οποία χρησιμοποιεί τμήματα των 64-bit. Παρόλα αυτά, είναι δυνατόν ο DES να μετατραπεί σε κρυπταλγόριθμο

στοιχειοσειράς (stream cipher) χρησιμοποιώντας τη μέθοδο Ανάδρασης Κρυπτογραφημάτων (Cipher FeedBack – CFB). Η αξιοποίηση κρυπταλγορίθμου ροής εξαλείφει την ανάγκη συμπλήρωσης ενός μηνύματος ώστε να αποτελείται από ακέραιο αριθμό τμημάτων, ενώ μπορεί να λειτουργήσει σε πραγματικό χρόνο. Κατά συνέπεια, εάν μεταδίδεται μία ροή χαρακτήρων κάθε χαρακτήρας μπορεί να κρυπτογραφηθεί και να διαβιβαστεί αμέσως χρησιμοποιώντας έναν κρυπταλγόριθμο ροής προσανατολισμένο σε χαρακτήρες.

3.3 Ασφάλεια μυστικού κλειδιού του κρυπταλγορίθμου τμημάτων

Όταν συζητάμε για τη ασφάλεια ενός κρυπτογραφικού συστήματος χρειάζεται να ορίζουμε ένα μοντέλο κατά προσέγγιση πραγματικό. Θα χρησιμοποιήσουμε το μοντέλο του Shannon. [5]



Σχήμα 3.1: Το μοντέλο του Shannon ενός γενικού συστήματος απορρήτου

Ο αποστολέας και ο παραλήπτης μοιράζονται το κοινό κλειδί K , το οποίο μεταδίδεται μέσω ενός ασφαλούς καναλιού. Ο αποστολέας κρυπτογραφεί το αρχικό κείμενο P χρησιμοποιώντας το μυστικό κλειδί K , στέλνει το C (κρυπτοκείμενο) μέσω ενός μη ασφαλούς καναλιού στον παραλήπτη, ο οποίος αποκαθιστά το C σε P χρησιμοποιώντας το K .

Ο εισβολέας έχει πρόσβαση στο μη ασφαλές κανάλι και μπορεί να λάβει το κρυπτοκείμενο. Σε αυτό το σημείο υποθέτουμε πως ο νόμιμος αποστολέας και παραλήπτης χρησιμοποιούν ένα μυστικό κλειδί κρυπτογράφησης $E_K(\cdot)$ με μέγεθος τμήματος n (bits), όπου το K είναι μεγέθους k bits. Για να εμποδίσουμε έναν εισβολέα να εικάσει πως τα νόμιμα μέλη έχουν κατασκευάσει το κοινό τους κλειδί, θα υποθέσουμε :

- **Υπόθεση 1:** Όλα τα κλειδιά είναι εξίσου πιθανά και το K πάντα επιλέγεται τυχαίως ομοιόμορφα.
- **Υπόθεση 2:** Ο εισβολέας (κρυπταναλυτής) γνωρίζει όλες τις λεπτομέρειες διαδικασίας κρυπτογράφησης και αποκρυπτογράφησης εκτός από την αξία του μυστικού κλειδιού.

3.3.1 Ταξινόμηση των επιθέσεων

Οι τύποι των επιθέσεων κρυπτανάλυσης μπορούν γενικότερα να διακριθούν σε πέντε κατηγορίες που είναι άμεσα συνυφασμένες με το είδος της πληροφορίας που διαθέτει ο κρυπταναλυτής που σχεδιάζει την επίθεση και ανάλογα με τις παραπάνω υποθέσεις ταξινομούνται ως εξής:

- **Ciphertext only attack**(Επίθεση μόνο του κρυπτοκειμένου):ο εισβολέας έχει στην διάθεσή του αρκετά κρυπτογραφημένα μηνύματα, με τον ίδιο αλγόριθμο και το ίδιο κλειδί, με σκοπό να μπορεί να υπολογίσει το καθαρό από το κρυπτογραφημένο κείμενο. Επίσης ο κρυπταναλυτής επιδιώκει να αποκρυπτογραφήσει όσο πιο πολλά μηνύματα μπορεί ή και να προσδιορίσει το κρυπτογραφικό κλειδί που χρησιμοποιήθηκε ή ακόμα και να επινοήσει έναν αλγόριθμο που θα του επιτρέψει να υπολογίζει το καθαρό από το κρυπτογραφημένο μήνυμα.
- **Known plaintext attack** (Επίθεση σε γνωστό αρχικό κείμενο):Είναι το είδος της επίθεσης κατά την οποία ο εισβολέας έχει στη διάθεσή του τόσο το δείγμα του κρυπτοκειμένου όσο και το αρχικό κείμενο που αντιστοιχεί σε αυτό. Δηλαδή ο εισβολέας αποκτά $P_1, P_2, \dots, P_s$ ένα σύνολο από s αρχικά κείμενα και τα αντιστοιχα κρυπτοκείμενα $C_1, C_2, \dots, C_s$. Ο κρυπταναλυτής επιδιώκει να προσδιορίσει το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση των μηνυμάτων. Εναλλακτικά επιδιώκει να επινοήσει έναν αλγόριθμο που θα του επιτρέψει να υπολογίζει από το κρυπτογραφημένο μήνυμα το αντίστοιχο καθαρό, το οποίο πλέον γνωρίζει.
- **Chosen plaintext attack** (Επίθεση σε επιλεγμένο αρχικό κείμενο): Ο εισβολέας επιλέγει εκ των προτέρων ένα σύνολο από s αρχικά κείμενα $P_1, P_2, \dots, P_s$ και αποκτά με κάποιο τρόπο πρόσβαση στα αντίστοιχα κρυπτοκείμενα $C_1, C_2, \dots, C_s$. Η επίθεση αυτή είναι πιο ισχυρή από την known plaintext attack, αφού οι κρυπταναλυτές έχουν την δυνατότητα να επιλέξουν τέτοια καθαρά μηνύματα προς κρυπτογράφηση, που δίνουν πιο πολλές πληροφορίες, για το κλειδί που χρησιμοποιείται σε αυτή την κρυπτογράφηση των μηνυμάτων ή να επινοηθεί ένας αλγόριθμος για την αποκρυπτογράφηση των νέων μηνυμάτων, που κρυπτογραφούνται με το ίδιο κλειδί. Μια ειδική περίπτωση αυτού του τύπου επιθέσεων είναι να μπορούν οι κρυπταναλυτές, όχι μόνο να επιλέγουν το καθαρό μήνυμα που κρυπτογραφείται, αλλά και να τροποποιούν την επιλογή βασιζόμενοι στα αποτελέσματα της προηγούμενης κρυπτογράφησης. Δηλαδή αφού επιλέξουν ένα τμήμα από το καθαρό κείμενο, στην συνέχεια να επιλέξουν ένα άλλο τμήμα με βάση τα αποτελέσματα της κρυπτογράφησης του πρώτου κτλ.
- **Adaptively chosen plaintext attack**(Επίθεση σε προσαρμοστικά επιλεγμένο αρχικό κείμενο): Ο εισβολέας επιλέγει ένα σύνολο από αρχικά κείμενα $P_1, P_2, \dots, P_s$ διαδραστικά καθώς αποκτά τα αντίστοιχα κρυπτοκείμενα $C_1, C_2, \dots, C_s$. Αυτό σημαίνει ότι επιλέγει το P_1 , αποκτά το C_1 , έπειτα επιλέγει το P_2 κ.τ.λ. Αποτελεί μία ειδική περίπτωση της chosen plaintext attack και λαμβάνει χώρα κυρίως σε ασύμμετρα κρυπτογραφικά συστήματα.
- **Chosen ciphertext attack** (Επίθεση σε επιλεγμένο κρυπτοκείμενο): Στην περίπτωση αυτή ο εισβολέας μπορεί να επιλέξει ένα τμήμα του κρυπτοκειμένου και να προσπαθήσει να αποκτήσει πρόσβαση στο αντίστοιχο αρχικό κείμενο. Για τους συμμετρικούς αλγορίθμους κρυπτογράφησης αυτή η επίθεση συμπίπτει με την επίθεση σε επιλεγμένο αρχικό κείμενο όπου οι ρόλοι των αρχικών κειμένων και κρυπτοκειμένων εναλλάσσονται. Η επίθεση αυτή γίνεται κυρίως σε ασύμμετρα κρυπτογραφικά συστήματα, όπου το μυστικό κλειδί χρησιμοποιείται για την αποκρυπτογράφηση και αποτελεί το ζητούμενο της επίθεσης, αφού το δημόσιο κλειδί για την κρυπτογράφηση είναι γνωστό σε όλους.
- **man-in the-middle attack**: Αυτή η επίθεση είναι σχετική με την κρυπτογραφημένη επικοινωνία και με τα πρωτόκολλα ανταλλαγής κλειδιών. Η βασική ιδέα είναι πως, όταν τα δύο άτομα, που επικοινωνούν, ανταλλάσσουν κλειδιά, ο επιτιθέμενος 'εγκαθίστανται' στην γραμμή επικοινωνίας. Στην συνέχεια ανταλλάσσει με τον καθένα εκ των δύο διαφορετικό κλειδί. Έτσι τα δύο ενδιαφερόμενα άτομα καταλήγουν να επικοινωνούν μεταξύ τους με ασφάλεια, στην πραγματικότητα όμως ο επιτιθέμενος παρεμβάλλεται και γνωρίζει τα πάντα.

3.3.2 Πρακτικές Απορρήτου

Ο σκοπός της κρυπτανάλυσης ήταν πάντα να βρεθεί ένα μυστικό κλειδί, ώστε να μπορεί ο κρυπταναλυτής να αποκρυπτογραφήσει το κείμενο. Υπάρχει όμως και η περίπτωση επιθέσεων από τρίτους οι οποίες δεν καταφέρνουν να εξάγουν το μυστικό κλειδί. Θα αναφερθούν ακολουθώντας τα είδη των επιθέσεων τα οποία γίνονται κατά κρυπταλγορίθμων τμημάτων:

- **Total break:** Ο εισβολέας βρίσκει το μυστικό κλειδί K .
- **Global deduction:** Ο εισβολέας βρίσκει έναν αλγόριθμο A , λειτουργικά ισοδύναμο με τον $E_K(\cdot)$ χωρίς να ξέρει το κλειδί K .
- **Instance (local) deduction:** Ο εισβολέας βρίσκει το αρχικό κείμενο (κρυπτοκείμενο) από ένα κρυπτοκείμενο (αρχικό κείμενο) το οποίο έχει υποκλέψει και το οποίο δεν έχει αποκτηθεί από τον νόμιμο αποστολέα.
- **Information deduction:** Ο εισβολέας κερδίζει μερικές (Shannon) πληροφορίες για το κλειδί, τα αρχικά κείμενα ή κρυπτοκείμενα τις οποίες δεν τις απέκτησε απευθείας από τον αποστολέα αλλά ούτε τις κατείχε πριν την επίθεση.

Προφανώς η ταξινόμηση είναι ιεραρχική, δηλαδή εάν είναι πιθανή η Total break τότε είναι πιθανή και η Global deduction. Έχει υποθετηθεί ότι οι παραπάνω επιθέσεις είναι ανεξάρτητες από το πως επιλέγονται τα κλειδιά από τα νόμιμα μέλη, δηλαδή χρησιμοποιείται η **Υπόθεση 1**.

Η Global deduction είναι πιθανή όταν ένας κρυπταλγόριθμος τμημάτων περιέχει μία "δομή μπλόκ". Εάν ορισμένα υποσύνολα του κρυπτοκειμένου είναι ανεξάρτητα από ορισμένα υποσύνολα του αρχικού κειμένου, τότε ανεξάρτητα από το πόσο μεγάλο είναι το κλειδί, ο κρυπταλγόριθμος είναι ευάλωτος σε Global deduction με επίθεση σε γνωστό αρχικό κείμενο.

Στους επαναληπτικούς αλγορίθμους κρυπτογραφίας τμημάτων τα κυκλικά κλειδιά δημιουργούνται συνήθως με κάποιον συγκεκριμένο τρόπο και έτσι σε επιθέσεις με τις οποίες κάποιος εισβολέας βρίσκει το κυκλικό κλειδί, πιθανόν να βρει και την πραγματική αξία του μυστικού κλειδιού, αφού με τα κυκλικά κλειδιά μπορεί να κρυπτογραφεί και να αποκρυπτογραφεί.

Η Information deduction μπορεί να γίνει τόσο επικίνδυνη όσο και η Total break, όταν ο αριθμός των αρχικών κειμένων είναι μικρός.

Η επίθεση Information deduction είναι η λιγότερο σοβαρή, όμως οι νόμιμοι χρήστες ενδιαφέρονται για το ότι οι διάφοροι εισβολείς δεν θα πρέπει να πάρουν καμία πληροφορία από τα αρχικά κείμενα, πράγμα το οποίο καθίσταται πολύ επικίνδυνο όταν ο χώρος των αρχικών κειμένων είναι υπεράριθμος.

3.3.3 Brute Force Attacks

Η επίθεση ωμής βίας αναφέρεται στην συνεχόμενη δοκιμή κάποιων πιθανών κλειδιών, ώστε να παραχθεί ένα κρυπτογράφημα με σκοπό την αποκάλυψη του αρχικού κειμένου. Τέτοιου είδους επιθέσεις μπορούν πάντα να πραγματοποιηθούν. Πολλές φορές όμως ο επιτιθέμενος, αρχίζει την επίθεσή του χρησιμοποιώντας τα πιο πιθανά κλειδιά, ώστε τελικά να καταφέρει να βρει το κλειδί σε πιο σύντομο χρόνο. Στην πράξη η όλη προσπάθεια αναζήτησης σταματάει όταν βρεθεί το κλειδί, χωρίς να είναι αναγκαία η περαιτέρω ενημέρωση της λίστας των κλειδιών.

Γενικά κάποιος αλγόριθμος κρυπτογράφησης, θεωρείται ότι είναι σπασμένος, όταν υπάρχει αλγόριθμος που μπορεί να βρει το κλειδί πιο απλά από ότι η μέθοδος brute – force, ανεξαρτήτως από το εάν η προσπάθεια του υπολογισμού είναι δυνατή στην πράξη. Τις πιο πολλές φορές το μήκος των κλειδιών κρυπτογράφησης επιλέγεται έτσι ώστε να απαιτείται υπερβολικά μεγάλος χρόνος υπολογισμών και έτσι να μην υπάρχει χρηστική αξία μιας τέτοιας επίθεσης.

Η επίθεση ωμής βίας λειτουργεί ως εξής, ανάλογα με τα τρία είδη παραβάσεων που αναφέρονται ακολούθως:

- **Total break:** Όλοι οι κρυπταλγόριθμοι τμημάτων είναι σε πλήρη βαθμό εύθραυστοι σε μία επίθεση μόνο του κρυπτοκειμένου, απλά δοκιμάζοντας όλα τα κλειδιά ένα προς ένα και ελέγχοντας εάν το αρχικό κείμενο που υπολογίζεται έχει νόημα, χρησιμοποιώντας μόνο περίπου N_{ud} κρυπτοκείμενα. Αυτή η επίθεση απαιτεί τον υπολογισμό περίπου 2^k κρυπτογραφήσεων. Εναλλακτικά, με την Table look-up attack ο εισβολέας κρυπτογραφεί σε ένα στάδιο προ-υπολογισμού το σταθερό αρχικό κείμενο P , κάτω από όλα τα πιθανά κλειδιά και ταξινομεί και αποθηκεύει όλα τα κρυπτοκείμενα. Στη συνέχεια ο κρυπταλγόριθμος είναι απολύτως εύθραυστος σε μια επίθεση επιλεγμένου αρχικού κειμένου. Ίσως υπάρχουν ορισμένα κλειδιά τα οποία κρυπτογραφούν το P στο ίδιο κρυπτοκείμενο. Επαναλαμβάνοντας την επίθεση μερικές φορές με $P' \neq P$ δίνεται ένα μοναδικό κλειδί.
- **Global/instance deduction:** Όλοι οι κρυπταλγόριθμοι τμημάτων είναι ευάλωτοι σε μία τέτοια παράβαση υπό την επίθεση γνωστού ή επιλεγμένου αρχικού κειμένου.
- **Information deduction:** Όλοι οι κρυπταλγόριθμοι τμημάτων είναι ευάλωτοι σε μία τέτοια παράβαση υπό την επίθεση μόνο του κρυπτοκειμένου.

Θεώρημα 3.3.1. [7] Κάθε κρυπταλγόριθμος τμημάτων n -bit που χρησιμοποιείται στις μεθόδους λειτουργίας ECB, CBC ή CFB είναι ευάλωτος σε μία παράβαση Information deduction με επίθεση μόνο του κρυπτοκειμένου με πολυπλοκότητα περίπου $2^{\frac{n}{2}}$.

Το αποτέλεσμα του θεωρήματος είναι ανεξάρτητο από το μέγεθος του κλειδιού. Επίσης ο Hellman έχει παρουσιάσει μία time-memory trade-off επίθεση για κάθε κρυπταλγόριθμο τμημάτων, η οποία βρίσκει το μυστικό κλειδί μετά από $2^{\frac{2k}{3}}$ κρυπτογραφήσεις χρησιμοποιώντας $2^{\frac{2k}{3}}$ λέξεις από τη μήνη. Οι $2^{\frac{2k}{3}}$ λέξεις από τη μήνη υπολογίζονται σε ένα στάδιο προ-επεξεργασίας, το οποίο διαρκεί όσο χρόνο διαρκούν 2^k κρυπτογραφήσεις.

Για να εκτιμήσει κανείς την πολυπλοκότητα μιας επίθεσης θα πρέπει να σκεφτεί ταυτόχρονα το χρόνο που χρειάζεται, την ποσότητα των δεδομένων που είναι απαραίτητα και το χώρο που απαιτείται.

- **Data Complexity:** Αποτελεί την ποσότητα των δεδομένων που χρειάζονται ως συμβολή σε μία επίθεση. Οι μονάδες μετριοούνται σε blocks μήκους n . Συμβολίζουμε αυτή την πολυπλοκότητα ως C_d .
- **Processing Complexity:** Αποτελεί το χρόνο που χρειάζεται για να προετοιμαστεί η επίθεση. Οι μονάδες του χρόνου μετριοούνται ως ο αριθμός των κρυπτογραφήσεων που ο εισβολέας θα πρέπει να πραγματοποιήσει μόνος. Συμβολίζουμε αυτή την πολυπλοκότητα ως C_p .
- **Storage Complexity:** Αποτελεί τις λέξεις στη μήνη που χρειάζονται ώστε να γίνει η επίθεση. Οι μονάδες μετριοούνται σε blocks μήκους n . Συμβολίζουμε αυτή την πολυπλοκότητα ως C_s .

Κατά κανόνα η πολυπλοκότητα μίας επίθεσης είναι το μέγιστο των τριών πολυπλοκότητων, δηλαδή $C_a = \max(C_d, C_p, C_s)$. Γενικά, υπάρχουν μερικές αποκλίσεις από αυτόν τον κανόνα και οι τρεις τύποι πολυπλοκότητας μιας επίθεσης έχουν άμεση σχέση με τον εισβολέα. Για παράδειγμα, η παραπάνω επίθεση του Hellman στον DES έχει πολυπλοκότητα $2^{2 \times \frac{56}{3}} \cong 2^{38}$. Παρόλο που ο χρόνος

του προ-υπολογισμού είναι 2^{56} , αρχικά αυτό γίνεται μία φορά, μετά την οποία κάθε κλειδί του DES μπορεί να προκύψει με πολυπλοκότητα 2^{38} , έπειτα μπορούν να συμβούν 2^{56} κρυπτογραφήσεις του DES σχετικά γρήγορα σε ειδικά σχεδιασμένες μηχανές λογισμικού. Αφ' ετέρου οι απαιτήσεις αποθήκευσης μπορεί να είναι μη ρεαλιστικές, για παράδειγμα η επίθεση στον DES θα απαιτεί περίπου 1000 Gigabytes μνήμης.

3.4 Σχεδιασμός των κρυπταλγορίθμων τμημάτων

Αρχές σχεδιασμού

Δύο είναι κυρίως οι αποδεκτές αρχές για τον σχεδιασμό πρακτικών κρυπταλγορίθμων τμημάτων, η αρχή της σύγχυσης και της διάχυσης από τον Shannon. Με την σύγχυση καθίσταται η σχέση της απλής στατιστικής, του κρυπτογραφημένου κειμένου, και της απλής περιγραφής του κλειδιού πολύ πολύπλοκη, ενώ στην σύγχυση η στατιστική δομή του αρχικού κειμένου οδηγεί σε πλεονασμό και έτσι διαχέεται σε στατιστικές οι οποίες έχουν μεγάλη εμβέλεια.[5]

O Massey ερμηνεύει τις έννοιες του Shannon για σύγχυση και διάχυση ως εξής:[8]

- **Confusion**(Σύγχυση): Οι στατιστικές του κρυπτοκειμένου θα πρέπει να εξαρτώνται από τις στατιστικές του αρχικού κειμένου με τρόπο τόσο περίπλοκο για να αξιοποιηθεί από τους κρυπταναλυτές.
- **Diffusion**(Διάχυση): Κάθε χαρακτήρας του αρχικού κειμένου και κάθε χαρακτήρας του μυστικού κλειδιού θα πρέπει να επηρεάζουν πολλούς χαρακτήρες του κρυπτοκειμένου.

3.5 Επιθέσεις στους Αλγορίθμους Μυστικού Κλειδιού

3.5.1 Διαφορική Κρυπτανάλυση (Differential Cryptanalysis)

Η διαφορική κρυπτανάλυση είναι μια επίθεση του τύπου επιλεγμένου κειμένου, δηλαδή αυτά τα δεδομένα τα οποία θα πρέπει να γνωρίζει ο αντίπαλος, είναι κάποια ζεύγη απλού κειμένου το οποίο θα πρέπει να διαλέξει. Τις πιο πολλές φορές οι επιθέσεις αυτές χρειάζονται πολλά δεδομένα, ώστε να υπάρχει η δυνατότητα υλοποίησης. Σε αυτό το είδος της επίθεσης ο αντίπαλος ορίζει μια σχέση που συνήθως είναι XOR, μεταξύ ζευγών απλού κειμένου για το οποίο το αποτέλεσμα είναι γνωστό π.χ. η σχέση $p \oplus p' = d$ μας δίνει την διαφορά d μεταξύ των ποσοτήτων p και p' . Η επίθεση του αντιπάλου συνεχίζεται με το να προσπαθεί να βρει κάποια x και x' , ώστε να ισχύει η σχέση $x \oplus x' = e$ με μεγάλη πιθανότητα (όπου το e είναι μια γνωστή ποσότητα). Ακολούθως ορίζονται τα χαρακτηριστικά μονοπάτια για κάθε παράγοντα του κρυπτογραφήματος, που είναι μονοπάτια διαφορών. Όταν συνδυάσουμε τα μονοπάτια όλων των παραγόντων, καταλήγουμε σε χαρακτηριστικά μονοπάτια του κάθε γύρου. Επειδή τα χαρακτηριστικά μονοπάτια επαναλαμβάνονται, στο τέλος θα έχουμε μονοπάτια για πολλούς γύρους. Έτσι οδηγούμαστε στον προσδιορισμό ενός διαφορικού. Διαφορικό ονομάζουμε την συλλογή χαρακτηριστικών μονοπατιών που καθορίζεται στην αρχή και στο τέλος του κρυπτογραφήματος.

Η επίθεση τώρα ολοκληρώνεται με την επιλογή ενός trial key και έλεγχο για να δούμε αν είναι σωστό. Συγκεκριμένα για ένα κρυπτοσύστημα με r γύρους, ο αντίπαλος φτιάχνει ένα διαφορικό $r - 1$ γύρων. Έστω τώρα ότι η επίθεση άρχισε με ένα ζεύγος απλού κειμένου (p, p') . Μετά τους $r - 1$ γύρους θα έχουμε το διαφορικό $x \oplus x'$, ο οποίος ισχύει με πιθανότητα P , ενώ το

κρυπτοκειμένο είναι το (c, c') . Άρα ισχύει ότι: $c = E_k(x)$ και $c' = E_k(x')$ ή ισοδύναμα $x = E_k^{-1}(c)$ και $x' = E_k^{-1}(c')$. Συνδυάζοντας τις δύο τελευταίες εξισώσεις έχουμε

$$e = x \oplus x' = E_k^{-1}(c) \oplus E_k^{-1}(c')$$

Άρα ο αντίπαλος υπολογίζει την σχέση $E_k^{-1}(c) \oplus E_k^{-1}(c')$, για κάθε trial key και αν $k = k'$ τότε $E_k^{-1}(c) \oplus E_k^{-1}(c') = e$ με πιθανότητα P ενώ αν $k \neq k'$ τότε $E_k^{-1}(c) \oplus E_k^{-1}(c') \neq e$ με τυχαία πιθανότητα.

Για τον DES ο υπολογισμός των πιθανοτήτων βασίζεται στα S-Boxes. Τα S-Boxes λέγονται κουτιά αντικατάστασης και αποτελούν συνήθως το μοναδικό μη γραμμικό στάδιο ενός αλγορίθμου κρυπτογράφησης. Κατά την διάρκεια της λειτουργίας του το S-Box προβαίνει σε αντιστοίχιση μιας ακολουθίας από m bits που λαμβάνει ως είσοδο, με μια άλλη ακολουθία από n bits που αποτελεί το αποτέλεσμα στην έξοδό του. Η αναπαράστασή τους γίνεται με έναν πίνακα και για την υλοποίησή τους, από τις γλώσσες προγραμματισμού, χρησιμοποιείται ένας πίνακας που έχει μια διάσταση, (για το S-Box μικρού μεγέθους), η είσοδος αποτελεί τον δείκτη του πίνακα, ενώ το περιεχόμενό του αποτελεί την έξοδο. Τα S-Boxes κατά την λειτουργία τους δημιουργούν αόριστες και δύσκολα ανιχνεύσιμες διαφορές μεταξύ του αρχικού κειμένου και του παραγόμενου κρυπτοκειμένου. Οι συναρτήσεις αντικατάστασης πρέπει να είναι αντιστρέψιμες έτσι ώστε να επιτρέπουν την αποκωδικοποίηση του κρυπτοκειμένου. Όμως έτσι καθίσταται όλο το σύστημα του αλγορίθμου μη ασφαλές. Για να μην συμβεί αυτό, θα πρέπει οι συναρτήσεις αντικατάστασης να ενισχυθούν με την ιδιότητα της διάχυσης και με την λειτουργία της ανάμειξης των κλειδιών κρυπτογράφησης στα διάφορα στάδια της εφαρμογής τους. Η εισαγωγή της ιδιότητας της σύγχυσης σε έναν αλγόριθμο κρυπτογράφησης, προσφέρει σημαντικό βαθμό αντίστασης σε περιπτώσεις που θα υπάρξει πιθανή διαφορική ή γραμμική επίθεση κρυπτανάλυσης.

Η διαφορική κρυπτανάλυση στηρίζεται στην ανάλυση της εξέλιξης που παρουσιάζουν οι διαφορές ανάμεσα σε δύο συσχετιζόμενα plaintexts, που κρυπτογραφούνται με το ίδιο κλειδί. Με προσεκτική ανάλυση των σχετιζομένων δεδομένων, μπορεί κάποιος να δημιουργήσει πιθανά κλειδιά, τα οποία μπορεί να χρησιμοποιήθηκαν για την κρυπτογράφηση.

Στο DES για κάθε S-Box κατασκευάζεται ένας πίνακας 64×16 με στοιχεία

$$N_i(a, b) = \#\{x \in Z_2^6 | S_i(x) \oplus S_i(x \oplus a) = b\}$$

η πιθανότητα υπολογίζεται ως $2^{-6} N_i(a, b)$. Η μέγιστη τιμή για το $N_i(a, b)$ είναι 16 και το καλύτερο χαρακτηριστικό μονοπάτι ισχύει με πιθανότητα $\frac{1}{234}$. Μετά από 14 γύρους έχουμε 2^{-55} . Η χρονική πολυπλοκότητα της επίθεσης είναι αντιστρόφως ανάλογη της πιθανότητας του χαρακτηριστικού μονοπατιού, άρα για το DES η διαφορική επίθεση θέλει χρόνο $O(2^{55})$, που είναι ανάλογο του χρόνου της εξαντλητικής μεθόδου.

3.5.2 Γραμμική Κρυπτανάλυση Linear Cryptanalysis

Αυτή είναι μια επίθεση του τύπου γνωστού απλού κειμένου, στο οποίο ο επιτιθέμενος προσπαθεί να βρει κάποιες γραμμικές σχέσεις, που πιθανώς να υπάρχουν, μεταξύ ενός υποσυνόλου από αρχικά κείμενα και ενός από state bits, πριν όμως εφαρμοστούν οι αντικαταστάσεις οι οποίες θα εκτελεστούν στον τελευταίο γύρο. Για τα στοιχεία του κρυπτοσυστήματος τα οποία δεν είναι γραμμικά, ο αντίπαλος βρίσκει προσεγγίσεις οι οποίες είναι αληθείς και μάλιστα με πιθανότητα $\frac{1}{2} + \epsilon$. Όταν λοιπόν συνδυαστούν οι προσεγγίσεις για το κάθε στοιχείο του κρυπτοσυστήματος, τότε βρίσκονται οι προσεγγίσεις για ένα γύρο και αν τελικά αυτές συνδυαστούν, βρίσκονται προσεγγίσεις για όλο το κρυπτοσύστημα. Από όλες λοιπόν τις προσεγγίσεις στο τέλος παίρνουμε την πληροφορία για ένα bit κλειδιού. Το συνολικό μέγεθος των δεδομένων το οποίο χρειάζεται ο επιτιθέμενος είναι ανάλογο του $\frac{1}{\epsilon^2}$.

Οι τεχνικές αυτού του τύπου της κρυπτανάλυσης (της γραμμικής), χρησιμοποιούν προσεγγίσεις οι οποίες δίδουν την δυνατότητα να περιγραφεί η συμπεριφορά ενός αλγορίθμου τμημάτων. Αν τώρα κάποιος έχει στην διάθεσή του πολλά ζεύγη από plaintext και το αντίστοιχο κρυπτογράφημα που προκύπτει, έχει την δυνατότητα να ανακτήσει κάποια κομμάτια πληροφορίας, τα οποία αποτελούν το κλειδί κρυπτογράφησης. Όσο μεγαλύτερη είναι η πληροφορία που έχει κάποιος στην διάθεσή του, τόσες περισσότερες πιθανότητες έχει να δημιουργήσει το σωστό κλειδί. Η τεχνική αυτή αναπτύχθηκε εναντίον του αλγορίθμου DES. Ο DES είναι ανθεκτικός στην γραμμική κρυπτανάλυση, λόγω των κριτηρίων τα οποία ικανοποιούν τα S-boxes και την συνάρτηση αντιμετάθεσης P.

3.5.3 Επίθεση στα Αδύναμα Κλειδιά

Τα αδύναμα κλειδιά είναι κάποια μυστικά κλειδιά τα οποία έχουν μια συγκεκριμένη τιμή και για τα οποία το κρυπτογραφημένο κείμενο θα παρουσιάζει κάποιου είδους συμμετρία στην κρυπτογράφηση του κειμένου ή σε κάποιες άλλες περιπτώσεις το επίπεδο της κρυπτογράφησης είναι χαμηλό. Στην περίπτωση του αλγορίθμου DES υπάρχουν τέσσερα κλειδιά ενώ για τον IDEA υπάρχει κάποια ομάδα κλειδιών για τα οποία η κρυπτανάλυση διευκολύνεται σημαντικά και το κλειδί υπάρχει η δυνατότητα να ανακτηθεί. Τώρα για τους άλλους αλγορίθμους ο αριθμός των αδύναμων κλειδιών πιθανόν να είναι τόσο μεγάλος ώστε να δημιουργεί απειλή για την ικανότητά τους να αντιστέκονται σε επιθέσεις.

3.5.4 Αλγεβρικές Επιθέσεις

Οι αλγεβρικές επιθέσεις είναι μια κατηγορία από τεχνικές, των οποίων η επιτυχία εξαρτάται από το εάν κρυπτογραφήματα ομάδας παρουσιάζουν, σε αρκετά μεγάλο βαθμό, δομή μαθηματική. Όταν ένα κρυπτοκείμενο ομάδας παρουσιάζει δομή ομαδοποιημένη, τότε αν γινόταν κρυπτογράφηση σε κάποιο κείμενο με ένα κλειδί και αμέσως μετά εκτελούσαμε κρυπτογράφηση στο κρυπτοκείμενο που κρυπτογραφήθηκε πριν με ένα άλλο κλειδί, θα υπήρχε ένα αποτέλεσμα το οποίο θα ήταν ισοδύναμο με το κείμενο που θα προέκυπτε αν εκτελείτο κρυπτογράφηση στο αρχικό κείμενο με ένα τρίτο κλειδί. Με τον τρόπο όμως αυτό το κρυπτοκείμενο ομάδας δεν έγινε πολυπλοκότερο αλλά ούτε και περισσότερο ασφαλές, αφού θα μπορούσε να παραχθεί το ίδιο αποτέλεσμα εάν κρυπτογραφείτο το αρχικό κείμενο με ένα άλλο κλειδί.

3.6 Block and Key Size

Ένας κρυπταλγόριθμος τμημάτων είναι ευάλωτος σε μια επίθεση brute force attack στην περίπτωση που το μέγεθος ή του block ή του κλειδιού ή και των δύο αυτών είναι πολύ μικρό σε μέγεθος. Τέτοιες επιθέσεις στους αλγορίθμους είναι ανεξάρτητες από την δομή τους. Το μέγεθος των πιο πολλών από τους κρυπταλγορίθμους τμημάτων όπως οι DES, IDEA, FEAL, LOKI, SAFER, SHARK, είναι 64 bits. Γι' αυτούς τους αλγορίθμους όταν δέχονται επίθεση, απαιτείται η αποθήκευση 2^{32} τμημάτων κρυπτοκειμένου, ώστε να υπάρχει επιτυχής αντιμετώπιση στο μισό. Στην αρχή φαίνεται σχεδόν απίθανο να χρησιμοποιείται ένα και μόνο κλειδί, για να επεξεργαστούν μεγάλο αριθμό κρυπτοκειμένων. Στην συνέχεια η αποθήκευση των 2^{32} τμημάτων κρυπτοκειμένων για κάθε 64 bits θα απαιτεί περίπου $2^5 GB$ μνήμης. Στην περίπτωση δε που κάποιος επιτιθέμενος έχει την δυνατότητα να προβλέψει στο περίπου με πόση συχνότητα αλλάζει ένα κλειδί κρυπτογράφησης, μπορεί να επαναλάβει την επίθεση επανειλημμένα, με πιο λίγα τμήματα κρυπτοκειμένων, ώστε να έχει όσο γίνεται μεγαλύτερη πιθανότητα επιτυχίας.

Ο DES έχει μέγεθος κλειδιού 56 bits το οποίο είναι αρκετά μικρό. Οι κρυπταλγόριθμοι τμημάτων όπως οι IDEA, SAFER, SK-128, SHARK, SQUARE έχουν μέγεθος 128 bits. Οι RC5 και Blowfish έχουν ποικιλία μεγεθών κλειδιού. Υπάρχει εκτίμηση ότι για τα επόμενα χρόνια ένα μέγεθος κλειδιού των 90 bits θα είναι επαρκές.

3.7 Ευρέως Χρησιμοποιούμενοι Συμμετρικοί Αλγόριθμοι Κρυπτογράφησης

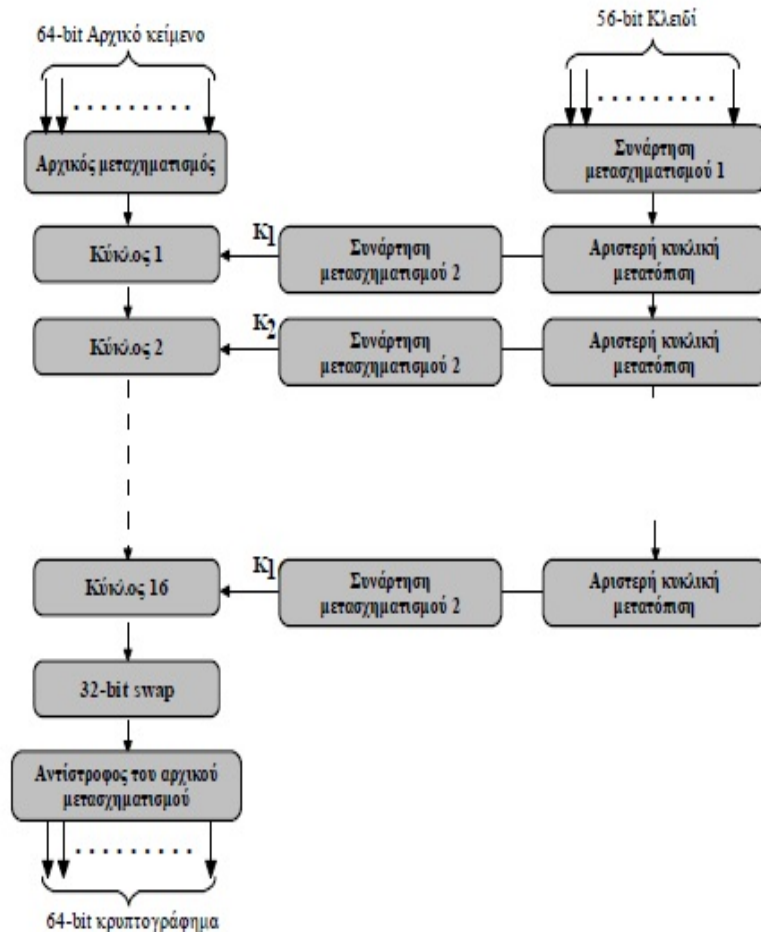
Οι περισσότεροι από τους συμμετρικούς αλγόριθμους που χρησιμοποιούνται περισσότερο, ακολουθούν μια λογική που είναι ίδια με αυτή της κρυπτογράφησης τμημάτων και ονομάζονται κωδικοποιητές τμημάτων. Οι πιο γνωστοί αλγόριθμοι οι οποίοι ακολουθούν αυτή την λογική είναι ο DES και ο TDES με την μετάβαση κατόπιν στον AES. Υπάρχουν ακόμα και άλλοι κωδικοποιητές ομάδων όπως ο MARS, ο RC2, ο RC4, ο RC5, ο RC6, ο Serpent, ο Twofish, ο Rijndael, ο IDEA, ο Blowfish και ο Cast-128.

3.7.1 DES (Data Encryption Standard)

Ο αλγόριθμος DES είναι αυτός ο οποίος χρησιμοποιήθηκε περισσότερο από του υπόλοιπους. Σχεδιάστηκε από την IBM και υιοθετήθηκε από το ινστιτούτο NIST National Institute of Standards and Technology σαν FIPS PUB 46 (Federal Information Processing Standard 46). Ο αλγόριθμος ο οποίος υλοποιήθηκε στο σύστημα DES αναφέρεται σαν DEA.

Ο αλγόριθμος DES χρησιμοποιεί το ίδιο κλειδί και στην κρυπτογράφηση, αλλά και στην αποκρυπτογράφηση. Είναι ένας αλγόριθμος τύπου Feistel με 16 ανακυκλώσεις και ο οποίος κυρίως χρησιμοποιείται για εμπορικές εφαρμογές. Το μήκος του κρυπτογραφήματος είναι στα 64 bits και το μήκος του κλειδιού είναι στα 56 bits. Αυτό που θα πρέπει να προσεχθεί είναι ότι τα κλειδιά του αλγορίθμου DES είναι συνήθως κλειδιά που αναπαρίστανται σαν σειρές από χαρακτήρες των 64 bits, από τα οποία τα 8 bits παράγονται σαν ψηφία ισοτιμίας και των υπολοίπων 56 bits. Έτσι το αποτέλεσμα είναι ότι για τον DES μπορούν να υπάρξουν μόνο 256 κλειδιά τα οποία είναι διαφορετικά και για τον λόγο αυτό θεωρείται ότι το μήκος του κλειδιού του είναι 56 bits. Για κάθε λοιπόν κλειδί με μήκος 56 bits παράγονται 16 μέρη κλειδιού που το κάθε μέρος έχει μήκος 48 bits.

Στο Σχήμα που ακολουθεί φαίνεται η δομή του DES όπου το μεν αρχικό κείμενο είναι μεγέθους των 64 bits και το μήκος του κλειδιού είναι στα 56 bits, αν τύχει και το κείμενο είναι πιο μεγάλου μεγέθους, τότε χωρίζεται σε κομμάτια των 64 bits, ώστε να μπορεί κάποιος να το επεξεργαστεί ευκολότερα.



Σχήμα 3.2: Γενική περιγραφή του αλγορίθμου κρυπτογράφησης DES

Στην αριστερή πλευρά του παραπάνω σχήματος φαίνονται τα τρία στάδια στα οποία εκτελείται η επεξεργασία του κειμένου. Αρχικά στο κείμενο γίνεται ένας αρχικός μετασχηματισμός, μέσα στα πλαίσια του οποίου τα bits αναδιατάσσονται ώστε να μπορέσει να δημιουργηθεί η είσοδος που μόλις μετασχηματίστηκε. Στην συνέχεια υπάρχει ένα στάδιο που περιλαμβάνει 16 επαναλήψεις που έχουν ίδια λειτουργία. Στο τέλος της 16ης επανάληψης η έξοδος αποτελείται από 64 bits τα οποία έχουν σχέση με το αρχικό κείμενο και το κλειδί. Κατόπιν το αριστερό μισό και το δεξιό μισό τμήμα της εξόδου αλλάζουν μεταξύ τους, με αποτέλεσμα να παραχθεί η αρχική έξοδος. Στην τιμή αυτή γίνεται τροποποίηση βάση ενός μετασχηματισμού, ώστε να παραχθεί το κρυπτοκείμενο των 64 bits.

Στο τμήμα της δεξιάς πλευράς του σχήματος παρουσιάζεται ο τρόπος με βάση τον οποίο χρησιμοποιείται το κλειδί των 56 bits. Στην αρχή το κλειδί υπόκειται σε τροποποίηση από μια συνάρτηση μετασχηματισμού. Ακολουθεί για την κάθε μια από τις 16 επαναλήψεις η παραγωγή και ενός υποκλειδιού το οποίο προκύπτει από έναν συνδυασμό μιας αριστερής κυκλικής μετατόπισης και ενός μετασχηματισμού. Ας σημειωθεί ότι η συνάρτηση του μετασχηματισμού παραμένει ίδια στην κάθε επανάληψη, αλλά και την κάθε φορά παραγωγής διαφορετικού υποκλειδιού, εξαιτίας της συνεχόμενης και επαναλαμβανόμενης μετατόπισης των ψηφίων που έχει το κλειδί.

Στον αλγόριθμο DES το κλειδί που έχει μήκος 56 bits, το οποίο και χρησιμοποιείται σαν είσοδος, τροποποιείται με κάποια μετάθεση που θα γίνει. Αυτό το κλειδί των 56 bits που θα προκύψει από αυτή την διαδικασία, αντιμετωπίζεται ακολούθως σαν να είναι δύο ποσότητες των 28 bits. Στην κάθε επανάληψη, οι ποσότητες αυτές υποβάλλονται ξεχωριστά σε μια αριστερή κυκλική

μετατόπιση ή σε κάποια περιστροφή ενός ή δύο bits. Οι τιμές λοιπόν που έχουν υποστεί μετατοπίσεις χρησιμεύουν σαν είσοδοι στην επανάληψη η οποία θα ακολουθήσει αμέσως μετά. Ακόμη χρησιμοποιούνται και σαν είσοδοι σε μια άλλη συνάρτηση μετασχηματισμού, η οποία συνάρτηση παράγει έξοδο που είναι μεγέθους 48 bits και η οποία αμέσως μετά γίνεται είσοδος για την εν λόγω συνάρτηση. Η ίδια διαδικασία ακολουθείται και για την αποκρυπτογράφηση, μόνο που τα κλειδιά τοποθετούνται σε αντίστροφη σειρά.

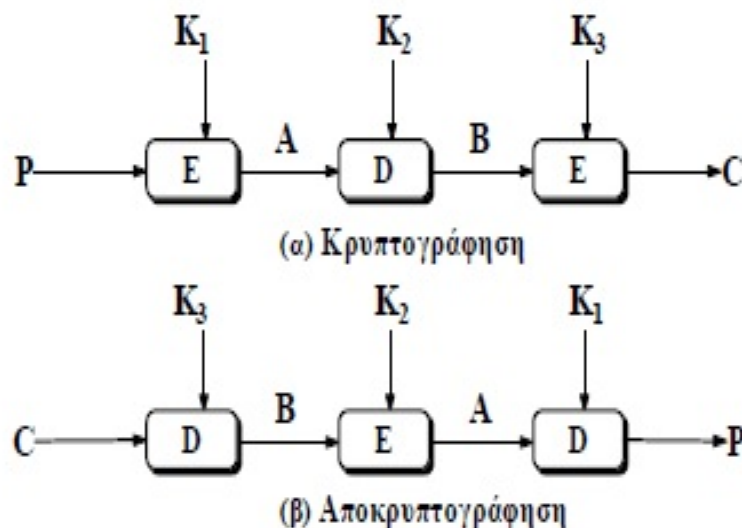
3.7.2 TDES (Triple Data Encryption Standard)

Ο TDES ή TDEA ή συνήθως 3DES, προτάθηκε αρχικά από τον W. Tuchman και το 1985 προτυποποιήθηκε στο ANSI X9.17, ώστε να χρησιμοποιηθεί σε οικονομικές εφαρμογές. Το 1999 ο TDES ενσωματώθηκε σαν τμήμα της προτυποποίησης κρυπτογράφησης δεδομένων DES. Ο TDES ακολουθεί τον 2DES, που δεν αξιοποιήθηκε ευρέως, γιατί θεωρήθηκε ευάλωτος σε επιθέσεις τύπου ενδιάμεσου (man-in-the-middle attack).

Στον TDES το μήνυμα κρυπτογραφείται και αποκρυπτογραφείται διαδοχικά με διαφορετικά κλειδιά, για την ενίσχυση του βασικού αλγορίθμου. Υπάρχουν διάφοροι τρόποι για να επιτευχθεί αυτό όπως π.χ.:

- **DES-EEE3 (Encrypt- Encrypt- Encrypt):** το μήνυμα διαδοχικά κρυπτογραφείται με τρία διαφορετικά κλειδιά.
- **DES-EDE3 (Encrypt- Decrypt- Encrypt):** το μήνυμα διαδοχικά κρυπτογραφείται, αποκρυπτογραφείται και τέλος κρυπτογραφείται με χρήση τριών διαφορετικών κλειδιών.

Ο TDES είναι ένας πολύ καλός αλγόριθμος, που για τον λόγο του ότι προέρχεται από τον DES, έχει την ίδια με αυτόν αντοχή σε διάφορες επιθέσεις. Επειδή ακόμη το μήκος κλειδιού είναι στα 168 bits, μπορεί ο αλγόριθμος αυτός να αντιμετωπίσει επιθέσεις εξαντλητικής αναζήτησης, τις οποίες κάνει πρακτικά αδύνατον να εκπληρωθούν. Για τον λόγο αυτός ο αλγόριθμος TDES θα χρησιμοποιείται όλο και περισσότερο τα χρόνια που ακολουθούν έως ότου υπάρξει μετάβαση στον AES. Παρακάτω έχουμε ένα σχήμα στο οποίο φαίνεται η λειτουργία του TDES.



Σχήμα 3.3: Γενική περιγραφή του αλγορίθμου κρυπτογράφησης TDES

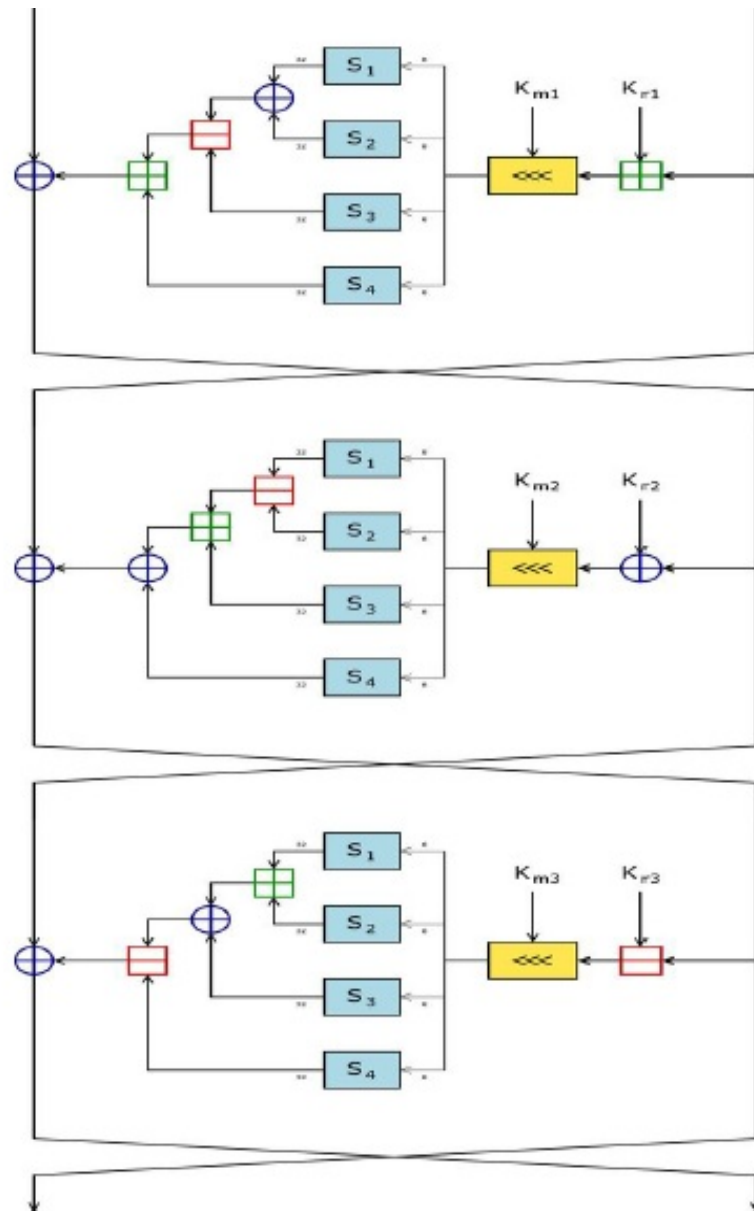
3.7.3 CAST-128

Ο CAST είναι ένας αλγόριθμος συμμετρικής κρυπτογράφησης ο οποίος αναπτύχθηκε το έτος 1997 από τους C. Adams και S. Tavares της εταιρείας Entrust Technologies και είναι η βάση για την διαδικασία με την οποία θα σχεδιάζονται άλλοι αλγόριθμοι της ίδιας κατηγορίας. Ένας άλλος αλγόριθμος ο οποίος αναπτύχθηκε στο τμήμα όπου γινόταν η μελέτη του CAST είναι ο CAST-128. Σε αυτόν χρησιμοποιείται κλειδί του οποίου το μέγεθος παίρνει τιμές από 40 μέχρι και 128 bits και το βήμα του είναι 8 bits. Η έρευνα, η μελέτη καθώς και η ανάπτυξή του αλγορίθμου CAST κράτησε μεγάλο χρονικό διάστημα με αποτέλεσμα να έχουν διατυπωθεί διάφορα σχόλια, από διάφορους κρυπταναλυτές, για τον συγκεκριμένο αλγόριθμο, είτε αυτά ήταν θετικά είτε ήταν αρνητικά.

Το CAST είναι μια διαδικασία που χρησιμοποιεί S-boxes τα οποία είναι σταθερά, αλλά μόνο αυτά που είναι κατά πολύ πιο μεγάλα από αυτά τα οποία χρησιμοποιεί ο DES. Τα S-boxes για να μπορούν να έχουν αντοχή σε διάφορες επιθέσεις κάποιων κακόβουλων θα πρέπει να έχουν σχεδιαστεί με τέτοιον τρόπο που να μην υπάρχει γραμμικότητα μεταξύ εισόδου και εξόδου.

Τα υποκλειδιά για τον CAST-128 ακολουθούν μια διαδικασία παραγωγής τους η οποία είναι εντελώς διαφορετική με αυτή που ακολουθείται για τους άλλους συμβατικούς αλγορίθμους κρυπτογράφησης τμημάτων. Αυτοί που σχεδίασαν τον CAST προσπάθησαν να παράγουν κλειδιά που θα αντέχουν στις γνωστές επιθέσεις και αυτό μπορεί να επιτευχθεί με την δημιουργία κλειδιών από το βασικό κλειδί με τη χρήση όμως κάποιων S-boxes, τα οποία παρουσιάζουν γραμμικότητα.

Ένα χαρακτηριστικό που αφορά τον CAST-128 και το οποίο παρουσιάζει μεγάλο ενδιαφέρον, είναι η συνάρτηση κύκλου, η οποία διαφέρει από κύκλο σε κύκλο, καθιστώντας έτσι αυτόν τον αλγόριθμο ακόμα πιο ανθεκτικό.



Σχήμα 3.4: Αλγόριθμος CAST-128

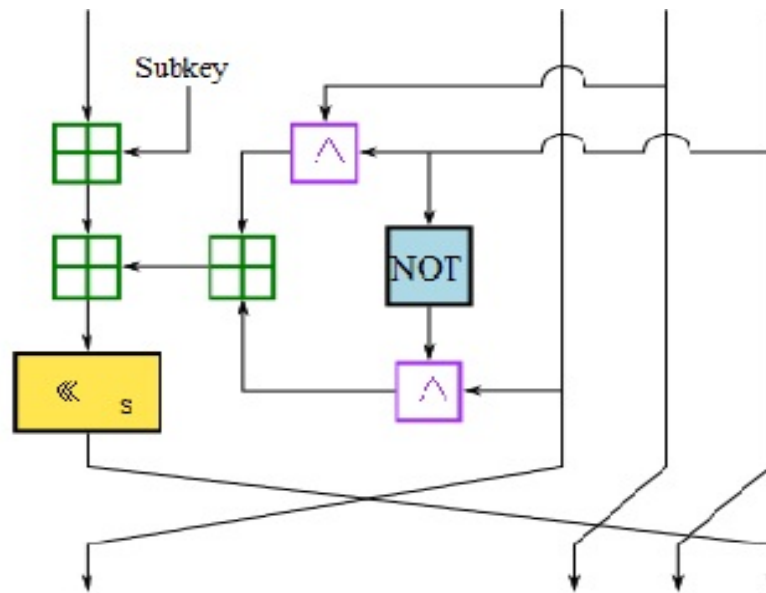
3.7.4 MARS

Ο αλγόριθμος MARS, περιλαμβάνει 32 κύκλους για μετασχηματισμούς, από τους οποίους μόνο οι 16 είναι αυτοί οι οποίοι βασίζονται στο μυστικό κλειδί, οι πράξεις δε που μπορούν να γίνουν είναι η πρόσθεση και ο πολλαπλασιασμός με κλειδιά τα οποία έχουν μήκος 32 bits, καθώς και η περιστροφή ή η ολίσθηση των δεδομένων. Οι 16 κύκλοι οι οποίοι απομένουν αξιοποιούν 8 S-boxes μεγέθους 32 S-bits με πράξεις οι οποίες μπορούν να λάβουν χώρα την πρόσθεση και την πράξη XOR.

3.7.5 RC2

Ένας άλλος αλγόριθμος συμμετρικής κρυπτογράφησης είναι ο RC2 ο οποίος αναπτύχθηκε από τον Ron Rivest της εταιρείας RSA Security κατά το έτος 1987. Αυτός ο κρυπταλγόριθμος τμήματος έχει μέγεθος 64 bits και χρησιμοποιεί 18 γύρους σε δίκτυο Feistel. Ένα βασικό χαρακτηριστικό

το οποίο έχει αυτός ο αλγόριθμος είναι ότι χρησιμοποιεί κλειδιά τα οποία είναι μεταβλητά και έχουν μήκος από 8 bits έως και 128 bits. Αν συμβεί το μέγεθος του κλειδιού να έχει μήκος πιο μεγάλο από τα 56 bits, τότε έχει μεγαλύτερη αντοχή σε επιθέσεις από ότι ο DES.



Σχήμα 3.5: Αλγόριθμος RC2

3.7.6 RC4

Ο RC4 είναι ένας από τους αλγορίθμους stream cipher ο οποίος σχεδιάστηκε, όπως και ο RC2 στα εργαστήρια της εταιρείας RSA Security κατά το έτος 1987 από τον Ron Rivest. Χρησιμοποιείται σε ευρεία κλίμακα για εμπορικές εφαρμογές όπως είναι η Oracle SSL, τα Microsoft Windows και τα SSL. Εκτός όμως αυτών των εφαρμογών χρησιμοποιείται και από πρότυπα IEEE 802.11 μέσω του Wireless Encryption Protocol (WEP) χρησιμοποιώντας όμως κλειδιά τα οποία έχουν μήκος 40 bits και 128 bits. Υπάρχουν όμως τεχνικές με τις οποίες κάποιος επιτιθέμενος μπορεί να παραβιάσει τα μέτρα ασφαλείας του WEP.

Στον αλγόριθμο RC4 το κλειδί το οποίο χρησιμοποιείται δεν έχει καμία σχέση με το αρχικό κείμενο στο οποίο χρησιμοποιήθηκε, αφού είναι εντελώς ανεξάρτητο. Σε ένα 8X8 S-box στο οποίο κάθε είσοδος είναι μια μετάθεση των αριθμών από 0 έως 255 και αποτελούν την συνάρτηση ενός κλειδιού το οποίο έχει μεταβλητό μήκος που κυμαίνεται από 40 bits έως και 256 bits. Στον αλγόριθμο αυτό υπάρχουν ακόμα δύο μετρητές με αρχική τιμή το μηδέν. Έτσι δημιουργείται μια ροή που είναι ψευδοτυχαία από bits, η οποία όμως έχει σχέση και συνδυάζεται με το αρχικό κείμενο, χρησιμοποιώντας την λογική πράξη XOR.

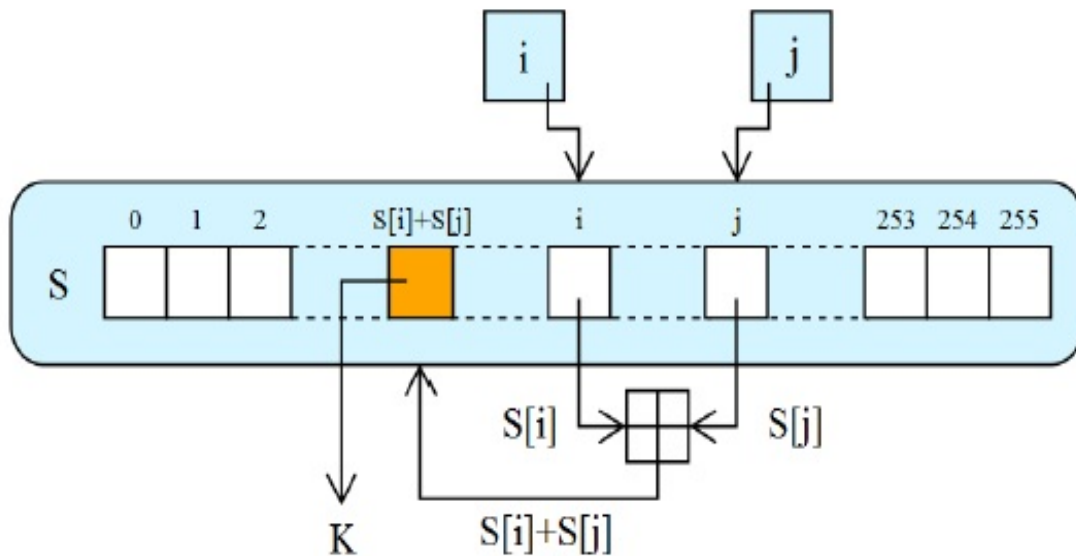
Αυτός ο αλγόριθμος υλοποιείται περνώντας από δύο φάσεις, πρώτα τη δημιουργία κλειδιού, που είναι και η πιο δύσκολη διαδικασία και ακολούθως τη φάση της κρυπτογράφησης.

Τα πλεονεκτήματα του αλγορίθμου είναι:

- Η δυσκολία του να καθίσταται γνωστό το που βρίσκεται η κάθε τιμή του πίνακα.
- Η δυσκολία του να είναι γνωστό ποια θέση στον πίνακα χρησιμοποιείται για την επιλογή της κάθε τιμής στην ροή.
- Το κάθε κλειδί μπορεί να χρησιμοποιηθεί μόνο μια φορά.

- Ο αλγόριθμος αυτός είναι περίπου κατά δέκα φορές πιο ταχύς από τον DES.

Παρουσιάζει όμως και κάποια μειονεκτήματα όπως ότι ένα κλειδί σε κάθε 256 κλειδιά μπορεί να είναι αδύναμο.



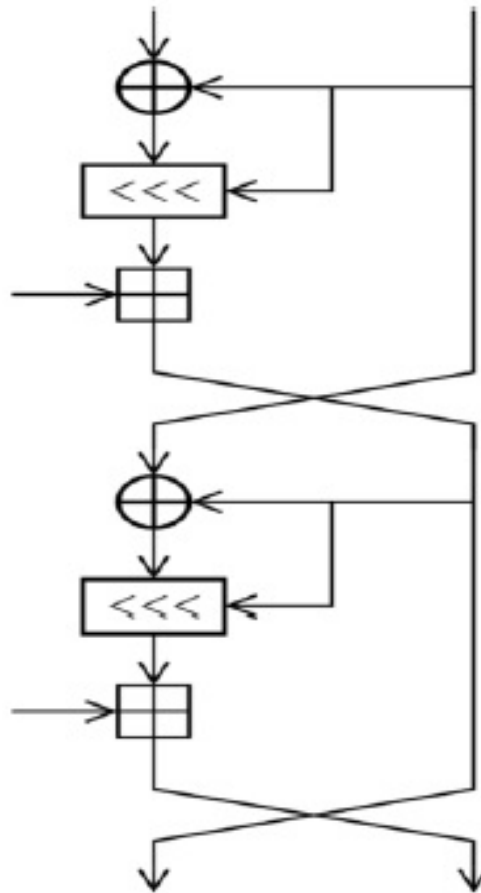
Σχήμα 3.6: Αλγόριθμος RC4

3.7.7 RC5

Τον αλγόριθμο RC5 ανέπτυξε ο Ron Rivest, το έτος 1994, και ήταν ένας από αυτούς που σχεδίασαν τον αλγόριθμο RSA. Ο συμμετρικός κρυπταλγόριθμος RC5 σχεδιάστηκε με τέτοιον τρόπο ώστε να μπορεί να υποστηρίζει τα εξής χαρακτηριστικά:

- Είναι κατάλληλος για να υλοποιηθεί σε υλικό ή λογισμικό.
- Είναι ταχύς και οι βασικές του λειτουργίες στηρίζονται σε πλήρεις λέξεις δεδομένων την κάθε στιγμή.
- Έχει προσαρμοστικότητα σε επεξεργαστές που εκτελούν διαφορετικά μήκη λέξεων τα οποία παράγουν διαφορετικούς αλγορίθμους.
- Υπάρχει μήκος γύρων το οποίο μεταβάλλεται. Ο αριθμός των γύρων επιτρέπει την εναλλαγή ανάμεσα σε υψηλότερη ταχύτητα και υψηλότερη ασφάλεια.
- Έχει μεταβαλλόμενο μήκος κλειδιού, που επιτρέπει να εναλλάσσεται η υψηλότερη ταχύτητα με την υψηλότερη ασφάλεια.
- Ο αλγόριθμος RC5 είναι απλός, αφού έχει απλή δομή, υλοποιείται εύκολα και διευκολύνει στο να υπολογιστεί η ισχύς του εν λόγω αλγορίθμου.
- Υπάρχει χαμηλή απαίτηση σε μνήμη, που έτσι ο αλγόριθμος καθίσταται κατάλληλος για να χρησιμοποιηθεί σε έξυπνες κάρτες και σε κάθε συσκευή η οποία έχει περιορισμένη μνήμη.
- Υπάρχει βέβαια και ασφάλεια σε υψηλό βαθμό, προσδιορίζοντας τις κατάλληλες παραμέτρους.

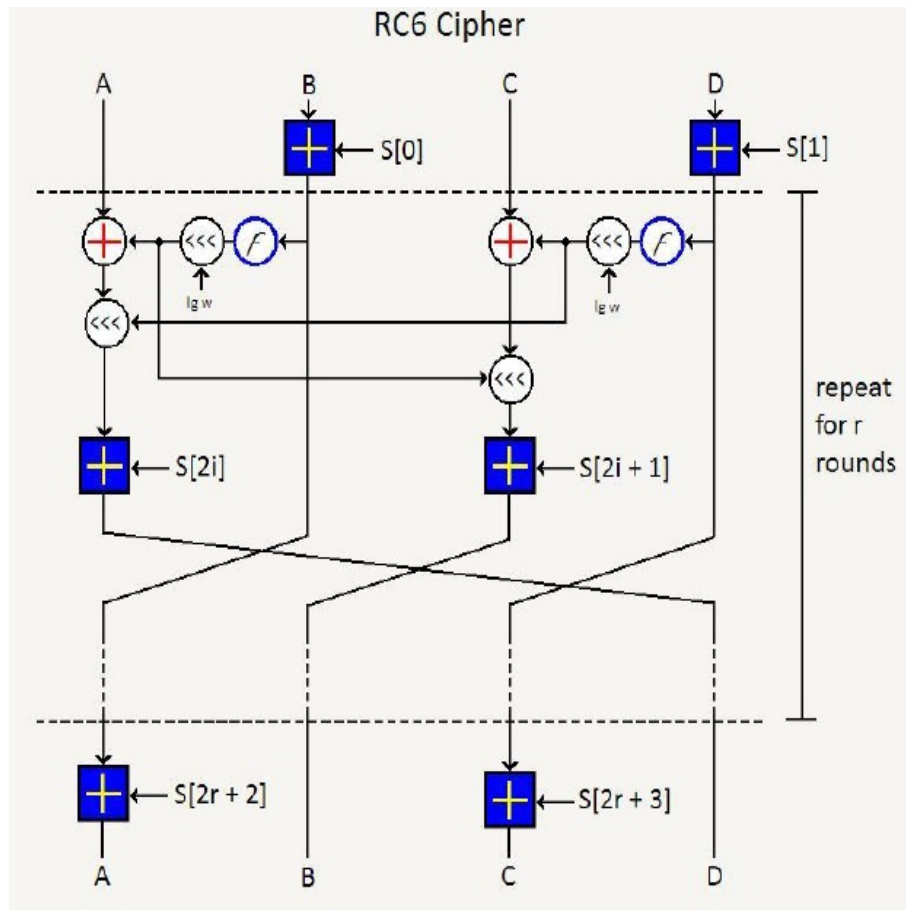
- Τέλος εκτελεί περιστροφές οι οποίες εξαρτώνται από τα δεδομένα. Ο αλγόριθμος RC5 ενσωματώνει τις περιστροφές, κυκλικές δηλαδή μετατοπίσεις σε δυαδικά ψηφία, ο αριθμός των οποίων είναι ένα στοιχείο το οποίο εξαρτάται από τα δεδομένα. Έτσι ο αλγόριθμος βγαίνει ενισχυμένος ώστε να μπορεί να αντιμετωπίζει τις επιθέσεις τρίτων.



Σχήμα 3.7: Αλγόριθμος RC5

3.7.8 RC6

Ο κρυπταλγόριθμος RC6 αναπτύχθηκε και δημοσιεύτηκε το έτος 1998. Περιλαμβάνει 20 κύκλους μετασχηματισμών και σε όλους αυτούς τους κύκλους εκτελείται μεταβλητή περιστροφή των δεδομένων. Οι πράξεις που γίνονται στην εκτέλεση του αλγορίθμου είναι ο πολλαπλασιασμός, η πρόσθεση, η πρόσθεση υποκλειδιών και τέλος η πράξη XOR. Το μέγεθος του τμήματος είναι στα 128bits ενώ το μέγεθος των κλειδιών είναι 128, 192 και 256 bits.

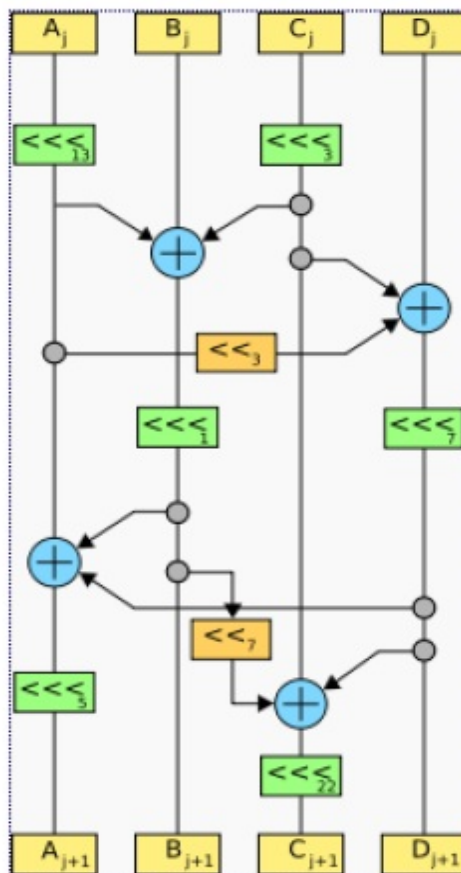


Σχήμα 3.8: Αλγόριθμος RC6

3.7.9 SERPENT

Ο συμμετρικός αλγόριθμος SERPENT περιλαμβάνει 32 κύκλους μετασχηματισμών. Σε αυτόν τον αλγόριθμο προσδιορίζεται μια μετάθεση αρχική και μια μετάθεση τελική. Οι δύο αυτές μεταθέσεις διευκολύνουν τους εναλλακτικούς τρόπους λειτουργίας του αλγορίθμου. Στον κάθε ένα από τους 32 κύκλους μετασχηματισμών, περιλαμβάνονται τρία επιμέρους επίπεδα (μετασχηματισμού) τα οποία είναι:

- η πράξη XOR με το υποκλειδί
- 32 παράλληλες εφαρμογές ενός από τα 8 S-boxes
- και ένας γραμμικός μετασχηματισμός

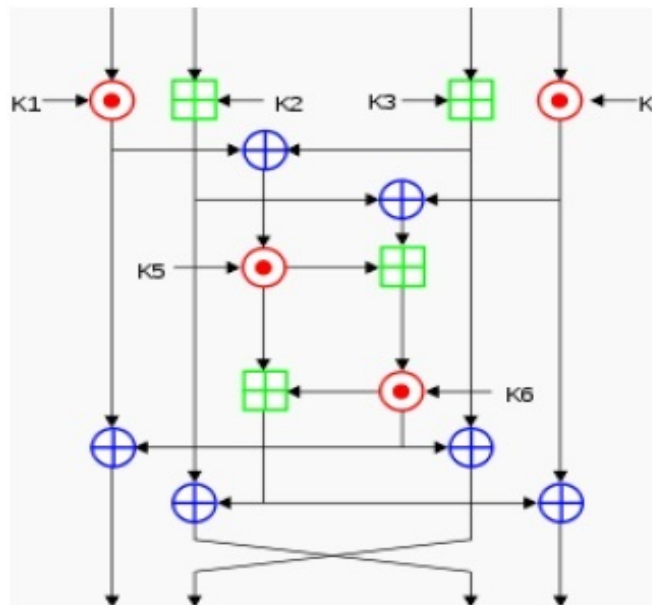


Σχήμα 3.9: Αλγόριθμος SERPENT

3.7.10 International Data Encryption Algorithm (IDEA)

Ο IDEA (International Data Encryption Algorithm) είναι ένας συμμετρικός κρυπταλγόριθμος τμημάτων ο οποίος αναπτύχθηκε το έτος 1991 από τον X Lai και τον J Massey στο Ινστιτούτο Swiss Federal Institute of Technology. Το κλειδί το οποίο χρησιμοποιείται από αυτόν τον αλγόριθμο είναι μήκους 128 bits και η διαφορά του με τον αλγόριθμο DES είναι στην συνάρτηση F καθώς και στην συνάρτηση με την οποία γίνεται η παραγωγή των υποκλειδιών. Για την συνάρτηση F ο IDEA δεν χρησιμοποιεί τα S-boxes, αλλά οι εργασίες στις οποίες βασίζεται είναι τρεις διαφορετικές πράξεις οι

οποίες είναι η δυαδική λογική πράξη XOR η δυαδική πρόσθεση ακεραίων αριθμών των 16 bits και τέλος ο δυαδικός πολλαπλασιασμός μεταξύ ακεραίων των 16 bits. Οι δύο αυτές συναρτήσεις είναι συνδυασμένες με τέτοιον τρόπο που να μπορεί να δημιουργηθεί ένας μετασχηματισμός ο οποίος παρουσιάζει πολυπλοκότητα και που αναλύεται αρκετά δύσκολα. Αυτό έχει σαν αποτέλεσμα το έργο των κρυπταναλυτών να γίνεται αρκετά δύσκολο. Ο αλγόριθμος ο οποίος παράγει δευτερεύοντα κλειδιά στηρίζεται πάνω στην εφαρμογή των κυκλικών μετατοπίσεων, οι οποίες χρησιμοποιούνται με έναν τρόπο που παρουσιάζεται πολύπλοκος. Ο τρόπος αυτός χρησιμοποιείται για την παραγωγή οκτώ (8) κλειδιών, τα οποία είναι δευτερεύοντα, για τον καθένα από τους οκτώ γύρους που εκτελεί ο IDEA. Ο IDEA ήταν ένας από τους αυτούς, που είχαν μέγεθος 128 bits και ήταν προτεινόμενοι να αντικαταστήσουν τον DES. Μετά από διεξοδική έρευνα ο IDEA παρουσιάζει αρκετά καλή αντοχή σε επιθέσεις. Ο IDEA τέλος θεωρείται ένας από τους ασφαλείς αλγορίθμους και τόσο η ανάπτυξή του όσο και η θεωρητική βάση του έχουν δημιουργήσει αρκετές συζητήσεις μεταξύ ερευνητών και μη. Τέλος αυτό που πρέπει να αναφερθεί και είναι αρκετά σημαντικό είναι ότι η σπουδαιότερη χρήση που έχει είναι η εφαρμογή την οποία έχει το πακέτο που προσφέρεται δωρεάν και είναι το πρωτόκολλο Pretty Good Privacy (PGP).



Σχήμα 3.10: Αλγόριθμος IDEA

3.7.11 Towfish

Ο κρυπταλγόριθμος Towfish περιλαμβάνει 16 κύκλους και εκτελούνται τέσσερα S-boxes σε κάθε έναν από αυτούς τους κύκλους. Αυτά τα S-boxes που εφαρμόζονται έχουν άμεση εξάρτηση από το μυστικό κλειδί. Στα αμέσως επόμενα στάδια της διαδικασίας γίνεται η αξιοποίηση των S-boxes τα οποία είναι σταθερά, λαμβάνει χώρα κατόπιν η διενέργεια του μετασχηματισμού Pseudo-Hadamand και τέλος γίνεται η πρόσθεση του υποκλειδιού.

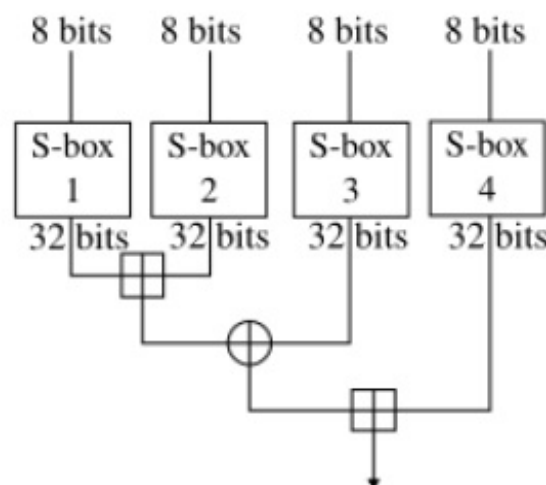
3.7.12 Blowfish

Ο συμμετρικός κρυπταλγόριθμος Blowfish είναι ένας αλγόριθμος ο οποίος αναπτύχθηκε το 1993 από τον B Schneier και καθιερώθηκε σαν μία από τις πιο δημοφιλείς εναλλακτικές λύσης προς

αντικατάσταση του DES. Αυτός ο αλγόριθμος κατασκευάστηκε έτσι ώστε να υπάρχει η εύκολη δυνατότητα υλοποίησής του αφενός και ταχύτερη δυνατότητα εκτέλεσής του αφετέρου. Ένα ενδιαφέρον χαρακτηριστικό του αλγορίθμου είναι το μέγεθος του κλειδιού κρυπτογράφησης, το οποίο μεταβάλλεται και έτσι μπορεί να πάρει τιμές μέχρι 448 bits, αν και στην πράξη τα κλειδιά που χρησιμοποιούνται είναι της τάξεως των 128 bits. Ένα άλλο χαρακτηριστικό του είναι ότι έχει 16 γύρους.

Όπως ο αλγόριθμος DES έτσι και ο Blowfish χρησιμοποιεί S-boxes, την πράξη XOR καθώς και την δυαδική πρόσθεση. Σε αντίθεση όμως με τον DES χρησιμοποιεί S-boxes τα οποία είναι σταθερά και επιπλέον χρησιμοποιεί και S-boxes τα οποία είναι δυναμικά και τα οποία παράγονται σαν μία συνάρτηση του κλειδιού κρυπτογράφησης. Τα υποκλειδιά και τα S-boxes σε αυτόν τον αλγόριθμο, παράγονται μετά από επαναλαμβανόμενη εφαρμογή του ίδιου του Blowfish στο κλειδί. Συνολικά θα απαιτηθεί να γίνουν 521 εκτελέσεις του αλγορίθμου ώστε να μπορέσουν να παραχθούν τα υποκλειδιά και τα S-boxes. Με βάση τα παραπάνω χαρακτηριστικά το συμπέρασμα που εξάγεται είναι ότι ο Blowfish δεν ενδείκνυται για εφαρμογές οι οποίες χρειάζονται συχνή αλλαγή του μυστικού κλειδιού.

Ο Blowfish αποτελεί έναν από τους καλύτερους συμβατικούς αλγορίθμους για κρυπτογράφηση που έχουν χρησιμοποιηθεί και ακόμη τα κλειδιά και τα S-boxes είναι το αποτέλεσμα των πολλαπλών και επανειλημμένων εφαρμογών του ίδιου του Blowfish πάνω στον εαυτό του. Αυτές οι πολλές επαναλήψεις δημιουργούν τροποποίηση εξ' ολοκλήρου στα δυαδικά ψηφία και καθιστούν το έργο της κρυπτανάλυσης αρκετά δύσκολο.



Σχήμα 3.11: Αλγόριθμος BLOWFISH

3.7.13 Safer K-64

Ο Safer K-64 είναι ένας block cipher αλγόριθμος, στον οποίο το αρχικό μήνυμα είναι των 64 bits και περιλαμβάνει κάποια μπλοκ κρυπτογραφήματα. Περιλαμβάνει κάποιους r γύρους που μοιάζουν και οι οποίοι ακολουθούνται από μία έξοδο μετασχηματισμού. Η σύσταση στην αρχή των έξι (6) γύρων ακολουθούνται από κάποια υπόδειξη η οποία θα υιοθετήσει ένα λίγο τροποποιημένο πρόγραμμα για το κλειδί και θα κάνει χρήση οκτώ γύρων με ανώτερους γύρους τους 10. Τα προγράμματα κλειδιών είναι αυτά τα οποία επεκτείνουν το μέγεθος του εξωτερικού κλειδιού από τα 64 bits σε $2r + 1$ υποκλειδιά των 64 bits το κάθε ένα.

Ο αλγόριθμος SAFER αποτελείται καθ' ολοκληρίαν από κάποιες απλές λειτουργίες από byte, εκτός από τις περιστροφές των byte στο πρόγραμμα του κλειδιού. Έτσι το συμπέρασμα είναι ότι ο εν λόγω αλγόριθμος είναι κατάλληλος να χρησιμοποιηθεί για επεξεργαστές οι οποίοι έχουν μικρό μέγεθος λέξεων όπως συμβαίνει στις chipcards. Στον SAFER K-64 χρησιμοποιούνται κάποιες λειτουργίες κατά την κρυπτογράφηση, οι οποίες χρησιμοποιούνται, και οι οποίες διαφέρουν από αυτές της αποκρυπτογράφησης. Στην συνέχεια ο SAFER SK-64 είναι ένας αλγόριθμος ο οποίος χρησιμοποιεί ένα ενισχυμένο πρόγραμμα κλειδιού και είναι ένα πρόγραμμα το οποίο έχει βελτιωθεί στο πρόγραμμα του κλειδιού σε σχέση με αυτό του SAFER, έχει όμως μερικές αλλαγές.

3.7.14 RIJNDAEL

Ο συμμετρικός αλγόριθμος Rijndael έχει υιοθετηθεί σαν AES αλγόριθμος, ο οποίος έχει τα στοιχεία της απλότητας, της ευελιξίας, της αντοχής ως προς όλες τις γνωστές επιθέσεις και τέλος έχει και υψηλή ταχύτητα λειτουργίας. Αυτός ο κρυπταλγόριθμος σχεδιάστηκε από τον Rijndael και μάλιστα δεν ακολουθεί τις κλασικές δομές Feistel. Αυτό όμως που γίνεται είναι ότι ο κάθε κύκλος λειτουργίας του αλγορίθμου, περιλαμβάνει τρεις μετασχηματισμούς, που μοιάζουν μεταξύ τους, αλλά με μια προϋπόθεση, ότι υπάρχει δηλαδή ισοτιμία στην αντιμετώπιση στο κάθε ξεχωριστό bit, τα οποία είναι γνωστά σαν επίπεδα και θα αναφερθούν ακολούθως:

- το επίπεδο γραμμικής ανάμιξης (linear mixing layers), το οποίο πετυχαίνει την διάχυση σε πολλαπλούς κύκλους.
- το μη γραμμικό επίπεδο (non-linear layer) το οποίο αφορά στην παράλληλη εφαρμογή των S-boxes, τα οποία εμφανίζουν πολύ καλές ιδιότητες οι οποίες είναι μη γραμμικές, για την χειρότερη περίπτωση που θα παρουσιαστεί.
- το επίπεδο πρόσθεσης κλειδιού (key addition layer) που αφορά στην συσχέτιση στο ενδιάμεσο αποτέλεσμα το οποίο προκύπτει με το υποκλειδί του κύκλου με την πράξη XOR.

Ο κρυπταλγόριθμος Rijndael περιλαμβάνει τρεις περιπτώσεις για τον αριθμό των κύκλων, οι οποίοι μπορεί να είναι 10, 12 και 14. Ο αριθμός των κύκλων είναι ανάλογος με το μέγεθος του μυστικού κλειδιού. Ο κάθε ένας κύκλος περιλαμβάνει τέσσερις μετασχηματισμούς οι οποίοι είναι:

- Ο Bytesub μετασχηματισμός εφαρμόζεται σε όλα τα bytes του τμήματος
- Ο ShiftRow ο οποίος υποστηρίζει την γραμμική ανάμειξη των δεδομένων του τμήματος
- Ο MixColumn ο οποίος υποστηρίζει την γραμμική ανάμειξη των δεδομένων του τμήματος
- Ο AddKeyRound ο οποίος κάνει έναν συσχετισμό μεταξύ των byte τμήματος του κλειμένου με τα byte των υποκλειδιών με την πράξη XOR. Επιπλέον εκτελείται μία παραπάνω φορά κατά την φάση που γίνεται η αρχικοποίηση πριν από τον πρώτο κύκλο, ενώ στον τελευταίο κύκλο θα παραληφθεί ο μετασχηματισμός Mix Column.

3.7.15 Advanced Encryption Standard (AES)

Εάν η επιλογή του κρυπταλγορίθμου TDES αφορούσε μόνο την ασφάλεια, θα ήταν μια πολύ καλή επιλογή. Έχει όμως ένα βασικό μειονέκτημα που είναι το θέμα της ταχύτητας, είναι αρκετά αργός, σε υλοποιήσεις με την χρήση λογισμικού. Επίσης ο TDES είναι πολύ πιο αργός από τον DES, επειδή οι γύροι του είναι μέχρι τρεις φορές περισσότεροι. Ένα άλλο μειονέκτημα των αλγορίθμων TDES και DES, είναι η προϋπόθεση που απαιτούν να υπάρχει ώστε να χρησιμοποιούν τμήματα που έχουν μέγεθος στα 64 bits, το οποίο απαιτείται για λόγους απόδοσης και ασφάλειας, μέγεθος που πρέπει να είναι μεγαλύτερο. Για τους λόγους αυτούς ο αλγόριθμος TDES δεν είναι δυνατόν να θεωρείται αποτελεσματικός.

Για να υπάρχει η δυνατότητα να αντιμετωπιστούν τα παραπάνω προβλήματα, ήδη από το 1997 το ινστιτούτο NIST προκήρυξε έναν παγκόσμιο διαγωνισμό, ο οποίος ζητούσε να δημιουργηθεί και να παρουσιαστεί ένα νέο προηγμένο πρότυπο κρυπτογράφησης, που θα ήταν ο αντικαταστάτης του DES και το οποίο ήταν ο αλγόριθμος AES, Advanced Encryption Standard και προσδιόρισε ότι αυτός ο καινούργιος αλγόριθμος, θα αποτελεί έναν κρυπταλγόριθμο τμημάτων, ο οποίος θα έχει ένα συμμετρικό σύστημα κρυπτογράφησης με μήκος τμήματος που είναι στα 128 bits και το οποίο υποστηρίζει κλειδιά με μέγεθος 128, 192 και 256 bits.

Τα κριτήρια συγκριτικής αξιολόγησης για τους αλγορίθμους που είναι υποψήφιοι, χωρίστηκαν στις ακόλουθες τρεις κατηγορίες:

- η πρώτη κατηγορία κριτηρίων είναι αυτή η οποία αφορά κατά πρώτον στην ασφάλεια των αλγορίθμων, δηλαδή την αντοχή τους σε διαφόρους τύπους επιθέσεων και κατά δεύτερον σύγκριση της ασφάλειας με την αντίστοιχη άλλων αλγορίθμων. Σε γενικές γραμμές θα πρέπει τα χαρακτηριστικά ασφάλειας των αλγορίθμων, να είναι τουλάχιστον ισοδύναμα με τα χαρακτηριστικά του TDES, αλλά συγχρόνως να έχουν μια αρκετά καλή απόδοση.
- Η δεύτερη κατηγορία αφορά το κόστος. Τα κριτήρια αυτής της κατηγορίας περιλαμβάνουν τις απαιτήσεις που θα πρέπει να έχουν οι χρήστες για μνήμη και υπολογιστική ισχύ του αλγορίθμου καθώς και αυτές που έχουν σχέση με την προστασία δικαιωμάτων, πνευματικής ιδιοκτησίας και διάφορων πατεντών.
- Η τρίτη κατηγορία αφορά την δομή και τα χαρακτηριστικά υλοποίησης. Στην περίπτωση αυτή τα κριτήρια έχουν σχέση με την απλότητα και την ευελιξία, δηλαδή με το πόσο μπορεί ο αλγόριθμος να χειριστεί διάφορα μεγέθη μυστικών κλειδιών και τμημάτων από ένα κρυπτογραφημένο κείμενο, τα οποία μάλιστα μπορεί να είναι και μεγάλα. Σχετίζονται επιπλέον με την δυνατότητα να υλοποιηθεί ο αλγόριθμος σε πολλών ειδών περιβάλλοντα και με την παροχή λειτουργιών οι οποίες είναι συμπληρωματικές.

Με βάση λοιπόν τα παραπάνω κριτήρια υπήρξαν διάφορα στάδια επιλογής για το πιο κατάλληλο πρότυπο. Στο τέλος του πρώτου σταδίου (Αύγουστο του 1998), υπήρχαν 15 υποψήφιοι αλγόριθμοι. Μετά το δεύτερο στάδιο (Μάρτιο του 1999) υπήρξε ανάλυση των αποτελεσμάτων για κάθε υποψηφιότητα και στο τέλος Αυγούστου του 1999 επιλέχθηκαν οι πέντε πιο επικρατέστεροι αλγόριθμοι οι οποίοι ήταν ο MARS, ο Rijndael, ο Serpent, ο RC6 και ο Twofish. Σε επόμενο στάδιο, αφού είχε προηγουμένως γίνει συστηματική ανάλυση και μελέτη των πέντε αυτών αλγορίθμων, τον Απρίλιο του 2000 αφού υπήρξαν διάφορες προτάσεις, κατέληξαν στην επιλογή του Rijndael και στην συνέχεια τον Οκτώβριο του 2000 το NIST ανακοίνωσε επίσημα ότι ο συγκεκριμένος αλγόριθμος επιλέχθηκε σαν το πρότυπο AES. Η τελική προτυποποίηση του αλγορίθμου έγινε τον Νοέμβριο του 2001 όταν και αντικατέστησε τον DES, σαν τον περισσότερο ασφαλή αλγόριθμο κρυπτογράφησης.

Ο αλγόριθμος AES λειτουργεί σε πολλές παραλλαγές, οι οποίες εξαρτώνται από το μέγεθος του κλειδιού το οποίο χρησιμοποιεί. Έτσι υπάρχουν τρεις παραλλαγές που είναι ο AES-128, ο AES-192 και ο AES-256, αν το κλειδί είναι 128, 192 και 256 bits αντίστοιχα.

Η όλη διαδικασία της λειτουργίας του αλγορίθμου AES είναι η ακόλουθη. Στην υλοποίησή του θα εκτελούνται, σε ένα αρχικό κείμενο των 128 bits, οι διάφοροι κύκλοι επαναλήψεων, ανάλογα με το μήκος του κλειδιού. Εισάγεται στην αρχή ένα τμήμα του αρχικού κειμένου ταυτόχρονα με το αρχικό κλειδί κρυπτογράφησης και ακολούθως στον κάθε κύκλο επανάληψης προκύπτει η είσοδος και το νέο κλειδί του συγκεκριμένου κύκλου, από εκείνο το τμήμα του κειμένου του κύκλου που έγινε προηγουμένως. Η έξοδος είναι ένα κρυπτοκείμενο με μέγεθος 128 bits, όσο είναι δηλαδή και το μέγεθος του αρχικού κειμένου.

Όλες οι διεργασίες λειτουργίας του AES γίνονται σε κάποια ενδιάμεσα σημεία που ονομάζονται καταστάσεις (States). Η αναπαράσταση αυτών των καταστάσεων γίνεται με έναν πίνακα που έχει δύο διαστάσεις. Ο πίνακας αυτός έχει τέσσερες γραμμές και τόσες στήλες ώστε να είναι ανάλογες με το μέγεθος του αρχικού κειμένου. Η κάθε κατάσταση κάνει χρήση μιας μεταβλητής s καθώς και δύο δεικτών ώστε να μπορεί να γίνει η αναπαράστασή της στον πίνακα. Το αρχικό κείμενο το ονομάζουμε N_b και οι τιμές που μπορεί να πάρει είναι 4, 6 και 8, όταν είναι για τμήμα κειμένου των 32 bits, με δεδομένο βέβαια ότι το μέγεθος του αρχικού κειμένου μπορεί να είναι 128, 192 και 256 bits. Κατ' αντιστοιχία ορίζεται και μια επιπλέον παράμετρος, η N_k , που χρειάζεται για να δηλώνει το μέγεθος των κλειδιών σε τμήματα των 32 bits. Επειδή στον AES τα μεγέθη των κλειδιών είναι 128, 192 και 256 bits, ανάλογα και η παράμετρος N_k θα μπορεί να παίρνει τιμές 4, 6 και 8 αντιστοίχως για τη κάθε περίπτωση. Ο συμβολισμός για τον αριθμό των επαναληπτικών γύρων του αλγορίθμου είναι N_r και ο οποίος υπόκειται σε μεταβολή ανάλογα με το μέγεθος του κλειδιού και οι τιμές που μπορεί να πάρει είναι 10, 12 και 14 και οι οποίες τιμές καθορίζονται αυστηρά από το πρότυπο AES.

Στην αρχή το τμήμα του κειμένου που δεν έχει κρυπτογραφηθεί, αναπαρίσταται στον πίνακα των καταστάσεων (δηλαδή των state). Στην συνέχεια προστίθεται το κλειδί του κύκλου ο οποίος εξήχθη από μια διαδικασία που ακολουθήθηκε για την επέκταση κλειδιού. Στην συνέχεια μετά από τους διάφορους επαναληπτικούς κύκλους εξάγεται η τελική μορφή που θα έχει η κατάσταση state την οποία παρέχει το κρυπτογραφημένο κείμενο. Όταν λειτουργεί ο αλγόριθμος πραγματοποιούνται τέσσερις διαφορετικές διαδικασίες. Η διαδικασία Shift Rows κατά την οποία εκτελείται ολίσθηση των διαφόρων bytes τα οποία ευρίσκονται στον πίνακα των state. Η διαδικασία Sub Bytes με την οποία γίνεται αντικατάσταση των bytes με βάσει κάποιον πίνακα αντικατάστασης. Επίσης η διαδικασία Mix Columns με την οποία πραγματοποιείται η ανάμιξη των bytes και τελευταία η διαδικασία Add Round Key με την οποία εκτελείται η πρόσθεση ενός κλειδιού στον πίνακα των state. Για την διαδικασία της αποκρυπτογράφησης μπορούν να χρησιμοποιηθούν οι ίδιοι μετασχηματισμοί, με ακριβώς αντιστροφή στην σειρά των μετασχηματισμών.

Αντοχή του AES σε Γραμμική και Διαφορική Κρυπτανάλυση

Η διαφορική και η γραμμική κρυπτανάλυση είναι δύο μέθοδοι, που χρησιμοποιούνται σε μεγάλη έκταση, για να πραγματοποιηθούν επιθέσεις σε κρυπταλγόριθμους τμημάτων. Είναι μέθοδοι οι οποίες ανήκουν στην κατηγορία των επιθέσεων με επιλεγμένο το αρχικό κείμενο.

Κατά πρώτον η γραμμική κρυπτανάλυση είναι μια μέθοδος, η οποία υπήρξε επινοήση του Mitsuru Matsui και παρουσιάστηκε το 1992. Εφαρμόζεται κυρίως σε κρυπταλγόριθμους γινομένου και προσπαθεί να βρει γραμμικές προσεγγίσεις στη σχέση μεταξύ ενός μέρους ή του συνόλου από τα bits του αρχικού κειμένου, του κλειδιού καθώς και του κρυπτοκειμένου. Οι γραμμικές σχέσεις που προκύπτουν ισχύουν με κάποια πιθανότητα $P \in [0, 1]$. Ορίζεται ακόμα, σαν πόλωση, η ποσότητα $\epsilon = P - \frac{1}{2}$.

- εάν $\epsilon = 0 \Leftrightarrow P = \frac{1}{2}$, τότε η γραμμική κρυπτανάλυση είναι ανώφελη.
- εάν υπάρχουν γραμμικές προσεγγίσεις με $\epsilon \neq 0$, τότε ένα κρυπτοσύστημα είναι ευάλωτο στην γραμμική κρυπτανάλυση. Όσο πιο πολλές γραμμικές προσεγγίσεις προκύψουν και όσο μεγαλύτερη είναι σε αυτές η ποσότητα $|\epsilon|$, τόσο πιο ευάλωτο θεωρείται ότι είναι το κρυπτοσύστημα.

Στην συμμετρική κρυπτογραφία, ο μόνος μετασχηματισμός που δεν είναι γραμμικός, είναι τα S-Boxes και για τον λόγο αυτό στόχος της γραμμικής κρυπτανάλυσης είναι να γίνει ακριβέστερη η γραμμικοποίησή τους. Άρα η ανθεκτικότητα ενός κρυπταλγορίθμου, σε επιθέσεις αυτού του είδους, εξαρτάται από την δομή των S-Boxes. Ακόμη καλό είναι να αναφερθεί πως μεγαλύτερη πιθανότητα να βρεθούν γραμμικές σχέσεις, που να είναι αποτελεσματικές, υπάρχει για τα κλειδιά ιδιαίτερα του τελευταίου γύρου.

Η διαφορική κρυπτανάλυση είναι μια μέθοδος που δημιουργήθηκε από τον Eli Biham και τον Adi Shamir στο τέλος του έτους 1980. Η μέθοδος αυτή έχει πολλές ομοιότητες με την μέθοδο της γραμμικής κρυπτανάλυσης. Η διαφορά τους είναι ότι αντί να δημιουργεί γραμμικές σχέσεις, εξετάζει την συχνότητα με τη οποία εμφανίζεται διαφορά, αν υπάρχει, μεταξύ δύο κρυπτοκειμένων, σε σχέση με μια δεδομένη διαφορά δύο αρχικών κειμένων. Η διαφορά Δx δύο κρυπτοκειμένων ή δύο αρχικών κειμένων x και x' , ορίζεται από μια συνάρτηση διαφοράς $h(x, x')$, που είναι σχεδόν πάντα η πράξη XOR, συνήθως δηλαδή $\Delta x = x \oplus x'$.

Ένα κρυπτοσύστημα με μήκος τμήματος l_b θα έχει 2^{l_b} πιθανές τιμές κρυπτοκειμένου, επομένως και ισάριθμες πιθανές τιμές διαφορών κρυπτοκειμένου (έξοδος).

Αν η πιθανότητα εμφάνισης μιας εξόδου είναι 2^{-l_b} , για κάθε έξοδο, τότε η διαφορική κρυπτανάλυση δεν μπορεί να έχει αποτέλεσμα στο συγκεκριμένο κρυπτοσύστημα. Ένα κρυπτοσύστημα θα είναι ευάλωτο στην διαφορική κρυπτανάλυση, όταν οι διαφορές του κρυπτοκειμένου δεν ακολουθούν ομοιόμορφη κατανομή, αλλά υπάρχουν τιμές με μηδενική πιθανότητα εμφάνισης και κάποιες άλλες με πολλαπλάσια πιθανότητα του 2^{-l_b} . Όσο πιο κοντά είναι η κατανομή των διαφορών στην ομοιόμορφη, τόσο πιο ασφαλές είναι το κρυπτοσύστημα σε τέτοιου είδους επιθέσεις.

Για τον AES έχει αποδειχθεί ότι ακόμη και εάν παραλλαχθεί π.χ. σε τέσσερις γύρους, παραμένει να είναι ασφαλής, στις δύο επιθέσεις που αναλύθηκαν πιο πριν. Έτσι η δομή του AES δεν έχει σημεία τα οποία να είναι τρωτά και τα οποία να δίνουν στις δύο μεθόδους την ευκαιρία να τα εκμεταλλευτούν.

Αντοχή του AES σε άλλα είδη επιθέσεων

Έχουν γίνει δοκιμές της αντοχής του AES σε άλλα είδη επιθέσεων, οι οποίες ήταν ή πιο σύγχρονες ή πιο προσανατολισμένες γι' αυτόν τον αλγόριθμο. Τέτοιες επιθέσεις είναι:

- επίθεση κόλουργων διαφορικών (truncated differentials attack)
- επίθεση κορεσμού (saturation attack)
- επίθεση Gilbert-Minier
- επιθέσεις παρεμβολής (interpolation attack)
- αναζήτηση αδύναμων κλειδιών, σαν αυτά των κρυπταλγορίθμων DES και IDEA
- επιθέσεις σχετιζομένων κλειδιών (related key attacks)

Σε όλα αυτά τα είδη των επιθέσεων που αναφέρθηκαν αμέσως προηγούμενα, ο AES είναι σίγουρα απόλυτα ασφαλής. Το μόνο τρωτό του σημείο είναι η μέθοδος κρυπτανάλυσης XSL συνδυασμένη με το μοντέλο BES. Η μέθοδος αυτή παρουσιάστηκε από τους Nicolas Courtois και Josef Pieprzyk, η οποία τελικά όμως δεν ήταν εφαρμόσιμη. Το έτος 2003 οι Sean Murphy και Matthew Robshaw παρουσίασαν μια άλλη μαθηματική προσέγγιση για τον AES, ο οποίος ήταν ο κρυπταλγόριθμος BES που επιτρέπει να απλοποιηθεί η μαθηματική περιγραφή για τον AES. Υπάρχει πιθανότητα η μέθοδος XSL να έχει αρκετά καλά αποτελέσματα στην περίπτωση που εφαρμοστεί στον BES, όμως δεν έχει αποδειχθεί κάτι τέτοιο.

Αλγόριθμος	Μήκος Κλειδιού	Αριθμός κύκλων	Μαθηματικές Πράξεις	Εφαρμογές
DES	56 bits	16	XOR, σταθερά S-boxes	SET, Kerberos
Triple DES	112 ή 168	48	XOR, σταθερά S-boxes	Financial key management, PGP, S/MIME
IDEA	128	8	XOR, πρόσθεση, πολλαπλασιασμός	PGP
Blowfish	Μεταβλητό μέχρι 448 bits	16	XOR, μεταβλητά S-boxes, πρόσθεση	
RC5	Μεταβλητό μέχρι 2048 bits	Μεταβλητό μέχρι 255	πρόσθεση, αφαίρεση, XOR, περιστροφή	
CAST-128	40 μέχρι 128 bits	16	πρόσθεση, αφαίρεση, XOR, περιστροφή, σταθερά S-boxes	PGP

Σχήμα 3.12: Συμμετρικοί Αλγόριθμοι Κρυπτογράφησης

3.7.16 Κουτιά Αντικατάστασης (S-boxes)

Τα S-boxes είναι στις πιο πολλές των περιπτώσεων, το στάδιο ενός αλγορίθμου το οποίο δεν είναι γραμμικό. Στην διάρκεια που κάποιος αλγόριθμος λειτουργεί, το S-box κάνει αντιστοίχιση μιας ακολουθίας από m bits η οποία λαμβάνει στην είσοδο, με μια άλλη ακολουθία από n bits που αποτελεί το αποτέλεσμα στην έξοδο. Η αναπαράσταση των S-boxes γίνεται, τις πιο πολλές φορές, με ένα πίνακα και για την υλοποίησή τους, χρησιμοποιείται ένας άλλος πίνακας, όπου για τις περιπτώσεις μικρών μεγεθών S-box, ο πίνακας έχει μια διάσταση, με δείκτη την είσοδο και περιεχόμενο την έξοδο. Τα S-boxes προσθέτουν την γνωστή ιδιότητα της σύγχυσης, σε αλγορίθμους οι οποίοι τα χρησιμοποιούν. Κατά την διάρκεια που τα S-boxes λειτουργούν δημιουργούν κάποιες διαφορές, που υπάρχουν μεταξύ του αρχικού μηνύματος και του παραγόμενου κρυπτογραφήματος, οι οποίες είναι αόριστες και δύσκολα ανιχνεύσιμες.

Οι συναρτήσεις αντικατάστασης θα πρέπει να είναι αντιστρέψιμες, για να μπορούν να εκτελούν αποκωδικοποίηση του μηνύματος το οποίο είναι κρυπτογραφημένο, αυτό όμως δημιουργεί ένα πρόβλημα, το οποίο είναι ότι όλο το αλγοριθμικό σύστημα καθίσταται μη ασφαλές. Για να μπορέσουμε να έχουμε ασφάλεια θα πρέπει οι συναρτήσεις αντικατάστασης να ενισχυθούν με την ιδιότητα της διάχυσης καθώς και με την ανάμιξη των κλειδιών, στα στάδια της εφαρμογής τους. Η δε ενίσχυση των κρυπταλγορίθμων με την ιδιότητα της σύγχυσης, προσφέρει σε αυτούς μεγάλη βοήθεια στο να αντιστέκονται σε γραμμικές ή διαφορικές επιθέσεις.

Ο πιο απλή μορφή ενός S-box δέχεται μια ακολουθία από bits στην είσοδό του και κατόπιν με την βοήθεια ενός πίνακα lookup table καθορίζει την ακολουθία bits στην έξοδό του. Όταν γίνεται αποκρυπτογράφηση αυτός ο πίνακας αντιστρέφεται. Η κατασκευή όπως και ο σχεδιασμός των S-boxes είναι μια διαδικασία η οποία περιέχει κάποιον βαθμό δυσκολίας και μάλιστα απαιτεί να υπάρχει μια βαθιά γνώση καθώς και συνεχής μελέτη των διάφορων σύγχρονων μεθόδων για κρυπτογράφηση. Η χρήση κάποιων συγκεκριμένων patterns στην είσοδο του S-box θα παράγει patterns στην έξοδο με μια πιθανότητα η οποία είναι ισοδύναμη με μια τυχαία συνάρτηση.

Οι παράμετροι οι οποίες κάνουν ένα S-box ασφαλές και αφορούν την κρυπτογραφία, είναι το μέγεθός του καθώς και ο τρόπος με τον οποίο συμπληρώνεται το περιεχόμενο του πίνακά του. Μια τεχνική σχεδίαση ενός S-box για να είναι ορθολογική και αποδεκτή, θα πρέπει να απαιτεί να τηθούν βασικά κριτήρια, τα οποία είναι:

- **μη γραμμικότητα (non-Linearity)**, είναι βασικό κριτήριο γιατί, αφού το S-box είναι γραμμικό, μπορεί εύκολα να γίνει ο αδύνατος κρίκος σε μια ενδεχόμενη επίθεση κρυπτανάλυσης.
- **αμφίεση (Bijection)**, είναι απαραίτητο για τον μονοσήμαντο ορισμό της διαδικασίας της αποκρυπτογράφησης.
- **αυστηρής χιονοστιβάδας (strict avalanche)**, είναι το κριτήριο που θα πρέπει να ικανοποιεί ένα S-box για κάθε S-bit της εισόδου του, η αντιστροφή του προκαλεί και την αντιστροφή σε κάθε S-bit της εξόδου η οποία είναι ίση με $\frac{1}{2}$. Αυτό το κριτήριο το εισήγαγαν οι Webster και Tavares αφού χρησιμοποίησαν την διάχυση και την σύγχυση του Shannon.
- **ανεξαρτησία εξόδου (Output independence)**, αυτό το κριτήριο ικανοποιείται στην περίπτωση που δεν είναι φανερές οι συσχετίσεις στις ακολουθίες των S-bits εισόδου και εξόδου.

Γίνεται λοιπόν κατανοητό ότι η ασφάλεια των συμμετρικών αλγορίθμων εξαρτάται από τις ιδιότητες που έχουν τα S-boxes, έτσι ώστε να μπορούν να είναι ανθεκτικά σε επιθέσεις.

Ένα ιδεατό S-box, θεωρητικά θα πρέπει να πληροί τις ακόλουθες ιδιότητες:

- κάθε γραμμικός συνδυασμός των στηλών του S-box να είναι Bent.
- κάθε είσοδος του πίνακα XOR να είναι ίση με 0 ή 2.
- το S-box να ικανοποιεί το κριτήριο maximum order strick avalanche.
- το S-box να ικανοποιεί το κριτήριο maximum order bit independence.
- τα βάρη κάθε γραμμής του πίνακα M να είναι μια δυναμική κατανομή με μέσο $\frac{n}{2}$.
- τα βάρη κάθε ζεύγους γραμμών του πίνακα M να έχουν μια δυναμική κατανομή με μέσο $\frac{n}{2}$.
- τα βάρη κάθε στήλης να είναι βάρους Hamming 2^{n-1} .

Τα S-boxes που ικανοποιούν την πρώτη ιδιότητα αποδεικνύονται πιο ασφαλή και ανθεκτικά σε επιθέσεις γραμμικής κρυπτανάλυσης. Επίσης τα S-boxes που ικανοποιούν την δεύτερη ιδιότητα πετυχαίνουν καλύτερη ασφάλεια σε περιπτώσεις διαφορικής κρυπτανάλυσης. Ακόμη τα S-boxes που ικανοποιούν την πρώτη, την πέμπτη και την έβδομη ιδιότητα εξασφαλίζουν την ύπαρξη καλών δυναμικών χαρακτηριστικών. Τέλος τα S-boxes που ικανοποιούν την δεύτερη, την τρίτη και την τέταρτη ιδιότητα εξασφαλίζουν την ύπαρξη καλών και δυναμικών χαρακτηριστικών. Για να αυξηθεί λοιπόν η ασφάλεια των αλγορίθμων κρυπτογράφησης θα πρέπει τα S-boxes να είναι έτσι κατασκευασμένα ώστε να πληρούν όσες γίνεται περισσότερες από τις ιδιότητες που αναφέρθηκαν προηγουμένως, επιπλέον θα πρέπει να έχουν όσο γίνεται πιο μικρό χρόνο στην κατασκευή τους και τέλος να παρουσιάζουν ανθεκτικότητα σε πιθανές κρυπταναλυτικές επιθέσεις του κάθε είδους.

Κεφάλαιο 4

Αλγόριθμοι Δημόσιου ή Ασύμμετρου Κλειδιού

Το μεγαλύτερο πρόβλημα διαχρονικά, για τα περισσότερα κρυπτοσυστήματα ήταν η αδυναμία τους στην διανομή των κλειδιών. Αν κάποιος επιτιθέμενος σε ένα κρυπτοσύστημα, όσο και ισχυρό αν είναι, είχε την δυνατότητα να υποκλέψει το κλειδί της κρυπτογράφησης και το κλειδί της αποκρυπτογράφησης, τότε το σύστημα αυτό θα καταστεί άχρηστο. Βασική αρχή της κρυπτογραφίας είναι ότι τα κλειδιά θα πρέπει να είναι ταυτόσημα ή από το ένα να προκύπτει το άλλο με εύκολο τρόπο. Ακόμη το κλειδί, θα πρέπει να διαμοιραστεί σε όλους τους χρήστες του συστήματος αφενός, και να προστατευθεί αφετέρου.

Οι Diffie και Hellman, του Πανεπιστημίου του Στάνφορντ, το έτος 1976, μετά από έρευνες κατέληξαν σε ένα διαφορετικό από τα μέχρι τότε γνωστά κρυπτοσυστήματα, στο οποίο το κλειδί με το οποίο γίνεται η κρυπτογράφηση ήταν διαφορετικό από το κλειδί της αποκρυπτογράφησης και δεν μπορούσε το ένα να προκύπτει από το άλλο. Σύμφωνα με την πρόταση αυτών των δύο ερευνητών, οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης με τα κλειδιά τους E και D αντίστοιχα, θα πρέπει να ικανοποιούν τις τρεις απαιτήσεις που ακολουθούν:

- $D(E(P)) = P$
- Είναι εξαιρετικά δύσκολα να προκύψει το D από το E .
- Ο E δεν μπορεί να σπάσει με μια επίθεση επιλεγμένου αρχικού κειμένου

Πιο απλά, η πρώτη απαίτηση λέει ότι αν εφαρμόσουμε τον αλγόριθμο κρυπτογράφησης D σε ένα κρυπτογραφημένο κείμενο $E(P)$ θα παράγουμε το αρχικό καθαρό κείμενο P . Χωρίς αυτή την ιδιότητα, ο νόμιμος παραλήπτης δε θα μπορούσε να αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο. Η δεύτερη απαίτηση είναι αυτονόητη. Η τρίτη απαίτηση κρίνεται απαραίτητη γιατί οι εισβολείς έχουν τη δυνατότητα να πειραματιστούν με τον αλγόριθμο όσο επιθυμούν. Επομένως, αν ισχύουν αυτές οι τρεις συνθήκες τότε ο αλγόριθμος κρυπτογράφησης και το κλειδί μπορούν να δημοσιευτούν, απ' όπου προέρχεται και το όνομα κρυπτογραφία δημόσιου κλειδιού (public key cryptography). Η κρυπτογραφία δημόσιου κλειδιού χρησιμοποιείται κυρίως για αυθεντικοποίηση μηνυμάτων και διανομή μυστικών κλειδιών.

4.1 Δομή Κρυπτοσυστημάτων Δημοσίου Κλειδιού

Οι αλγόριθμοι κρυπτογράφησης δημόσιου κλειδιού, έχουν την βάση τους σε μαθηματικές συναρτήσεις και όχι σε πράξεις απλές με bits. Αυτός ο τύπος κρυπτογράφησης είναι ασύμμετρος και

χρησιμοποιεί ένα ζευγάρι κλειδιών, σε αντίθεση με την συμμετρική κρυπτογράφηση η οποία χρησιμοποιεί μόνο ένα κλειδί. Το πλεονέκτημα λοιπόν της ασύμμετρης κρυπτογραφίας είναι ότι με κάποιες σημαντικές αλλαγές, εξασφαλίζεται όσο γίνεται καλύτερα και σε μεγαλύτερο βαθμό, η εμπιστευτικότητα, η αυθεντικότητα καθώς και η διανομή των κλειδιών.

Αρχικά, είναι απαραίτητο να γίνει αναφορά σε κάποιες λανθασμένες αντιλήψεις σχετικά με την κρυπτογράφηση δημόσιου κλειδιού. Η πρώτη αφορά την εντύπωση ότι η ασύμμετρη είναι πιο ανθεκτική σε επιθέσεις τρίτων, σε σχέση με την συμμετρική κρυπτογράφηση. Η πραγματικότητα όμως σε αυτό το θέμα είναι ότι η ανθεκτικότητα στις επιθέσεις εξαρτάται από το μήκος του κλειδιού κρυπτογράφησης και την υπολογιστική ισχύ που χρειάζεται κάποιος κρυπταναλυτής, για να μπορέσει να παραβιάσει καθώς και να αποκρυπτογραφήσει ένα μήνυμα. Η δεύτερη λανθασμένη αντίληψη έχει σχέση με το ότι η ασύμμετρη κρυπτογραφία επικρατεί έναντι της συμμετρικής. Όμως το γεγονός είναι ότι γίνεται χρήση και των δύο κρυπτοσυστημάτων και δεν υπάρχει πρόβλεψη να εγκαταλειφθεί η συμμετρική κρυπτογράφηση, για τον λόγο ότι θα χρειάζεται αρκετά μεγάλος χρόνος, ώστε να εκτελεστούν εργασίες σε ένα περιβάλλον ασύμμετρου κρυπτοσυστήματος. Μια τρίτη λανθασμένη εντύπωση είναι ότι η διανομή των κλειδιών κρυπτογράφησης, είναι πιο εύκολη στην ασύμμετρη από ότι στην συμμετρική. Πρακτικά στην κρυπτογραφία δημόσιου κλειδιού, είναι απαραίτητο να εκτελεστούν πρωτόκολλα και διαδικασίες οι οποίες σε καμία περίπτωση δεν είναι πιο απλές ή ακόμη και πιο αποδοτικές από αυτές που χρειάζονται στην συμμετρική κρυπτογράφηση.

4.2 Μέθοδος Λειτουργίας

Όπως δείχνει και το όνομά της η κρυπτογραφία δημόσιου κλειδιού, έχει σαν σκοπό την χρήση αυτού του κλειδιού από όλους, σε αντίθεση με το ιδιωτικό κλειδί, το οποίο είναι για χρήση μόνο από τον κάτοχό του. Έτσι ένα κλειδί δημόσιο χρησιμοποιείται για την κρυπτογράφηση και ένα άλλο ιδιωτικό κλειδί (το οποίο είναι και μοναδικό) για την αποκρυπτογράφηση, τα οποία κλειδιά είναι διαφορετικά μεταξύ τους.

Παρακάτω περιγράφονται τα βήματα που ακολουθούνται:

- Κάθε χρήστης παράγει ένα ζεύγος κλειδιών που θα χρησιμοποιηθούν κατά τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης των μηνυμάτων.
- Κάθε χρήστης τοποθετεί το δημόσιο κλειδί σε μια βάση δεδομένων ενός φορέα. Το ιδιωτικό κλειδί, διαφυλάσσεται διατηρώντας τη μυστικότητα. Για επίτευξη στοιχειώδους λειτουργικότητας, είναι απαραίτητο κάθε χρήστης να μπορεί να ανακτήσει εύκολα τα δημόσια κλειδιά των άλλων.
- Έστω ότι ο νόμιμος αποστολέας επιθυμεί να αποστείλει ένα μήνυμα στον νόμιμο παραλήπτη και αποτελεί τεθείσα απαίτηση η διασφάλιση της εμπιστευτικότητας του μηνύματος, τότε ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη.
- Ο παραλήπτης λαμβάνει το μήνυμα και το αποκρυπτογραφεί με το ιδιωτικό του κλειδί. Το μήνυμα αυτό δε μπορεί να αποκρυπτογραφηθεί από κανέναν άλλο, καθώς μόνο ο παραλήπτης γνωρίζει το ιδιωτικό του κλειδί το οποίο είναι μοναδικά συσχετιζόμενο με το αντίστοιχο δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση.

Αναλυτικότερα: Έστω ο παραλήπτης, ένα άτομο που επιθυμεί να λάβει ένα μυστικό μήνυμα, επινοεί αρχικά δύο αλγόριθμους οι οποίοι ικανοποιούν τις παραπάνω απαιτήσεις. Ο αλγόριθμος κρυπτογράφησης και το κλειδί του παραλήπτη δημοσιεύονται. Προκειμένου να δηλώσουμε τον αλγόριθμο κρυπτογράφησης με παράμετρο το δημόσιο κλειδί του παραλήπτη θα χρησιμοποιήσουμε

τη σημειογραφία E_{Π} . Όμοια, ο αλγόριθμος αποκρυπτογράφησης με παράμετρο το ιδιωτικό κλειδί του παραλήπτη συμβολίζεται με D_{Π} . Ο αποστολέας κάνει το ίδιο πράγμα, δημοσιεύοντας το E_A αλλά κρατώντας μυστικό το D_A .

Έστω ότι ο παραλήπτης και ο αποστολέας δεν είχαν καμία επικοινωνία στο παρελθόν, η εγκαθίδρυση ενός ασφαλούς καναλιού ανάμεσά τους πραγματοποιείται ως εξής: Θεωρούμε ότι το κλειδί κρυπτογράφησης του παραλήπτη E_{Π} αλλά και του αποστολέα E_A είναι τοποθετημένα σε αρχεία αναγνώσιμα από όλους. Ο παραλήπτης λαμβάνει το πρώτο μήνυμα P , υπολογίζει το $E_A(P)$, και το στέλνει στον αποστολέα, ο οποίος το αποκρυπτογραφεί χρησιμοποιώντας το μυστικό κλειδί του D_A , δηλαδή υπολογίζει $D_A(E_A(P)) = P$. Κανείς άλλος δε είναι σε θέση να διαβάσει το κρυπτοκείμενο $E_A(P)$, διότι υποθέσαμε ότι το κρυπτογραφικό σύστημα είναι αρκετά ισχυρό και άρα είναι δύσκολο να υπολογιστεί το D_A από το δημόσια γνωστό E_A . Για να μπορέσει να στείλει απάντηση R , ο αποστολέας μεταδίδει το $E_{\Pi}(R)$. Τώρα ο παραλήπτης και ο αποστολέας μπορούν να επικοινωνήσουν με ασφάλεια.

Προϋπόθεση αυτής της προσέγγισης είναι τα δημόσια κλειδιά να είναι προσβάσιμα σε όλους τους συμμετέχοντες, ενώ τα ιδιωτικά να παράγονται τοπικά για τον κάθε συμμετέχοντα προκειμένου να εξασφαλίζεται η μυστικότητά τους. Ένας χρήστης έχει τη δυνατότητα να αλλάξει το ιδιωτικό του κλειδί ανά πάσα στιγμή και ταυτόχρονα να γνωστοποιήσει το αντίστοιχο νέο δημόσιο κλειδί, ώστε να αντικατασταθεί το προηγούμενο, μη πλέον ισχύον δημόσιο κλειδί.

Το κλειδί που χρησιμοποιείται στη συμμετρική κρυπτογράφηση αναφέρεται ως μυστικό κλειδί (secret). Το ζεύγος κλειδιών (key pair) που χρησιμοποιείται στην ασύμμετρη κρυπτογράφηση περιέχει το δημόσιο κλειδί (public key) και το ιδιωτικό κλειδί (private key), το οποίο παραμένει μυστικό αλλά προκειμένου να αποφευχθεί εννοιολογική σύγχυση με τη συμμετρική κρυπτογράφηση, αναφέρεται ως ιδιωτικό κι όχι μυστικό κλειδί.

4.3 Ο Αλγόριθμος RSA

Το 1977, λίγο μετά την παρουσίαση της ιδέας του συστήματος με δημόσιο κλειδί, αναπτύχθηκε στο MIT ένα από τα πρώτα ασύμμετρα κρυπτογραφικά συστήματα από τους μαθηματικούς R. Rivest, A. Shamir και L. Aleman, το οποίο δημοσιεύτηκε για πρώτη φορά το 1978. Από εκείνη τη στιγμή ο RSA επικράτησε ως ο πλέον αποδεκτός και προσεγγιστικά εύκολα υλοποιήσιμος αλγόριθμος για ασύμμετρα κρυπτοσυστήματα. Στον αλγόριθμο του RSA το αρχικό κείμενο και το κρυπτοκείμενο είναι ακέραιοι αριθμοί με τιμές μεταξύ 0 και $n - 1$, για κάποιο n .

Η κρυπτογράφηση για ένα κείμενο M και αποκρυπτογράφηση για ένα κρυπτοκείμενο C συμβολίζεται ως εξής:

$$C = M^e \bmod n$$

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

Οι τιμές των n και e θα πρέπει να είναι γνωστοποιημένες τόσο στον αποστολέα όσο και στον παραλήπτη. Την τιμή d αντιθέτως, πρέπει να τη γνωρίζει μόνο ο παραλήπτης. Στην ουσία ο RSA είναι ένας αλγόριθμος ασύμμετρου κρυπτοσυστήματος με δημόσιο κλειδί $KU = \{e, n\}$ και ιδιωτικό κλειδί $KR = \{d, n\}$. Παρακάτω παρατίθενται οι απαιτήσεις που πρέπει να πληρεί ο αλγόριθμος αυτός ώστε να καθίσταται ικανοποιητικός:

- Επιλογή δύο μεγάλων πρώτων αριθμών, p και q (συνήθως των 1024)
- Υπολογισμός των $n = p \times q$ και $\phi(n) = (p - 1)(q - 1)$
- Επιλογή ενός αριθμού που είναι αμοιβαία πρώτος με το $\phi(n)$, τον οποίο ονομάζουμε d

- Εντοπισμός του e και $e \times d = 1 \bmod \phi(n)$

Το δημόσιο κλειδί αποτελείται από το ζευγάρι (e, n) και το ιδιωτικό κλειδί από το ζευγάρι (d, n) . Έχοντας υπολογίσει τις παραπάνω παραμέτρους ξεκινά η κρυπτογράφηση κειμένου M με τα ακόλουθα βήματα:

- το κείμενο που θα κρυπτογραφηθεί και θεωρείται σαν συρμός bit, διαιρείται σε μπλοκ, έτσι ώστε κάθε μήνυμα κειμένου M , να πέφτει στο διάστημα $0 \leq M \leq n$. Αυτό γίνεται με ομαδοποίηση του κειμένου σε μπλοκ των k bit, όπου το k είναι ο μεγαλύτερος ακέραιος για τον οποίο η σχέση $z^k < n$ είναι αληθής.
- υπολογίζεται το $C = M^e \bmod n$ όπου το C είναι το κρυπτογραφημένο κείμενο

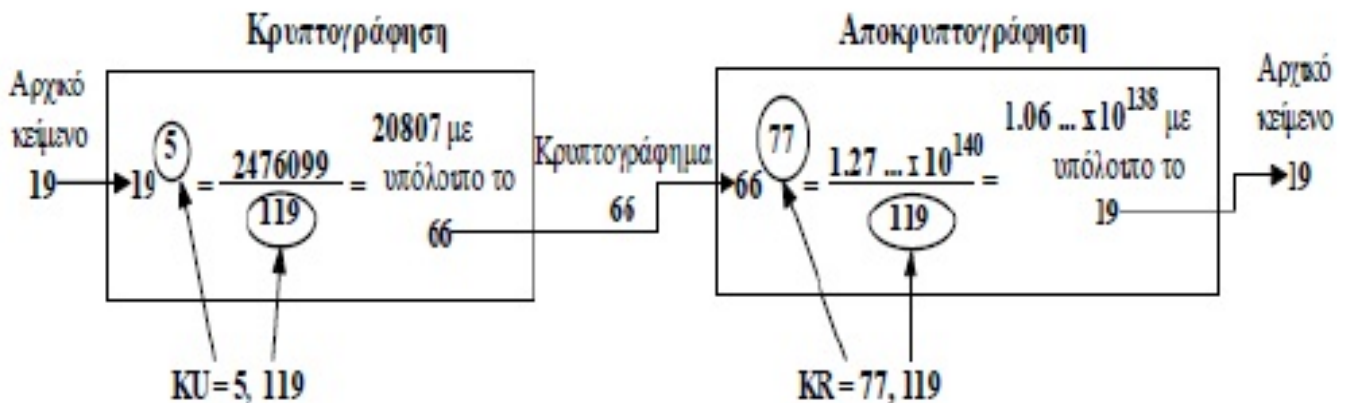
Τώρα για την αποκρυπτογράφηση του κειμένου C εκτελούνται τα παρακάτω:

- υπολογίζεται το $M = C^d \bmod n$ όπου το M είναι το αρχικό κείμενο

Η ασφάλεια της μεθόδου οφείλεται στην δυσκολία παραγοντοποίησης μεγάλων αριθμών. Εάν ο κρυπταναλυτής μπορούσε να παραγοντοποιήσει το δημόσια γνωστό n , θα μπορούσε στην συνέχεια να βρει τα p και q και από αυτά το $\phi(n)$.

Αν διαθέτει τα $\phi(n)$ και d μπορεί να βρει το e με την βοήθεια του αλγορίθμου του Ευκλείδη. Σύμφωνα με τον Rivest, η παραγοντοποίηση ενός αριθμού με 200 ψηφία, απαιτεί 4 δισεκατομμύρια χρόνια υπολογιστικού χρόνου, θεωρώντας ότι γίνεται χρήση ενός υπολογιστή με χρόνο 1μsec.

Ακόμα και αν οι υπολογιστές συνεχίσουν να γίνονται γρηγορότεροι κατά μια τάξη μεγέθους ανά δεκαετία, θα χρειάζονται αιώνες, για να γίνει δυνατή η παραγοντοποίηση αριθμών με 500 ψηφία, αλλά και τότε θα είναι δυνατόν να επιλέγονται μεγαλύτεροι p και q . Σήμερα απαιτείται τα κλειδιά που παράγονται από τον RSA να έχουν μήκος τουλάχιστον 1024 bits, έτσι ώστε να παρέχεται ικανοποιητική ασφάλεια στις επικοινωνίες μέσα στα επόμενα χρόνια.



Σχήμα 4.1: Παράδειγμα Αλγορίθμου RSA

4.3.1 Λειτουργία του Αλγορίθμου RSA

Στην αρχή, για την παραγωγή των κλειδιών κρυπτογράφησης, επιλέγονται δυο αριθμοί p, q οι οποίοι πρέπει να είναι μεγάλοι και να κρατιούνται μυστικοί, και ύστερα υπολογίζεται το γινόμενο τους $n = p \times q$, το οποίο αποτελεί βασικό παράγοντα για τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης. Στη συνέχεια εφαρμόζεται η τιμή της συνάρτησης $\phi(n)$, που είναι γνωστή ως συνάρτηση του Euler για το n ($\phi(n) = (p-1)(q-1)$), και η οποία δείχνει το πλήθος των θετικών ακέραιων αριθμών που είναι μικρότεροι από n και πρώτοι με αυτόν. Στη συνέχεια επιλέγεται ένας αριθμός e ώστε να είναι μικρότερος του n . Ο αριθμός αυτός δεν είναι απαραίτητο να είναι πρώτος αλλά πρέπει οπωσδήποτε να είναι περιττός. Επιπλέον, ο αριθμός e πρέπει να είναι πρώτος ως προς το $\phi(n)$, δηλαδή ο μέγιστος κοινός διαιρέτης του e και του $\phi(n)$ να είναι το 1. Στο τέλος υπολογίζεται ο d , ως φυσικός αντίστροφος αριθμός $e \bmod \phi(n)$, από τη σχέση $d = e^{-1} \bmod \phi(n)$. Ο d ονομάζεται πολλαπλασιαστική ανάστροφος του e .

Ας υποθέσουμε ότι ο χρήστης A έχει γνωστοποιήσει το δημόσιο κλειδί του στον χρήστη B ο οποίος επιθυμεί να στείλει ένα μήνυμα M στον A. Αρχικά το μήνυμα M (το οποίο θεωρούμε ως μια ακολουθία bits) παριστάνεται με έναν ακέραιο αριθμό που βρίσκεται εντός της περιοχής $[0, n-1]$. Σε περίπτωση που το μήνυμα M είναι μεγάλο, διαιρείται σε μικρότερα τμήματα. Ακολουθώντας, κάθε ένα τμήμα του μηνύματος αναπαρίσται με έναν ακέραιο αριθμό που βρίσκεται εντός της περιοχής $[0, n-1]$. Σ' αυτό το σημείο πρέπει να τονίσουμε ότι ο αριθμός αυτός είναι διαφορετικός για κάθε τμήμα του μηνύματος αλλά έχει το ίδιο σταθερό μήκος για όλα τα τμήματα. Ύστερα ο B κρυπτογραφεί κάθε τμήμα του μηνύματος με βάση την παράσταση $C = M^e \bmod n$ και μεταδίδει το C . Για την αποκρυπτογράφηση του μηνύματος, ο χρήστης A υπολογίζει την παράσταση $M = C^d \bmod n$.

Παρακάτω φαίνεται συνοπτικά η λειτουργία του αλγορίθμου:

Παραγωγή κλειδιών	
Επέλεξε p, q	p και q οι δυο πρώτοι
Υπολόγισε $n = p \times q$	
Υπολόγισε $\phi(n) = (p-1)(q-1)$	
Επέλεξε ακέραιο e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Υπολόγισε d	$d = e^{-1} \bmod \phi(n)$
Δημόσιο κλειδί	$KU = \{ e, n \}$
Ιδιωτικό κλειδί	$KR = \{ d, n \}$
Αποκρυπτογράφηση	
Κρυπτοσύστημα:	C
Αρχικό κείμενο:	$M = C^d \bmod n$
Κρυπτογράφηση	
Κρυπτογράφημα:	$M < n$
Αρχικό κείμενο:	$C = M^e \bmod n$

Σχήμα 4.2: Αλγόριθμος RSA

4.3.2 Πλεονεκτήματα του Αλγορίθμου RSA

Ο RSA παρέχει μερικά πλεονεκτήματα τα οποία βοήθησαν στην υλοποίηση πιο ασφαλών και ευκολότερα διαχειρίσιμων συναλλαγών. Τα πλεονεκτήματα αυτά είναι:

- η απλοποίηση στην διαχείριση των κλειδιών που αποτελεί έναν από τους λόγους που πλεονεκτεί ο αλγόριθμος RSA. Για την συμμετρική κρυπτογραφία ο αριθμός των κλειδιών είναι ανάλογος του n^2 , ενώ στην ασύμμετρη κρυπτογραφία ο αριθμός των κλειδιών είναι $2n$. Στα κρυπτοσυστήματα δημόσιου κλειδιού η σχέση που υπάρχει ανάμεσα στον αριθμό των χρηστών και στον αριθμό των κλειδιών, είναι γραμμική και έτσι είναι εύκολο να διαχειριστεί, ακόμα και εάν οι χρήστες είναι πάρα πολλοί.
- η ενισχυμένη ασφάλεια στις συναλλαγές, όπου ο κάθε χρήστης παράγει μόνος του και για αποκλειστικά δική του χρήση κάποιο ζευγάρι κλειδιών κρυπτογράφησης. Το ιδιωτικό κλειδί θα πρέπει να διατηρείται μυστικό και κρυφό, από τον καθένα που δεν έχει εξουσιοδότηση. Από την άλλη το δημόσιο κλειδί είναι διαθέσιμο σε όλους και άρα μπορεί να μεταφερθεί μέσα από ένα δίκτυο, χωρίς να δημιουργείται πρόβλημα στο να διατηρηθεί η μυστικότητα του κλειδιού.

Ο αλγόριθμος RSA είναι κάτι παραπάνω από δεδομένο στην κρυπτογραφία δημοσίου κλειδιού σε σημείο μάλιστα που οι δύο έννοιες να θεωρούνται ταυτόσημες. Η ισχύς του RSA είναι τόσο μεγάλη που η κυβέρνηση των ΗΠΑ έχει περιορίσει σημαντικά την εξαγωγή του αλγορίθμου σε ξένες χώρες.

4.3.3 Ασφάλεια του Αλγορίθμου RSA

Η ασφάλεια του RSA εξαρτάται εξ' ολοκλήρου από το πρόβλημα της επεξεργασίας μεγάλων αριθμών. Τεχνικά αυτό δεν είναι απόλυτα η αλήθεια. Δεν έχει αποδειχθεί ποτέ μαθηματικά ότι χρειάζεται να επεξεργαστούμε το n για να υπολογίσουμε το M από το C και το e . Θα έπρεπε να έχει βρεθεί ένας διαφορετικός τρόπος για να κρυπτανalύσουμε τον RSA. Ωστόσο, αν αυτός ο καινούριος τρόπος επιτρέπει στον κρυπτανalυτή να μειώσει το d , θα μπορούσε επίσης να χρησιμοποιηθεί σαν ένας τρόπος για να επεξεργαστούμε μεγάλους αριθμούς.

Είναι επίσης πιθανό να υλοποιήσουμε τον RSA με το να μαντεύουμε την αξία του $(p-1)(q-1)$. Αυτή η υλοποίηση δεν είναι πιο εύκολη από την διαδικασία επεξεργασίας του n . Το να επαληθεύσουμε ακόμα και συγκεκριμένα ψηφία μιας πληροφορίας από ένα κρυπτογραφημένο με RSA κείμενο είναι το ίδιο δύσκολο με το να αποκρυπτογραφήσουμε το συγκεκριμένο μήνυμα. Η επεξεργασία του n είναι η πιο προφανής έννοια αυτής της υλοποίησης. Κάθε οντότητα θα έχει το δημόσιο κλειδί, e , και το n . Για να βρει το κλειδί της αποκρυπτογράφησης, d , πρέπει να επεργαστεί το n . Είναι σίγουρα πολύ πιθανό για έναν κρυπτανalυτή να δοκιμάσει κάθε πιθανό d μέχρι να πετύχει το σωστό. Αυτή η εξαναγκαστική υλοποίηση είναι ακόμα λιγότερο αποτελεσματική από το να δοκιμάσει να επεξεργαστεί το n .

Από καιρό σε καιρό, οι άνθρωποι ισχυρίζονται ότι έχουν βρει εύκολους τρόπους να σπάσουν τον RSA. Για παράδειγμα, το 1993 ο William Payne πρότεινε μια μέθοδο βασισμένη στο θεώρημα του Fermat. Δυστυχώς αυτή η μέθοδος είναι επίσης πιο αργή από το να επεξεργαστούμε το n .

4.3.4 Πιθανές Επιθέσεις του Αλγορίθμου RSA

Οι τρόποι που υπάρχουν ώστε να είναι εφικτή και επιτυχημένη κάποια επίθεση στον RSA αναφέρονται στην συνέχεια:

- ένας τρόπος είναι η συνεχής και εξαντλητική αναζήτηση, δοκιμάζοντας τα πιθανά κλειδιά, έτσι όσο πιο μεγάλο είναι το μέγεθος των κλειδιών τόσο πιο ασφαλής είναι ο αλγόριθμος. Όμως γίνεται πιο αργός, λόγω του μεγάλου μεγέθους των κλειδιών.
- δεύτερος τρόπος είναι το λεγόμενο πρόβλημα RSA, δηλαδή η παραγοντοποίηση του δημόσιου κλειδιού. Σε αυτήν την επίθεση ο κάθε επίδοξος εισβολέας, σε κάποιο δίκτυο επικοινωνίας, έχει αποκλειστικό σκοπό την ανάκτηση του αρχικού κειμένου από το αντίστοιχο κρυπτογραφημένο κείμενο δεδομένου του δημόσιου κλειδιού του παραλήπτη. Από την στιγμή που ο επιτιθέμενος καταφέρει να υπολογίσει το δημόσιο κλειδί, μπορεί και να αποκρυπτογραφήσει την κάθε πληροφορία που στέλνεται σε κάποιον χρήστη. Αυτή είναι από τις πιο δημοφιλείς επιθέσεις στα συστήματα δημόσιου κλειδιού. Για να είναι επιτυχής θα πρέπει να λυθούν διάφορα είδη μαθηματικών προβλημάτων όπως να παραγοντοποιηθεί ένας αριθμός ο οποίος έχει σχέση με το δημόσιο κλειδί, και βέβαια το πρόβλημα δυσκολεύει περισσότερο όσο πιο μεγάλοι είναι οι αριθμοί.
- ένας άλλος τρόπος για να πετύχει μια επίθεση είναι η επίθεση επανάληψης. Είναι το είδος της επίθεσης στο οποίο το κρυπτογραφημένο κείμενο αποκρυπτογραφείται πολλές φορές, έως ότου αποκτηθεί το αρχικό κείμενο. Με μεγάλο αριθμό επαναλήψεων στην αποκρυπτογράφηση μπορεί κάποιος τρίτος μη εξουσιοδοτημένος, να καταφέρει να αποκτήσει το αρχικό κείμενο. Αυτή όμως η μέθοδος δεν είναι πρακτική όταν το κλειδί έχει μεγάλο μήκος.
- τέταρτη περίπτωση είναι η επίθεση στο υπόλοιπο RSA n . Αυτή η μέθοδος εφαρμόζεται σε περιπτώσεις που μια ομάδα χρηστών που επικοινωνούν έχουν κλειδιά με το ίδιο n . Όταν χρησιμοποιείται ο RSA χρειάζεται απαραίτητα ο κάθε χρήστης να διαλέγει το δικό του υπόλοιπο RSA n .
- τέλος ένας επιπλέον τρόπος είναι η αλγοριθμική επίθεση, να βρεθεί δηλαδή μια αδυναμία στο μαθηματικό πρόβλημα, πάνω στο οποίο βασίζεται το σύστημα κρυπτογράφησης. Κάποια στιγμή βρέθηκε ένας μαθηματικός τρόπος με τον οποίο ανακτάται το μυστικό κλειδί από το δημόσιο μέσα σε πολύ μικρό χρόνο.

4.4 Ο Αλγόριθμος Diffie and Hellman

Αυτός προτάθηκε από τους Diffie και Helman το έτος 1976 και είναι ο πρώτος από τους κρυπταλγόριθμους δημόσιου κλειδιού. Ο συγκεκριμένος αλγόριθμος είναι πρωτόκολλο συμφωνίας κλειδιού, όπου ο καθένας από δύο χρήστες που βρίσκονται σε επικοινωνία, χρησιμοποιεί πάντα το ιδιωτικό του κλειδί από την μια μεριά και το δημόσιο κλειδί του άλλου, με αντικειμενικό σκοπό την δημιουργία ενός κλειδιού που είναι συμμετρικό, το οποίο κανένας άλλος χρήστης δεν καταφέρνει να υπολογίσει. Στην αρχή, όταν πρωτοδημιουργήθηκε αυτός ο αλγόριθμος, δεν ήταν ανθεκτικός σε επιθέσεις man-in-the-middle. Όμως το έτος 1992, δημιουργήθηκε μία πιο ανανεωμένη έκδοση αυτού του αλγορίθμου με σκοπό να αντιμετωπιστεί η εν λόγω επίθεση. Η έκδοση αυτή αναπτύχθηκε από τους Diffie, Oorschot και Wiener. Οι επικοινωνούντες ανταλλάσσουν μηνύματα τα οποία είναι υπογεγραμμένα με τα ιδιωτικά τους κλειδιά και παράλληλα χρησιμοποιούν πιστοποιητικά, για να μπορέσουν να αποκτήσουν τα σωστά δημόσια κλειδιά.

4.5 Ο Αλγόριθμος El Gamal

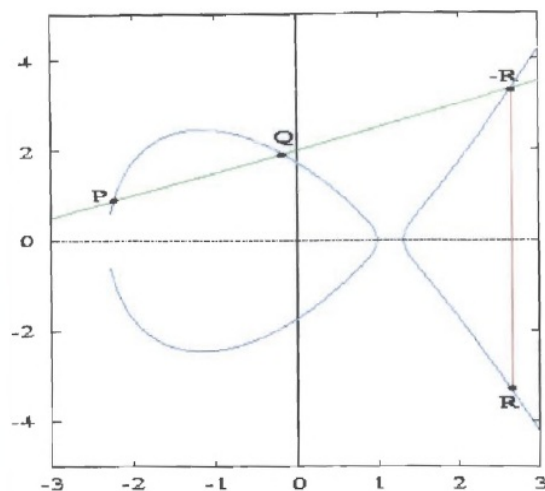
Είναι ένα κρυπτοσύστημα δημόσιου κλειδί, το οποίο στηρίζεται στο δυσεπίλυτο πρόβλημα του διακριτού λογαρίθμου. Το σύστημα αυτό αποτελείται τόσο από αλγορίθμους όσο και από ψηφιακές υπογραφές. Ο αλγόριθμος El Gamal μοιάζει πολύ με τον αλγόριθμο Diffie και Helman. Ακόμα οι αλγόριθμοι El Gamal και RSA έχουν ασφάλεια σε επιθέσεις παρόμοια, με την προϋπόθεση ότι τα κλειδιά είναι αντίστοιχου μήκους. Τα κυριότερα μειονεκτήματα του αλγορίθμου είναι αφενός η αργή του ταχύτητα και αφετέρου ότι κατά την διάρκεια της κρυπτογράφησης, η επέκταση των μηνυμάτων από έναν παράγοντα δεν πραγματοποιούνται.

4.6 Ο Αλγόριθμος DSA

Ο αλγόριθμος DSA δημοσιοποιήθηκε από το NIST, που είναι ένα αμερικάνικο ινστιτούτο, τον Μάιο του 1994. Είναι ο πρώτος αλγόριθμος για την δημιουργία ψηφιακών υπογραφών και είναι ο επίσημος αλγόριθμος για την παραγωγή τους. Η λογική της λειτουργίας του στηρίζεται σε αυτή της ασύμμετρης κρυπτογράφησης, αφού ο κάθε χρήστης έχει την δυνατότητα να δημιουργήσει ένα ζευγάρι από κλειδιά ήτοι ένα δημόσιο και ένα ιδιωτικό. Και αυτός βασίζεται στο πρόβλημα του διακριτού λογαρίθμου και χρησιμοποιείται αποκλειστικά και μόνο για την παραγωγή ψηφιακών υπογραφών με την διαφορά, σε σχέση με τον RSA, ότι στον DSA η παραγωγή της υπογραφής είναι πολύ γρηγορότερη από την επιβεβαίωσή της, ενώ στον RSA συμβαίνει το ακριβώς αντίθετο. Τα μειονεκτήματά του είναι η έλλειψη ευελιξίας, αργής επιβεβαίωσης στις ψηφιακές υπογραφές καθώς και της αδυναμίας του να συνεργαστεί με άλλα πρωτόκολλα πιστοποίησης ταυτότητας.

4.7 Αλγόριθμος Ελλειπτικών Καμπυλών

Η κρυπτογραφία των ελλειπτικών καμπυλών (Elliptic Curve Cryptography) προτάθηκε το 1985 από τους Neal Koblitz και V S Miller, ανεξάρτητα ο ένας από τον άλλον. Και αυτή βασίζεται στο πρόβλημα του διακριτού λογαρίθμου και βρίσκει εφαρμογή χρησιμοποιώντας τον DSA και DH ελλειπτικών καμπυλών δηλαδή του ECDSA και του ECDH αντίστοιχα. Οι δύο αυτοί αλγόριθμοι εκτελούνται χρησιμοποιώντας ένα σύνολο από σημεία τα οποία προκύπτουν σαν λύση της εξίσωσης μιας ελλειπτικής καμπύλης, πάνω σε ένα πεπερασμένο σώμα. Η ασφάλεια αυτών των δύο αλγορίθμων στηρίζεται στην δυσκολία που υπάρχει στον υπολογισμό λογαρίθμων οι οποίοι είναι πάνω σε ένα σύνολο από σημεία σε μια ελλειπτική καμπύλη. Το μέγεθος των κλειδιών κρυπτογράφησης των αλγορίθμων αυτών είναι τουλάχιστον στα 192 έτσι ώστε να μπορεί να εξασφαλιστεί ασφάλεια που να είναι αρκετή για τα συστήματα επικοινωνιών τα χρόνια που ακολουθούν. Ο ECDSA είναι ένας αλγόριθμος εγκεκριμένος, ο οποίος χρησιμοποιείται για την δημιουργία καθώς και για την επαλήθευση των ψηφιακών υπογραφών.



Σχήμα 4.3: Ελλειπτική Καμπύλη

4.8 Αλγόριθμοι MD2, MD4 και MD5

Οι αλγόριθμοι MD2 MD4 και MD5 είναι αλγόριθμοι κατακερματισμού, οι οποίοι αναπτύχθηκαν από τον Ron Rivest, ο μεν πρώτος το 1989, ο δεύτερος το 1990 και ο τρίτος το 1991. Προορίζονταν για να παράγονται ψηφιακές υπογραφές. Κατά την διαδικασία εφαρμογής τους κατά πρώτον το μήνυμα υπόκειται σε σμίχρυνση και κατόπιν το message digest του μηνύματος κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα. Και οι τρεις αυτοί αλγόριθμοι παίρνουν στην είσοδό τους μήνυμα με αυθαίρετο μήκος και κατόπιν δίνουν στην έξοδο ένα message digest το οποίο έχει μέγεθος 128 bits. Ο αλγόριθμος MD2 είχε σχεδιαστεί για μηχανές των 8 bits ενώ ο MD4 και ο MD5 είχαν προορισμό για μηχανές των 32 bits.

Στον MD2 το μήνυμα αρχικά συμπληρώνεται με τον κατάλληλο αριθμό από bytes έτσι ώστε το μήκος των bytes να μπορεί να διαιρεθεί με τον αριθμό 16. Ένα αρχικό checksum των 16 bits προστίθεται στο τέλος του μηνύματος που αποστέλλεται και το τελικό message digest παράγεται από το αποτέλεσμα που είχε η αμέσως προηγούμενη ενέργεια.

Στον MD4 το μήκος που έχει το μήνυμα συμπληρώνεται με τέτοιον αριθμό bits ώστε το μήκος σε bits προσθέτοντας σε αυτά και τον αριθμό 448, το νούμερο το οποίο προκύπτει να διαιρείται με τον αριθμό 512. Μια δυαδική παράσταση από 64 bits προστίθεται στο μήνυμα και το αποτέλεσμα που εξάγεται μπαίνει σε διαδικασία επεξεργασίας με compression function. Τα block τα οποία διαχειρίζεται ο compression function έχουν μήκος 512 bits και το κάθε block τίθεται σε πλήρη επεξεργασία σε τρεις διακριτούς γύρους. Μετά από έρευνα αποδείχτηκε ότι η διαδικασία μπορεί να αντιστραφεί και κάτω από ορισμένες συνθήκες ο αλγόριθμος δεν είναι αμφιμονοσήμαντος.

Ο τρίτος αλγόριθμος, ο MD5 είναι μια πιο καλή και βελτιωμένη έκδοση του αλγορίθμου MD4 και για αυτόν τον λόγο δεν είναι τόσο γρήγορος. Η μόνη διαφορά την οποία έχουν είναι στην χρήση τεσσάρων επαναλήψεων στο κάθε block. Οι απαιτήσεις που υπάρχουν στο μέγεθος του block καθώς και για το μήκος του μηνύματος παραμένουν ίδιες.

4.9 Αλγόριθμοι SHA και SHA-1

Ο SHA, όπως και SHA-1, αναπτύχθηκαν από την Εθνική Υπηρεσία Ασφάλειας των Η.Π.Α (NIST). Ο SHA-1 αποτελεί επανέκδοση του SHA με διόρθωση μιας ατέλειες του τελευταίου. Αυτός σχεδιάστηκε αποκλειστικά για χρήση σε συνδυασμό με τον DSA και άρα δεν μπορεί να χρησιμοποιηθεί

με τον RSA ή οποιονδήποτε άλλο αλγόριθμο δημόσιου κλειδιού για ψηφιακή υπογραφή. Οι σχεδιαστικές αρχές του SHA-1 είναι παρεμφερείς με αυτές των συναρτήσεων κατακερματισμού MD2, MD4 και κυρίως της συνάρτησης MD5. Ο αλγόριθμος μπορεί να έχει σαν είσοδο μήνυμα μήκους μικρότερου από 264 bits. Η έξοδος του αλγορίθμου ονομάζεται σύνοψη μηνύματος και έχει μήκος 160 bits, είναι πιο αργός από τον MD5, αλλά παράγει μεγαλύτερο message digest, με αποτέλεσμα να είναι πιο ισχυρός σε προσπάθειες αντιστροφής του.

4.10 Ripemd-160

Οι αλγόριθμοι Ripemd είναι μια οικογένεια κρυπτογραφικών συναρτήσεων κατακερματισμού, που αναπτύχθηκαν στο Leuven στο Βέλγιο από τους Hans Dobbertin, Antoon Bosselaers και Bart Preneel, η οποία ήταν μία ερευνητική ομάδα από το καθολικό Πανεπιστήμιο του Λεουβέν. Δημοσιεύτηκε για πρώτη φορά το 1996 και δημιουργήθηκε με βάση τις αρχές σχεδιασμού που χρησιμοποιούνται στην MD4 και είναι παρόμοια στην απόδοση με την SHA-1.

Ο Ripemd-160 είναι μία βελτιωμένη έκδοση των 160 bits, σε σχέση με τον αρχικό Ripemd. Χρησιμοποιείται λιγότερο συχνά από ότι ο SHA-1. Υπάρχουν επίσης εκδόσεις των 128, 256 και 320 bits. Ο Ripemd-128 έχει αμφίβολη ασφάλεια σε επιθέσεις, ενώ οι Ripemd-256 και Ripemd-320 μειώνουν την πιθανότητα τυχαίων επιθέσεων, και δεν έχουν υψηλότερα επίπεδα ασφάλειας σε σχέση με τις εκδόσεις Ripemd-128 και Ripemd-160.

Ο Ripemd-160 εκπροσωπείται συνήθως σαν 40-ψήφιος δεκαεξαδικός αριθμός. Η σχεδιαστική του φιλοσοφία είναι να οικοδομηθεί, όσο γίνεται περισσότερο, η εμπειρία που αποκτήθηκε από την αξιολόγηση των MD4 και MD5 καθώς και του απλού Ripemd. Τέλος ο Ripemd-160 είναι συντονισμένος για επεξεργασία 32-bits.

	MD5	SHA-1	RIPEMD-160
Μήκος Σύνοψης	128 bits	160 bits	160 bits
Βασική μονάδα επεξεργασίας	512 bits	512 bits	512 bits
Αριθμός βημάτων	64 (4 rounds of 16)	80 (4 rounds of 20)	160 (5 paired rounds of 16)
Μέγιστο μέγεθος μηνύματος	a	$2^{64} - 1$ bits	a
Αρχική τυπική συνάρτηση	4	4	5
Επιπλέον χρησιμοποιούμενες σταθερές	64	4	9

Σχήμα 4.4: Συγκριτική παρουσίαση των αλγορίθμων MD5, SHA-1, RIPEMD-160

4.11 Επιθέσεις στους Αλγορίθμους Δημόσιου Κλειδιού

Οι αλγόριθμοι του δημόσιου κλειδιού είναι θεωρητικά πολύ πιο ευάλωτοι σε επιθέσεις, σε σχέση τους συμμετρικούς αλγορίθμους. Αυτό συμβαίνει γιατί αυτός ο οποίος επιτίθεται είναι πολύ πιθανό να έχει αντίγραφο του δημόσιου κλειδιού το οποίο χρησιμοποιήθηκε για την κρυπτογράφηση του μηνύματος. Η δουλειά του κάθε επιτιθέμενου γίνεται ακόμα πιο εύκολη, επειδή το ίδιο μήνυμα είναι πιθανό να υποδηλώνει με ποιόν αλγόριθμο εκτελέστηκε η κρυπτογράφηση. Οι επιθέσεις για αυτήν την κατηγορία των αλγορίθμων είναι δύο κατηγοριών, οι επιθέσεις παραγοντοποίησης και οι αλγοριθμικές.

4.11.1 Επιθέσεις παραγοντοποίησης (factoring attacks)

Οι πιο δημοφιλείς επιθέσεις στους αλγορίθμους δημόσιου κλειδιού, είναι οι επιθέσεις παραγοντοποίησης, για τον λόγο του ότι είναι πολύ εύκολο να κατανοηθούν. Ο σκοπός αυτών των επιθέσεων είναι να εξάγουν το ιδιωτικό κλειδί του χρήστη από το αντίστοιχο δημόσιο κλειδί. Στην επίθεση παραγοντοποίησης θα πρέπει να επιλυθούν πολλά μαθηματικά προβλήματα. Επί παραδείγματι στον αλγόριθμο RSA για να μπορέσει να πετύχει η επίθεση, θα χρειαστεί να παραγοντοποιηθεί ένας αριθμός που να έχει σχέση με το δημόσιο κλειδί. Η παραγοντοποίηση δυσκολεύει κατά πολύ εάν υπάρχουν μεγάλοι αριθμοί, έχουν βρεθεί βέβαια, για μια κατηγορία αριθμών, κάποιες εύκολες μέθοδοι, παρόλα αυτά όμως παραμένει μια δύσκολη δουλειά. Η πιο γνωστή επίθεση παραγοντοποίησης είναι η RSA-129 αριθμού που έγινε γνωστή το 1994. Η Data Security δημοσιεύει κατά διαστήματα κάποιες λίστες, οι οποίες περιλαμβάνουν τέτοιους αριθμούς οι οποίοι είναι στην διάθεση του καθενός να παραγοντοποιήσει κάποιους από αυτούς, έναντι χρηματικής αμοιβής.

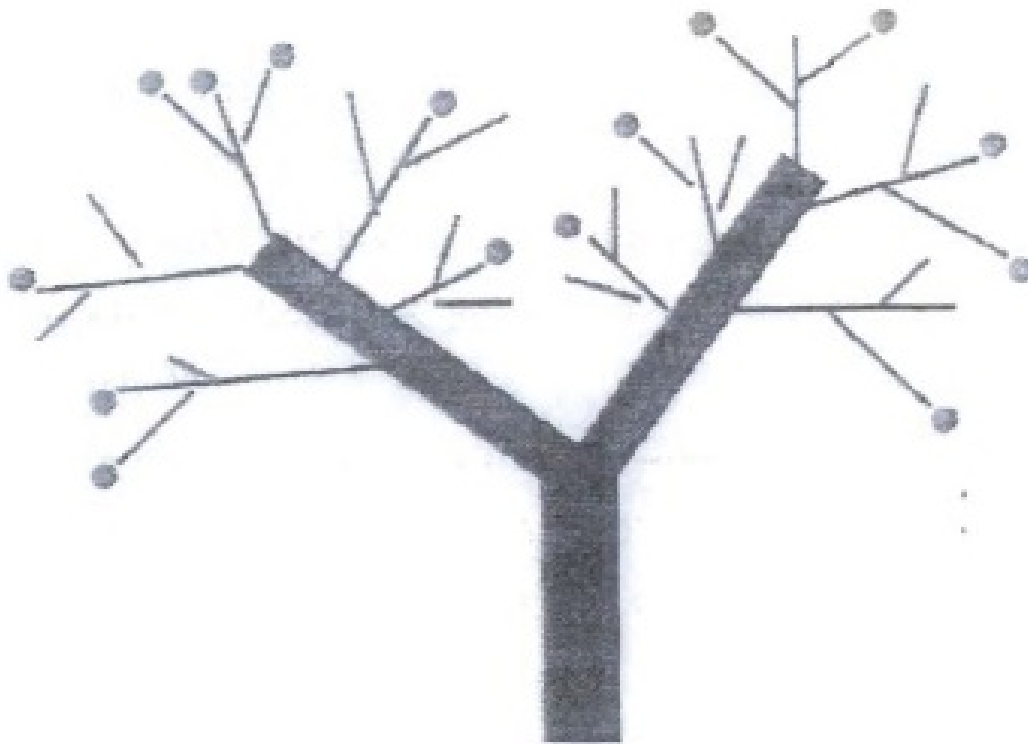
4.11.2 Επιθέσεις αλγοριθμικές

Η αλγοριθμική επίθεση είναι κάποιος άλλος τρόπος ώστε να βρεθεί κάποιο μειονέκτημα ή κάποια αδυναμία στο μαθηματικό πρόβλημα πάνω στο οποίο έχει βασιστεί το κρυπτογραφικό σύστημα. Το πρώτο κρυπτογραφικό σύστημα στο οποίο εφαρμόστηκε είχε βασιστεί σε ένα μαθηματικό πρόβλημα το οποίο είναι γνωστό σαν Super Increasing Knapsack Problem. Είναι το πρόβλημα αθροίσματος υποσυνόλου, το οποίο είναι ένα σημαντικό πρόβλημα της επιστήμης των υπολογιστών, που δεν έχει λυθεί. Δηλαδή είναι το ερώτημα το οποίο τίθεται ότι αν κάθε πρόβλημα, που η ύπαρξη λύσης μπορεί να επιβεβαιωθεί γρήγορα από κάποιον υπολογιστή, τότε μπορεί να λυθεί γρήγορα από τον υπολογιστή. Μετά από κάποια χρόνια βρέθηκε τρόπος με τον οποίο μπορεί κάποιος να αποκτήσει το ιδιωτικό κλειδί από το δημόσιο και μάλιστα σε μικρά χρονικά διαστήματα.

4.12 Στεγανογραφία

Η στεγανογραφία είναι η απόκρυψη της ύπαρξης του ίδιου του μηνύματος. Η διάκριση με την κρυπτογραφία είναι πολύ λεπτή, υπάρχουν όμως πολλές και σημαντικές διαφορές μεταξύ τους.

Κατά καιρούς έχουν αναφερθεί διάφορες στεγανογραφικές μέθοδοι όπως, η μέθοδος να χρησιμοποιούνται εικόνες για την μεταφορά μηνυμάτων. Στο παρακάτω σχήμα βλέπουμε ένα ομορφό δένδρο, στο οποίο υπάρχει ένα κρυμμένο μήνυμα με τον ακόλουθο τρόπο: ακολουθώντας το περίγραμμα του δένδρου με την φορά των δεικτών του ωρολογίου και σημειώνοντας με '1' τα κλαδιά τα οποία έχουν επάνω τους φρούτα και με '0' τα κλαδιά τα οποία δεν έχουν φρούτα, μπορούμε να σχηματίσουμε την ακολουθία των δυαδικών ψηφίων η οποία αποτελεί το μήνυμα.



Σχήμα 4.5: Μια εικόνα που περιέχει το κρυμμένο μήνυμα (110, 010, 111, 010, 010, 010, 100, 101, 011, 001)

Κεφάλαιο 5

Πρωτόκολλο SSL (Secure Socket Layer)

5.1 Γενικά

Το SSL πρωτόκολλο αναπτύχθηκε και εξελίχθηκε από την Netscape Communications, και σκοπός της ήταν να υπάρξει κατά πρώτον όσο γίνεται πιο ασφαλής επικοινωνία στο Internet και δεύτερον να προφυλαχθούν σημαντικές πληροφορίες και δεδομένα όπως είναι τα προσωπικά δεδομένα και οι πιστωτικές κάρτες. Για το πρωτόκολλο αυτό έχει αποδειχθεί ότι είναι από τα καλύτερα standard για να χρησιμοποιηθεί κωδικοποιημένη επικοινωνία και για ένα όσο γίνεται πιο σωστό authentication μεταξύ των clients και των servers.

Το συγκεκριμένο πρωτόκολλο SSL είναι γενικού σκοπού και χρησιμοποιείται, εκτός των άλλων χρήσεων και για κρυπτογραφημένες πληροφορίες ή δεδομένα μέσω του Internet. Αυτό που κάνει είναι να κρυπτογραφήσει τις πληροφορίες που αποστέλλονται από τον client, μέσω του Internet, προς τον server. Στον server γίνεται η διαδικασία της αποκρυπτογράφησης όλων των δεδομένων που εστάλησαν. Το SSL είναι σχεδιασμένο με τέτοιον τρόπο ώστε να εξασφαλίζεται το απόρρητο της επικοινωνίας ανάμεσα σε δύο χρήστες που ο ένας λειτουργεί σαν client και ο άλλος σαν server, πράγμα που σημαίνει ότι προσφέρεται μια point to point υπηρεσία η οποία είναι αξιόπιστη και ασφαλής. Πιο συγκεκριμένα το πρωτόκολλο SSL, όταν το χρησιμοποιεί κάποιος χρήστης μπορεί να κάνει κάποιες ενέργειες, όπως να εισάγει τον αριθμό της πιστωτικής του κάρτας, σε κάποια φόρμα η οποία είναι ασφαλής, μέσω ενός web browser, τον οποίο (αριθμό της κάρτας του) μπορεί να μεταδώσει μέσα από το Internet προς έναν server που είναι ασφαλής, χωρίς δηλαδή να υπάρχει κίνδυνος να αποκαλυφθεί η μεταδιδόμενη πληροφορία ή τα δεδομένα.

Το πρωτόκολλο SSL τρέχει πάνω από το TCP/IP Protocol και κάτω από τα πρωτόκολλα HTTP, IMAP, TELNET. Το πρωτόκολλο αυτό έχει την δυνατότητα να επεκταθεί ή ακόμη και να προσαρμοστεί. Τώρα αν κάποιος από τους επικοινωνούντες δεν χρησιμοποιεί τους ίδιους αλγόριθμους, τότε δεν συνεργάζονται και δεν δουλεύουν τα πρωτόκολλα κρυπτογράφησης. Έτσι στην περίπτωση που κάποιο πρόγραμμα, που δουλεύει το SSL, κάνει την προσπάθεια να επικοινωνήσει με κάποιο άλλο πρόγραμμα, τότε αυτά τα δύο προγράμματα κάνουν σύγκριση ηλεκτρονικά των στοιχείων τα οποία καθορίζουν το ποιος είναι ο πιο δυνατός κρυπταλγόριθμος, τον οποίο διαθέτουν από κοινού.

5.2 Υπηρεσίες που προσφέρει το SSL

Οι υπηρεσίες που προσφέρει το SSL είναι:

- παρέχει εμπιστευτικότητα στην κρυπτογράφηση δεδομένων
- παρέχει ακεραιότητα στα δεδομένα, όταν εκτελέσει την τεχνική MACs (Message Authentication Codes)
- παρέχει επικύρωση της ταυτότητας του client και του server αν αυτοί το επιθυμούν, με υπογεγραμμένα ψηφιακά πιστοποιητικά, που εκδίδονται από έμπιστα τρίτα πρόσωπα τα οποία είναι πιστοποιημένα

Η χρήση του SSL συναντάται σε πολλές εφαρμογές όπως είναι οι περιπτώσεις του Web-banking και Web-shopping στα οποία ο κάθε χρήστης θα πρέπει να αποστείλει κάποια προσωπικά του δεδομένα όπως είναι στοιχεία από πιστωτικές κάρτες. Σε περιπτώσεις πιθανών υποκλοπών σε πληροφορίες ή δεδομένα, το οποίο είναι ότι χειρότερο θα μπορούσε να συμβεί, εμφανίζεται ο SSL, ο οποίος κάνει κρυπτογράφηση των δεδομένων, ώστε κανένας να μην μπορεί να τα υποκλέψει.

5.3 Χαρακτηριστικά του SSL

Η τρίτη έκδοση 3.0 του SSL προσφέρει πολλά θεωρητικά καθώς και πρακτικά χαρακτηριστικά, τα οποία παρουσιάζουν εξαιρετικό ενδιαφέρον. Τέτοια χαρακτηριστικά θα αναφερθούν στην συνέχεια:

- **Διαχωρισμός καθηκόντων:** το πρωτόκολλο SSL χρησιμοποιεί ξεχωριστούς αλγόριθμους για την κρυπτογράφηση, την απόδειξη για την γνησιότητα καθώς και για την εξασφάλιση της ακεραιότητας των δεδομένων. Ακόμη χρησιμοποιεί και διαφορετικά κλειδιά για την κάθε λειτουργία του πρωτοκόλλου. Από αυτά, τα μεν μεγάλα κλειδιά χρησιμεύουν για να αποδειχθεί η γνησιότητα και η ακεραιότητα των δεδομένων, τα δε μικρά κλειδιά χρησιμεύουν για την μυστικότητα. Για το μήκος των κλειδιών, μετά από ρυθμίσεις, μπαίνουν κάποιοι περιορισμοί, μόνο όμως για την εμπιστευτικότητα και όχι για την ακεραιότητα και την γνησιότητα των δεδομένων.
- **Αποτελεσματικότητα:** είναι το χαρακτηριστικό με το οποίο το SSL με τις εφαρμογές του μπορεί να αποθηκεύει κρυφά ένα μυστικό (master secret) το οποίο παραμένει αναλλοίωτο, στις διάφορες συνδέσεις του SSL. Η διαδικασία αυτή χρειάζεται γιατί η κρυπτογράφηση και η αποκρυπτογράφηση είναι διαδικασίες οι οποίες είναι χρονοβόρες.
- **Πιστοποιητικό βασισμένο στην απόδειξη γνησιότητας:** παρέχεται από το πρωτόκολλο SSL για να αποδεικνύεται η γνησιότητα και του client αλλά και του server. Αυτό επιτυγχάνεται με την χρήση των ψηφιακών πιστοποιητικών καθώς και με τις ψηφιακά υπογεγραμμένες προκλήσεις αναγνώρισης. Η τρίτη έκδοση του SSL χρησιμοποιεί τα X.509 version 3 πιστοποιητικά.
- **Αναγνωστικό πρωτόκολλο:** αν και το SSL πρωτόκολλο σχεδιάστηκε για να τρέχει πάνω από το TCP/IP Protocol, στην ουσία μπορεί να τρέξει στην κορυφή του κάθε αξιόπιστου connection-oriented protocol και ένα τέτοιο είναι το X.25, ενώ το IP User Datagram Protocol δεν είναι αξιόπιστο.
- **Υποστήριξη για συμπίεση:** επειδή τα κρυπτογραφημένα δεδομένα δεν είναι δυνατόν να συμπιεστούν, τη διαδικασία αναλαμβάνει το SSL πρωτόκολλο που στο μέλλον θα έχει αυτήν την ικανότητα, αφού σήμερα δεν υπάρχει εφαρμογή του SSL που να ενσωματώνει την διαδικασία της συμπίεσης.

5.4 SSL και Μοντέλο OSI

Αυτό που έχει μεγάλη σημασία σε κάθε καινούργιο πρωτόκολλο επικοινωνίας, είναι να υπάρχει η δυνατότητα εύκολα να αντικατασταθεί ή να ενσωματωθεί στην ήδη υπάρχουσα δομή πρωτοκόλλων. Το SSL έχει αυτή την δυνατότητα και συγκεκριμένα μπορεί να προσαρμοστεί στο μοντέλο επτά στρωμάτων του OSI. Το SSL πρωτόκολλο αποτελείται από δύο υποπρωτόκολλα τα οποία είναι το SSLRP SSL Record Protocol και το SSLHP SSL Handshake Protocol. Το SSLRP SSL Record Protocol είναι αυτό το οποίο ορίζει το κύριο format των πληροφοριών ή των δεδομένων τα οποία ανταλλάσσονται σε κάθε σύνοδο μεταξύ επικοινωνούντων. Επιπλέον κάνει την συμπίεση δεδομένων, ελέγχει την ακεραιότητά τους και τέλος τα κρυπτογραφεί, με την προϋπόθεση όμως ότι και ο client και ο server γνωρίζουν κλειδιά κρυπτογράφησης. Το πρωτόκολλο αυτό υποστηρίζει την αλλαγή των αλγορίθμων για την κρυπτογράφηση καθώς και την αλλαγή των κλειδιών κρυπτογράφησης την κάθε στιγμή. Το SSLHP SSL Handshake Protocol είναι ένα πρωτόκολλο το οποίο χρησιμοποιείται για την διαπραγμάτευση του κρυπταλγορίθμου ο οποίος θα χρησιμοποιηθεί αφενός στην κρυπτογράφηση και αφετέρου στην ανταλλαγή των κλειδιών. Αυτά είναι τα κλειδιά τα οποία θα χρησιμοποιήσουν αυτοί οι οποίοι μετέχουν στην σύνοδο. Η χρήση του SSL πρωτοκόλλου δεν αποκλείει το να χρησιμοποιηθούν και άλλα πρωτόκολλα ασφάλειας υψηλού επιπέδου. Το SSL τέλος δουλεύει επιπλέον στην δομή του OSI και όχι σαν πρωτόκολλο αντικατάστασης.

5.5 Η Αρχιτεκτονική του SSL

Το SSL πρωτόκολλο παρέχει βασικές υπηρεσίες ασφάλειας στα πρωτόκολλα τα οποία βρίσκονται σε υψηλό επίπεδο. Σαν τμήματα του SSL, τρία είναι τα πρωτόκολλα τα οποία δουλεύουν σε υψηλό επίπεδο:

- **To Handshake Protocol**, το οποίο χωρίζεται σε δύο επιμέρους φάσεις. Η πρώτη αφορά την επιλογή των αλγορίθμων, την ανταλλαγή ενός master key καθώς και την πιστοποίηση ταυτότητας του server. Η δεύτερη φάση είναι αυτή η οποία διαχειρίζεται την πιστοποίηση της ταυτότητας του client και ολοκληρώνει την διαδικασία του handshaking. Όταν τελειώσουν αυτές οι δύο φάσεις, έχει τελειώσει και η διαδικασία του handshake, οπότε αρχίζει η μεταφορά δεδομένων ανάμεσα στους επικοινωνούντες. Το πακέτο των κρυπταλγορίθμων περιλαμβάνει την μέθοδο της ανταλλαγής κλειδιών, τον αλγόριθμο κρυπτογράφησης και τέλος τον μηχανισμό που παράγει τον MAC.
- **To Change Cipher Spec Protocol**, είναι το πιο απλό από τα SSL-specific πρωτόκολλα τα οποία χρησιμοποιούν το SSLRP. Αποτελείται από ένα μήνυμα που έχει μέγεθος ένα byte, με σκοπό αυτό το μήνυμα να προκαλέσει την εκκρεμή κατάσταση, να αντιγραφεί στην τρέχουσα κατάσταση που ενημερώνει το cipher suite και τέλος να χρησιμοποιήσει αυτήν την σύνδεση.
- **To Alert Protocol**, χρησιμοποιείται για να μεταφέρει συναγερμό στην ομότιμη οντότητα. Κάθε μήνυμα αποτελείται από δύο byte. Το πρώτο byte παίρνει την τιμή προειδοποίηση (1) ή μοιραίο (2) για να μεταφέρει την σημασία του μηνύματος. Το δεύτερο byte περιέχει έναν κώδικα που ορίζει τον συγκεκριμένο συναγερμό.

Αυτά τα τρία SSL specific πρωτόκολλα χρησιμοποιούνται στην διαχείριση των SSL ανταλλαγών.

Δύο σημαντικές έννοιες του SSL είναι η σύνδεση (connection) και η σύνοδος (session):

- **Η σύνδεση (connection)**: μια λογική σύνδεση client/server που παρέχει έναν κατάλληλο τύπο υπηρεσίας. Για το SSL, τέτοιες συνδέσεις είναι ένα προς ένα σχέσεις. Οι συνδέσεις

είναι παροδικές και κάθε σύνδεση σχετίζεται με μια σύνοδο. Μια κατάσταση σύνδεσης καθορίζεται από τις παρακάτω παραμέτρους:

- **server and client random**: είναι ακολουθίες από bytes που επιλέγονται από τον server και τον client.
 - **server write MAC secret**: το μυστικό κλειδί που χρησιμοποιείται σε MAC (Message Authentication code) λειτουργίες στα δεδομένα που στέλνονται από τον server.
 - **client write MAC secret**: το μυστικό κλειδί που χρησιμοποιείται σε MAC (Message Authentication code) λειτουργίες στα δεδομένα που στέλνονται από τον client.
 - **server write key**: το συμβατικό κλειδί κρυπτογράφησης για τα δεδομένα που κρυπτογραφούνται από τον server και που αποκρυπτογραφούνται από τον client.
 - **client write key**: το συμβατικό κλειδί κρυπτογράφησης για τα δεδομένα που κρυπτογραφούνται από τον client και που αποκρυπτογραφούνται από τον server.
 - **initialization vectors (IV)**: όταν χρησιμοποιείται ένας block-cipher CBC, ένα IV διατηρείται για κάθε κλειδί. Αυτό το πεδίο αρχικά προετοιμάζεται από το SSCHP. Έκτοτε το block του κρυπτογραφήματος συντηρείται από κάθε εγγραφή για την χρήση ως IV για την επόμενη εγγραφή.
 - **sequence numbers**: κάθε ένα από τα συμβαλλόμενα μέρη, διατηρεί χωριστούς τους αριθμούς ακολουθίας, για τα μεταδιδόμενα και για τα λαμβανόμενα μηνύματα, για κάθε σύνδεση. Όταν κάποιο από τα συμβαλλόμενα μέρη στέλνει ή λαμβάνει ένα Change Cipher Spec μήνυμα, ο πιο κατάλληλος αριθμός ακολουθίας τίθεται μηδέν.
- **Η σύνοδος (session)**: μια συσχέτιση μεταξύ ενός client και ενός server. Οι σύνοδοι δημιουργούνται από το Handshake Protocol και καθορίζουν ένα σύνολο κρυπτογραφικών παραμέτρων ασφάλειας, οι οποίες μπορούν να διαμοιραστούν σε πολλαπλές συνδέσεις. Οι σύνοδοι χρησιμοποιούνται για να αποφύγουν πολύπλοκες διαπραγματεύσεις των νέων παραμέτρων ασφάλειας για την κάθε σύνδεση. Μεταξύ κάθε ζευγαριού των συμβαλλομένων μερών, μπορούν να υπάρξουν πολλαπλές ασφαλείς συνδέσεις. Διάφορες καταστάσεις σχετίζονται με κάθε σύνοδο. Όταν μια σύνοδος καθιερώνεται, υπάρχει μια τρέχουσα λειτουργούσα κατάσταση και για διάβασμα και για γράψιμο (δηλαδή και για λήψη και για αποστολή). Μια κατάσταση συνόδου καθορίζεται και αυτή από παραμέτρους οι οποίες είναι:
- **session identifier**: είναι μια αυθαίρετη ακολουθία από bytes τα οποία επιλέγονται από τον server, για να προσδιορίσει μια ενεργή ή μια resumable κατάσταση συνόδου.
 - **peer certificate**: είναι ένα όμοιο πιστοποιητικό X 509. v3. Αυτό το στοιχείο μπορεί να είναι μηδενικό.
 - **compression method**: ο αλγόριθμος που χρησιμοποιείται για να συμπίεσει τα στοιχεία πριν από την κρυπτογράφηση.
 - **cipher spec**: διευκρινίζει τον αλγόριθμο κρυπτογράφησης (όπως τον DES) και έναν αλγόριθμο σύνοψης (όπως τον MD5 ή τον SHA-1). Καθορίζει επίσης τις κρυπτογραφικές ιδιότητες όπως το hash μέγεθος.
 - **master secret**: 48-byte μυστικό διαμοιραζόμενο μεταξύ του client και του server.
 - **resumable**: μια μεταβλητή που δείχνει εάν η σύνοδος μπορεί να χρησιμοποιηθεί για να αρχίσει τις νέες συνδέσεις.

5.6 Πρωτόκολλο SSLRP

Το SSL Record Protocol παρέχει δύο υπηρεσίες για SSL συνδέσεις, οι οποίες είναι εμπιστευτικότητα με την κρυπτογράφηση των δεδομένων και ακεραιότητα του μηνύματος, με την χρήση ενός MAC (Message Authentication Code).

Ένα πακέτο SSL αποτελείται από δύο μέρη την επικεφαλίδα και τα δεδομένα.

Η επικεφαλίδα μπορεί να είναι:

- 3 bytes, που υπάρχει μόνο σε εκδόσεις του πρωτοκόλλου μετά την δεύτερη και προβλέπεται για την ρύθμιση πληροφοριών out-of-hand. Το μέγιστο μέγεθός αυτής της περίπτωσης είναι μέχρι 16383 bytes.
- 2 bytes που χρησιμοποιείται όταν τα δεδομένα χρειάζονται συμπλήρωμα. Το μέγιστο μέγεθός αυτής της περίπτωσης είναι μέχρι 32767 bytes.

Τα δεδομένα είναι δύο τύπων, τα πραγματικά που κρυπτογραφούνται στην μετάδοση και τα δεδομένα συμπλήρωσης που θα χρησιμοποιηθούν εάν χρειαστεί. Αυτό θα γίνει αν οι αλγόριθμοι κρυπτογράφησης είναι σε χρήση block cipher και έχουν ρόλο να συμπληρώσουν τα πραγματικά δεδομένα με μέγεθος πολλαπλάσιο αυτού που μπορεί να δέχεται σαν είσοδο ο block cipher. Στην περίπτωση όμως των stream cipher δεν υπάρχει ανάγκη να συμπληρωθούν τα πραγματικά δεδομένα και έτσι είναι δυνατή η χρήση της επικεφαλίδας των δύο bytes.

Η λειτουργία του SSLRP είναι η εξής: το πρωτόκολλο πρώτα λαμβάνει το μήνυμα της εφαρμογής η οποία θα μεταδοθεί, ακολούθως τα δεδομένα τα μετατρέπει σε τμήματα των 214 bytes και τα συμπιέζει προαιρετικά. Για να υπολογιστεί τώρα το MAC, πάνω από τα δεδομένα που συμπιέστηκαν, χρησιμοποιείται ένα διαμοιραζόμενο μυστικό κλειδί. Έπειτα με συμμετρική κρυπτογράφηση κρυπτογραφεί το αποτέλεσμα. Για την κρυπτογράφηση ρεύματος, το συμπιεσμένο μήνυμα, μαζί με το MAC, κρυπτογραφούνται. Για την block κρυπτογράφηση, μπορεί να προστεθεί ένα padding μετά το MAC και πριν από την κρυπτογράφηση. Έπειτα προσθέτει μια επικεφαλίδα με τα εξής στοιχεία: τύπος περιεχομένου 8 bit, κύρια έκδοση 8 bit, δευτερεύουσα έκδοση 8 bit, και τέλος συμπιεσμένο μήκος των 16 bit. Μεταδίδει το αποτέλεσμα αυτό σε ένα TCP segment και στην συνέχεια τα δεδομένα τα οποία λαμβάνονται αποκρυπτογραφούνται, επιβεβαιώνονται, αποσυμπιέζονται, ξανασυγκεντρώνονται και διανέμονται στους χρήστες των ανωτέρων επιπέδων.

5.7 Εκδόσεις του SSL

Τον Ιούλιο του 1994, γίνεται η πρώτη σχεδίαση του SSL, που αποτέλεσε και την πρώτη έκδοση. Τον Οκτώβριο του 1994 δημοσιεύθηκε με την μορφή RFC (Request For Comments). Αυτή η έκδοση χρησιμοποιήθηκε μέσα στο Netscape.

Τον Δεκέμβριο του 1994 εκδίδεται η δεύτερη έκδοση, που αποτελεί μια αναθεώρηση του πρωτοκόλλου. Η δεύτερη έκδοση συμπεριλήφθηκε με τον Netscape Navigator 1 και 2.

Η τρίτη έκδοσή του παρουσιάστηκε στα τέλη του έτους 1995 ενώ άρχισε να εφαρμόζεται στα προϊόντα της επιχείρησης. Σε αυτή την έκδοση το πρωτόκολλο ενσωμάτωσε και τα πλεονεκτήματα του PCT Private Communication Technology πρωτοκόλλου. Επίσης στην Τρίτη έκδοση του SSL πρωτοκόλλου βασίζεται το TLS Transport Layer Security, το οποίο μοιάζει με την τρίτη έκδοση του πρωτοκόλλου SSL με κάποιες αλλαγές και δημιουργήθηκε από το IETF Internet Engineering Task Force.

5.8 SSL Ψηφιακά Πιστοποιητικά

Το πρωτόκολλο SSL κάνει σε μεγάλο βαθμό χρήση των πιστοποιητικών δημόσιου κλειδιού, ώστε να υπάρχει η δυνατότητα να αποδειχθεί η γνησιότητα των επικοινωνούντων οντοτήτων στις SSL ανταλλαγές. Ακόμη κάνει χρήση των X.509 version 3 πιστοποιητικών, ώστε να γίνει έλεγχος στα RSA ζεύγους κλειδιών. Κάνει επιπλέον έλεγχο με ένα X.509, το οποίο είναι τροποποιημένο, στα δημόσια κλειδιά.

Το πρωτόκολλο SSL υποστηρίζει κάποια είδη πιστοποιητικών τα οποία είναι:

- τα RSA πιστοποιητικά δημόσιου κλειδιού, με δημόσια κλειδιά αυθαίρετου μήκους
- τα RSA πιστοποιητικά δημόσιου κλειδιού που περιορίζονται στα 512 bits για χρήση
- τα κρυπτογραφικά λογισμικά που πρόκειται να εξαχθούν.
- τα RSA πιστοποιητικά που είναι μόνο για υπογραφή, τα οποία περιέχουν RSA δημόσια κλειδιά και χρησιμοποιούνται μόνο για την υπογραφή δεδομένων και όχι για κρυπτογράφηση
- τα DSS πιστοποιητικά
- τα Diffie-Hellman πιστοποιητικά

Η χρήση όλων αυτών των πιστοποιητικών δεν είναι υποχρεωτική. Το πρωτόκολλο SSL έχει απαίτηση για πιστοποιητικά server, εκτός από τη περίπτωση που οι SSL εφαρμογές και του client και του server χρησιμοποιούν το πρωτόκολλο για ανταλλαγή κλειδιών Diffie-Hellman. Τα προϊόντα όμως Netscape δεν εφαρμόζουν τους αλγορίθμους Diffie-Hellman.

5.9 Αντοχή του SSL σε γνωστές επιθέσεις

Dictionary Attack

Αυτή η επίθεση μπορεί να λειτουργήσει στην περίπτωση που ένα μέρος μόνο ενός μη κρυπτογραφημένου κειμένου περιέλθει στην κατοχή μη εξουσιοδοτημένων ατόμων, οπότε το κομμάτι αυτό κρυπτογραφείται κάνοντας χρήση κάθε πιθανού κλειδιού. Κατόπιν ελέγχεται όλο το κρυπτοκείμενο, έως ότου βρεθεί κάποιο τμήμα του το οποίο να ταιριάζει με κάποιο από τα προϋπολογισμένα. Αν τύχει και η έρευνα πετύχει, τότε το κλειδί που κρυπτογραφήθηκε το μήνυμα έχει βρεθεί. Επειδή τα κλειδιά των αλγορίθμων του πρωτοκόλλου είναι αρκετά μεγάλα, με μέγεθος 128 bits, τότε το πρωτόκολλο δεν κινδυνεύει από αυτό το είδος της επίθεσης. Ακόμα και οι αλγόριθμοι σε εξαγόμενα προϊόντα, υποστηρίζουν κλειδιά με μέγεθος 128 bits, παρά το ότι τα 88 bits από αυτά μεταδίδονται χωρίς ασφάλεια. Ο υπολογισμός 240 διαφορετικών ακολουθιών, ο οποίος θα πρέπει να γίνει, κάνει αδύνατη την επιτυχία αυτής της επίθεσης.

Replay Attack

Η επίθεση αυτή γίνεται στην περίπτωση που κάποιο τρίτο άτομο καταγράφει την ανταλλαγή μηνυμάτων μεταξύ δύο οντοτήτων οι οποίες επικοινωνούν. Τότε λοιπόν το τρίτο αυτό άτομο προσπαθεί να κάνει χρήση των μηνυμάτων του client για να μπορέσει να αποκτήσει πρόσβαση στον server. Όμως το πρωτόκολλο SSL κάνει χρήση του connection-id το οποίο παράγεται από τον server με κάποιον τυχαίο τρόπο και το οποίο διαφέρει για την κάθε σύνδεση. Έτσι λοιπόν δεν υπάρχει περίπτωση να υπάρξουν δύο ίδια connection-id και όλα τα μηνύματα που χρησιμοποιήθηκαν δεν είναι δυνατόν να γίνουν δεκτά από τον server. Το connection-id έχει μέγεθος 128 bits, ώστε να υπάρχει επιπλέον ασφάλεια.

Brute Force Attack

Με την χρήση όλων των πιθανών κλειδιών για την αποκρυπτογράφηση, μπορεί να πετύχει αυτή η επίθεση. Όσο όμως μεγαλύτερα είναι σε μέγεθος τα κλειδιά τα οποία χρησιμοποιούνται, τόσο πιο πολλά είναι τα πιθανά κλειδιά. Έτσι λοιπόν η επίθεση αυτή σε αλγόριθμους οι οποίοι χρησιμοποιούν κλειδιά των οποίων το μέγεθος είναι στα 128 bits είναι χωρίς ουσία. Μόνο ο αλγόριθμος DES με μέγεθος 56 bits cipher έχει ευαισθησία σε αυτές τις επιθέσεις και για αυτόν τον λόγο δεν συνιστάται η χρήση του.

Man-In-Middle- Attack

Αυτή η επίθεση γίνεται όταν κάποιος τρίτος μπορεί να παρεμβαίνει στην επικοινωνία μεταξύ δύο οντοτήτων που επικοινωνούν μεταξύ τους. Πρώτα αυτός κάνει επεξεργασία στα μηνύματα του client, αμέσως μετά τα τροποποιεί όπως επιθυμεί αυτός και τελικά τα προωθεί στον server. Το ίδιο ακριβώς κάνει και στα μηνύματα τα οποία στέλνονται από τον server. Το πρωτόκολλο SSL υποχρεώνει τον server να φανερώνει την ταυτότητά του, χρησιμοποιώντας ένα έγκυρο πιστοποιητικό, στο οποίο δεν μπορεί να γίνει τροποποίηση. Όπως όμως είναι γνωστό, υπάρχει η ευχέρεια επικοινωνίας των κλειδιών υπογεγραμμένα.

5.10 Αδυναμίες του SSL

Το πρωτόκολλο SSL δεν εξασφαλίζει τον κάθε χρήστη από διάφορους κακόβουλους, με τους οποίους πιθανώς να θέλει κάποιου είδους συνεργασία, χωρίς βέβαια ο χρήστης να γνωρίζει τις προθέσεις τους. Για να μπορέσει το SSL να εξασφαλίζει την εμπιστευτικότητα στην σύνδεση μεταξύ δύο οντοτήτων οι οποίες επικοινωνούν μεταξύ τους, χρησιμοποιεί μία μέθοδο η οποία είναι γνωστή σαν public key authentication. Όμως υπάρχει ένα πρόβλημα το οποίο αφορά στο ποιοι συνδέονται μεταξύ τους με την μέθοδο αυτή.

Αν ο server και ο client έχουν πρόβλημα, τα πράγματα θα δυσκολέψουν και αυτό γίνεται γιατί ο SSL server δεν μπορεί να εκτελέσει κάποιον έλεγχο στο εάν ο client είναι πράγματι ο νόμιμος ή κάποιος επιτιθέμενος που υπέκλεψε τα στοιχεία του. Ένα άλλο πρόβλημα είναι η παραδοχή ότι όλοι οι clients είναι οι νόμιμοι, πράγμα το οποίο θα οδηγήσει σίγουρα σε καταστάσεις εκτός ελέγχου δυσάρεστες για τους χρήστες. Όταν κάποιος χρήστης εκτελεί κάποια συναλλαγή και αμέσως μετά την ακυρώνει, αυτό σημαίνει ότι ο χρήστης που έκανε την παραγγελία, ίσως να μην είναι εξουσιοδοτημένος. Αυτό γίνεται επειδή το SSL αφήνει το χρήστη εκτός αφού κάνει αυτοματοποίηση στις διαδικασίες.

Αφού όπως φαίνεται το SSL πρωτόκολλο έχει κάποια κενά ασφάλειας, για να μπορεί ο κάθε χρήστης να προφυλαχθεί, θα πρέπει να καταφύγει στις εξής λύσεις:

- Να μπαίνει σε sites που ξέρει ότι έχουν καλό επίπεδο ασφάλειας και αξιοπιστίας.
- Πριν χρησιμοποιήσει ο χρήστης την πιστωτική του κάρτα να βεβαιωθεί για την αξιοπιστία του server.
- Ο χρήστης πρέπει ακόμα να κάνει έλεγχο στο site που μπαίνει, αν παρέχει ασφάλεια και σε πιο επίπεδο. Όσο πιο ψηλά είναι το encryption key τόσο πιο ασφαλής θα είναι και η συναλλαγή που θέλει να κάνει.

Κεφάλαιο 6

Αρχές Πιστοποίησης και Πιστοποιητικά Server

6.1 Αρχές Πιστοποίησης CA (Certification Authorities)

Η Αρχή πιστοποίησης είναι ένας οργανισμός ο οποίος λειτουργεί με ασφάλεια, για τους χρήστες, καθώς και με προδιαγραφές οι οποίες είναι αυστηρές. Σκοπός της αρχής πιστοποίησης είναι να δημιουργήσει και να διανείμει στους ενδιαφερόμενους ψηφιακά πιστοποιητικά. Οι αρχές πιστοποίησης επιβεβαιώνουν τις ταυτότητες των χρηστών που επικοινωνούν και ανταλλάσσουν μεταξύ τους πληροφορίες ή δεδομένα και αμέσως μετά εκδίδουν τα αντίστοιχα ψηφιακά πιστοποιητικά για τον καθένα.

Μια αρχή πιστοποίησης μπορεί να είναι των παρακάτω τύπων:

- ένας έμπιστος τρίτος φορέας (TTP) όπως μια εταιρεία ή μια κυβέρνηση, οι οποίες αντιστοιχούν τα δημόσια κλειδιά με τα αντίστοιχα πρόσωπα ή επιχειρήσεις στους οποίους ανήκουν.
- ένας οργανισμός, που μπορεί να λειτουργεί με τρεις μορφές:
 - Σαν εσωτερική αρχή, η οποία πιστοποιεί στους υπαλλήλους της τις θέσεις που κατέχουν καθώς και την εξουσία που έχουν.
 - Σαν αρχή εξωτερικής προέλευσης υπαλλήλου, στην οποία μια π.χ. εταιρεία συμφωνεί με μία εξωτερική φίρμα που προσφέρει υπηρεσίες πιστοποίησης για τους εργαζομένους της.
 - Σαν αρχή εξωτερικής προέλευσης πελάτη, στην οποία μια π.χ. εταιρεία πιθανόν να συμφωνήσει με μία εξωτερική φίρμα, η οποία θα διευθύνει μια αρχή πιστοποίησης που θα λειτουργεί έτσι ώστε να ωφελούνται οι τρέχοντες καθώς και οι μελλοντικοί πελάτες της, έτσι θα αποφύγει το κόστος της δημιουργίας διαδικασιών πιστοποίησης.

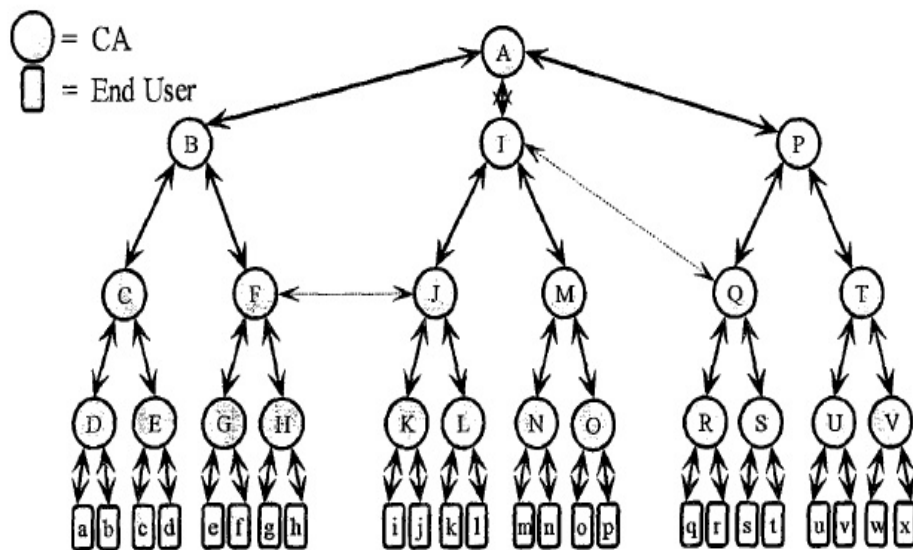
6.2 Ιεραρχίες Πιστοποίησης

Η κάθε αρχή πιστοποίησης θεωρητικά πρέπει να συμμετέχει σε μια ευρύτερη Υποδομή Δημόσιου Κλειδιού, της οποίας η δομή έχει ιεραρχική μορφή, όπου οι αρχές πιστοποίησης οι οποίες βρίσκονται σε ανώτερα επίπεδα, πιστοποιούν τις αρχές που βρίσκονται σε χαμηλότερο επίπεδο. Η κάθε χώρα μπορεί να έχει μία ή ακόμη και περισσότερες αρχές πιστοποίησης όπως επί παραδείγματι για τράπεζες, για νοσοκομεία, για την εκπαίδευση κλπ.

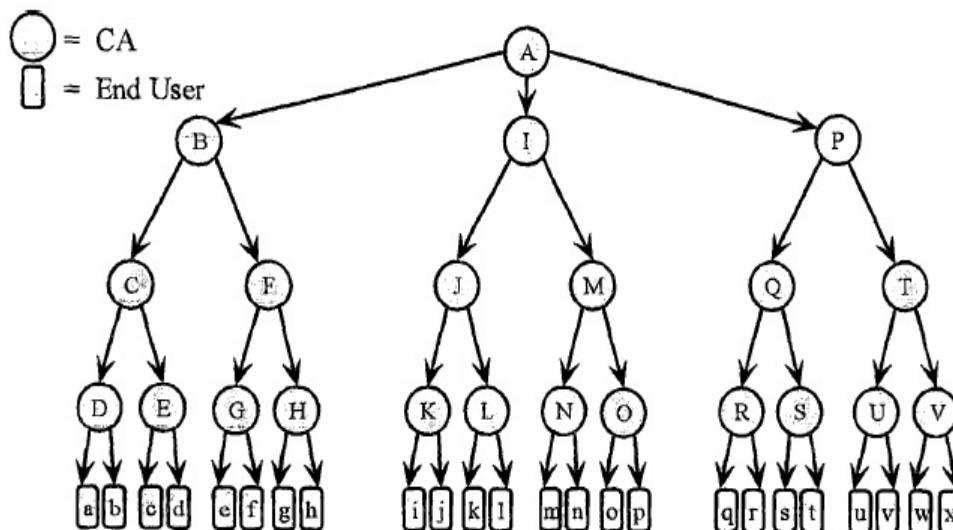
Αν ένας χρήστης θέλει να στείλει κάποια δεδομένα ή κάποια μηνύματα, σε κάποιον άλλο χρήστη και αυτοί οι δύο χρήστες πιστοποιούνται από διαφορετικές αρχές πιστοποίησης, τότε θα πρέπει να γίνει επαλήθευση της ταυτότητας όλων των αρχών πιστοποίησης που παρεμβάλλονται, μέχρι την στιγμή που ο αποστολέας αποκτήσει το δικό του πιστοποιητικό. Η όλη διαδικασία ονομάζεται επαλήθευση διαδρομής. Το μήκος της σχηματίζεται ή από τον αριθμό των αρχών που μεσολαβούν μεταξύ δύο επικοινωνούντων ή από το πλήθος των πιστοποιητικών που πρέπει να επαληθεύσει ο αποστολέας, μέχρι να αποκτήσει το δικό του δημόσιο κλειδί.

Υπάρχουν δύο τρόποι με τους οποίους γίνεται η ιεράρχηση μιας πιστοποίησης:

- η **γενική ιεραρχία**, στην οποία κάθε CA πιστοποιητικό, πιστοποιεί τον "γονέα" και "τα παιδιά της".
- η **κατερχόμενη ιεραρχία (top-down-hierarchy)**, η οποία είναι μια παραλλαγή της προηγούμενης, στην οποία η CA πιστοποιεί μόνο "τα παιδιά της", και η CA που είναι στο ανώτατο επίπεδο, είναι η αφετηρία όλων των διαδρομών πιστοποίησης. Η CA που αποτελεί την αφετηρία της διαδρομής πιστοποίησης, ονομάζεται root CA.



Σχήμα 6.1: Γενική ιεραρχία πιστοποίησης



Σχήμα 6.2: Κατερχόμενη ιεραρχία πιστοποίησης

Υπάρχουν όμως και άλλες PKI (υποδομή δημόσιου κλειδιού), οι οποίες δεν παρουσιάζουν καμία δομή, δηλαδή στην πράξη κάθε CA είναι και root CA του εαυτού της, και έχει τον πλήρη έλεγχο στην απόδοση εμπιστοσύνης. Οι αυθόρμητες αυτές CA μπορούν να λειτουργούν με διάφορους τρόπους.

Σε μια κατερχόμενη ιεραρχία, όλοι οι χρήστες πρέπει να χρησιμοποιούν την CA του ανώτατου επιπέδου σαν την root CA. Το γεγονός αυτό σημαίνει ότι όλοι οι χρήστες χρειάζονται το δημόσιο κλειδί της CA, του ανωτάτου επιπέδου, πριν να αρχίσουν να χρησιμοποιούν την PKI.

Μια γενική ιεραρχία επιτρέπει σε κάθε CA, να είναι η root CA. Αυτή η δομή βασίζεται αρκετά στις CA του ανωτάτου επιπέδου, αφού μεγάλες διαδρομές πιστοποίησης στην γενική ιεραρχία μπορεί να γίνουν πολύ μεγάλες.

Σε γενικές γραμμές οι οντότητες που βρίσκονται σε επικοινωνία και συμμετέχουν σε μια ιεραρχική δομή, στα πλαίσια όμως της Υποδομής Δημόσιου Κλειδιού, είναι:

- **Η αρχή έγκρισης πολιτικής (PPA).** Η αρχή αυτή:

- Θέτει τις αρχές που θα ακολουθούν τα PCAs, τα οποία βρίσκονται πιο κάτω στην ιεραρχία.
- Εγκρίνει τις πολιτικές των PCAs.
- Εκδίδει πιστοποιητικά για PCAs.
- Εκδίδει ακόμη πιστοποιητικά ρίζας (root certificates) που τα υπογράφει ψηφιακά με το ιδιωτικό κλειδί της. Η έκδοση αυτών των πιστοποιητικών γίνεται off-line.

- **Η αρχή πιστοποίησης πολιτικής (PCA).** Η αρχή αυτή:

- Θέτει την πολιτική που θα ακολουθείται από τις CA, οι οποίες βρίσκονται στα χαμηλά επίπεδα ιεραρχίας, και επίσης ελέγχει αν λειτουργούν σύμφωνα με αυτή.
- Εκδίδει πιστοποιητικά για CA, όχι όμως για τελικούς χρήστες. Η έκδοση αυτών των πιστοποιητικών γίνεται off-line.

- Επειδή η περίοδος ισχύος των PCA πιστοποιητικών είναι πιο μεγάλη από την περίοδο ισχύος των CA πιστοποιητικών, η ανανέωση της ισχύος των CA πιστοποιητικών δεν δημιουργεί πρόβλημα στους τελικούς χρήστες, οι οποίοι έχουν αυτά τα πιστοποιητικά.
 - Θέτει την αρχή έκδοσης πιστοποιητικών.
 - Ακολουθεί την πολιτική που έχει ορίσει η PCA και εκδίδει πιστοποιητικά για άλλες CA, για τελικούς χρήστες και για αρχές καταχώρησης (RA).
 - Μερικές φορές θέτει και δικές της πολιτικές, οι οποίες όμως είναι σύμφωνες με τις πολιτικές της PCA.
- **Η αρχή καταχώρησης (RA)**, αυτή η αρχή:
 - Είναι υπεύθυνη για την διαδικασία εγγραφής των τελικών χρηστών, οι οποίοι θα ανακτήσουν πιστοποιητικά της CA. Δεν εκδίδει η ίδια πιστοποιητικά.
 - Ελέγχει τις πληροφορίες ταυτότητας που δηλώνουν οι τελικοί χρήστες, σύμφωνα με τις διαδικασίες τις οποίες έχει ορίσει η CA.
 - **Ο τελικός χρήστης (end entity)**: Ο τελικός χρήστης μπορεί να είναι κάποιος ιδιώτης ή μια επιχείρηση ή ένας υπολογιστής ή τέλος κάθε οντότητα η οποία χρησιμοποιεί το πιστοποιητικό.

6.3 Υποδομή Δημόσιου Κλειδιού (PKI)

Το πρόβλημα που δημιουργείται στην κρυπτογραφία δημόσιου κλειδιού, είναι ότι ο κάτοχος ενός δημόσιου και ενός ιδιωτικού κλειδιού δεν μπορεί να αποδείξει στον καθένα με τον οποίο συναλλάσσεται, ότι το δημόσιο κλειδί που χρησιμοποιεί ανήκει πράγματι σε αυτόν και δεν το έχει υποκλέψει από κάποιον τον οποίο υποδύεται με σκοπό να έχει κάποια οφέλη. Για τον λόγο αυτό χρειάζεται να υπάρχει μια οργανωμένη υποδομή η οποία να είναι τέτοια ώστε να μπορεί να ασχοληθεί με θέματα έκδοσης, διανομής, ακύρωσης, πιστοποίησης κλπ των κλειδιών που χρησιμοποιούν οι επικοινωνούντες χρήστες. Αυτή η υποδομή είναι γνωστή σαν Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure-PKI) και ολοκληρώνει την κρυπτογραφία δημόσιου κλειδιού, παρέχοντας ψηφιακά πιστοποιητικά καθώς και τις αρχές πιστοποίησης, προκειμένου να γίνεται επαλήθευση της ταυτότητας επικοινωνούντων οντοτήτων.

Μια PKI είναι ένας συνδυασμός από λογισμικές τεχνολογίες κρυπτογράφησης και υπηρεσίες, με τέτοιον τρόπο ώστε να διασφαλίζονται οι επικοινωνίες και οι συναλλαγές στο Ίντερνετ. Ακόμη με τις PKI επιτυγχάνεται η διασφάλιση των αρχών ασφάλειας στην μετάδοση πληροφοριών ή δεδομένων, οι οποίες αρχές είναι η εμπιστευτικότητα, η ακεραιότητα, η ταυτοποίηση και η μη αποκρήρυξη ευθύνης. Για να μπορέσει μια PKI να πετύχει όλα αυτά που αναφέρθηκαν προηγουμένως, θα πρέπει να ενσωματώνει τουλάχιστον μία Αρχή Έκδοσης Πιστοποιητικών, όπως και τα εργαλεία με τα οποία θα μπορεί να γίνει διαχείριση, ανανέωση ή ακόμη και ανάκληση πιστοποιητικών.

6.3.1 Συστατικά Μέρη της Υποδομής Δημόσιου Κλειδιού

Μια PKI προσφέρει υπηρεσίες ασφάλειας, που απαιτούνται για την ολοκλήρωση ηλεκτρονικών συναλλαγών μεταξύ οντοτήτων οι οποίες δεν γνωρίζονται μεταξύ τους και φυσικό είναι να θέλουν ασφαλείς επικοινωνίες. Για τον λόγο αυτό βασίζονται στην χρήση ψηφιακών πιστοποιητικών, τα οποία είναι αποκλειστικά υπεύθυνα να συνδέσουν τις ψηφιακές υπογραφές των χρηστών με τα δημόσια κλειδιά τους.

Αυτά τα οποία πρέπει να περιλαμβάνει μια PKI είναι:

Μια **πολιτική ασφάλειας**: η οποία ορίζει τι πρέπει να ακολουθείται για να εξασφαλίζεται η ασφάλεια των πληροφοριών από τη μια μεριά και τους κανόνες κρυπτογράφησης από την άλλη. Ειδικότερα δίνει οδηγίες για την χρήση των κλειδιών, των πληροφοριών οι οποίες είναι σημαντικές και τέλος ορίζει τα επίπεδα ελέγχου ανάλογα με την σημαντικότητα των πληροφοριών. Όλα αυτά αναφέρονται σε μια δήλωση πρακτικής πιστοποίησης (CPS), που είναι ένα έγγραφο, το οποίο περιέχει όλες τις διαδικασίες που πρέπει να ακολουθούνται, ώστε να εφαρμόζεται η πολιτική ασφάλειας στην πράξη.

Η πολιτική ασφάλειας περιλαμβάνει τα ακόλουθα:

- πώς είναι κατασκευασμένα και πώς λειτουργούν τα πιστοποιητικά πιστοποίησης ταυτοτήτων.
- πώς δημιουργούνται και ανακαλούνται τα πιστοποιητικά, καθώς και το πώς αποθηκεύονται και γίνονται διαθέσιμα στους χρήστες.

Μια **αρχή πιστοποίησης**: η οποία είναι το βασικό συστατικό μιας PKI, και η οποία διαχειρίζεται τα πιστοποιητικά για τα δημόσια κλειδιά για όλη την διάρκεια ζωής τους.

Οι βασικές λειτουργίες της είναι:

- η δημιουργία πιστοποιητικών που συνδέουν την ταυτότητα του χρήστη ή ενός συστήματος με ένα δημόσιο κλειδί, με την βοήθεια ψηφιακών υπογραφών.
- ο προγραμματισμός των ημερομηνιών λήξης των πιστοποιητικών.
- η διασφάλιση για την ανάκληση των πιστοποιητικών όταν είναι απαραίτητο, με την δημοσίευση των λιστών ανάκλησης πιστοποιητικών (CRL).

Κάθε οργανισμός ο οποίος ορίζει τη δική του PKI, μπορεί να ορίσει ένα δικό του πιστοποιητικό. Οι λίστες ανάκλησης πιστοποιητικών περιέχουν πιστοποιητικά που έχουν ακυρωθεί πριν την ημερομηνία λήξης. Οι λόγοι για τους οποίους ανακαλείται κάποιο πιστοποιητικό είναι π.χ. το κλειδί που ορίζεται από το πιστοποιητικό να μην είναι ασφαλές ή το άτομο για το οποίο εκδόθηκε να μην έχει δικαιοδοσία να το χρησιμοποιήσει. Όταν γίνεται η επαλήθευση μιας υπογραφής, θα πρέπει ο κάθε χρήστης να συμβουλευτεί μια λίστα ανάκλησης πιστοποιητικών, ώστε να διαπιστωθεί αν το εν λόγω πιστοποιητικό δεν έχει αποσυρθεί. Οι λίστες ανάκλησης διατηρούνται και ανανεώνονται από τις αρχές πιστοποίησης, οι οποίες διαχειρίζονται και παρέχουν πληροφορίες από αυτές τις λίστες, όσο αφορά τα πιστοποιητικά που ανακλήθηκαν και είχαν εκδοθεί από την ίδια.

Μια **αρχή καταχώρησης (RA)**: η οποία παρέχει την διεπαφή μεταξύ ενός χρήστη και της αρχής πιστοποίησής του. Αυτή είναι υπεύθυνη για την πιστοποίηση της ταυτότητας του κάθε χρήστη και μεταφέρει στην αρχή πιστοποίησης όλες τις αιτήσεις που είναι έτοιμες να δημιουργήσουν τα αντίστοιχα πιστοποιητικά.

Ένα **σύστημα διανομής ψηφιακών πιστοποιητικών**: η διανομή των πιστοποιητικών γίνεται με πολλούς τρόπους και εξαρτάται από την δομή του PKI. Θα μπορούσε, υπεύθυνοι για την διανομή των πιστοποιητικών να είναι οι ίδιοι οι χρήστες ή διαφορετικά να γίνονται μέσα από μια υπηρεσία καταλόγου. Όταν μια αρχή πιστοποίησης εκδώσει κάποιο πιστοποιητικό το αποθηκεύει άμεσα σε μία αποθήκη πιστοποιητικών. Έτσι λοιπόν όταν κάποιος θέλει κάποια πληροφορία που αφορά ένα πιστοποιητικό το οποίο υπάρχει στην εν λόγω αποθήκη, μπορεί να την πάρει χωρίς να είναι απαραίτητο να το ζητήσει από τον κάτοχό του.

6.3.2 Υπηρεσίες Υποδομής Δημόσιου Κλειδιού

Υπηρεσίες κρυπτογράφησης: μια PKI πρέπει να μπορεί να παρέχει, όποτε και αν της ζητηθεί, υπηρεσίες κρυπτογράφησης. Τέτοιες υπηρεσίες είναι, η δημιουργία ζευγών των κλειδιών κρυπτογράφησης, η δημιουργία ψηφιακών υπογραφών και η επιβεβαίωση της εγκυρότητας των ψηφιακών υπογραφών.

Υπηρεσίες διαχείρισης πιστοποιητικών: αποτελούν τον πυρήνα μιας PKI. Τέτοιες υπηρεσίες είναι η έκδοση, η ανάκληση, η δημοσίευση και η αρχειοθέτηση πιστοποιητικών.

Βοηθητικές υπηρεσίες: υπάρχουν και άλλες όμως υπηρεσίες που είναι βασικά μέρη μιας τέτοιας υποδομής, όπως:

- **Η καταχώρηση:** μια υπηρεσία καταχώρησης είναι υπεύθυνη για την αναγνώριση και την διαχείριση των προσωπικών δεδομένων του καθένα που ζητάει ένα πιστοποιητικό. Μετά τον έλεγχο μπορεί να γίνει η έκδοση του ψηφιακού πιστοποιητικού.
- **Η αρχειοθέτηση δεδομένων:** οι υπηρεσίες αυτές αναλαμβάνουν την αρχειοθέτηση και την διαχείριση των ψηφιακών εγγράφων και των υπόλοιπων δεδομένων για μεγάλες χρονικές περιόδους. Επιπλέον φροντίζουν για την ασφαλή αποθήκευσή τους σε διάφορα μέσα.
- **Συμβολαιογραφική αυθεντικοποίηση:** αφορά την ταυτοποίηση του αποστολέα και την ακεραιότητα των ψηφιακών εγγράφων.
- **Ανάκτηση κλειδιού:** η υπηρεσία αυτή ασχολείται με την δημιουργία κρυφών αντιγράφων των κλειδιών, για τις περιπτώσεις που κάποιος χρήστης χάσει το κλειδί του ή ξεχάσει το συνθηματικό με το οποίο μπορεί να έχει πρόσβαση.
- **Αρχείο προσωπικών δεδομένων:** ασχολούνται με την διαχείριση δεδομένων που αφορούν τον κάθε χρήστη. Τα δεδομένα αυτά περιλαμβάνουν, εκτός από το ίδιο το πιστοποιητικό, και άλλα, όπως το τηλέφωνό του, την διεύθυνσή του κλπ.
- **Άλλες υπηρεσίες:** αν πχ, ένα κλειδί αποθηκεύεται σε μια έξυπνη κάρτα, τότε χρειάζονται επιπλέον υπηρεσίες για την δημιουργία των κλειδιών και την εγγραφή τους στην κάρτα.

6.4 Ψηφιακά Πιστοποιητικά

6.4.1 Γενικά

Τα πιστοποιητικά είναι κάποια έγγραφα που είναι ψηφιακά και τα οποία αποδεικνύουν τη σχέση που θα πρέπει να υπάρχει μεταξύ ενός δημόσιου κλειδιού και ενός χρήστη. Αυτά τα έγγραφα επιτρέπουν να γίνει η επαλήθευση ότι κάποιο δημόσιο κλειδί ανήκει σε έναν συγκεκριμένο χρήστη, γιατί έτσι αποτρέπεται κάποιος να υποδυθεί άλλον που χρησιμοποιεί ένα ψεύτικο κλειδί.

Το κάθε πιστοποιητικό δίνει τις παρακάτω πληροφορίες:

- το όνομα του κατόχου,
- το όνομα του εκδοτικού οργανισμού της CA,
- το δημόσιο κλειδί του ονόματος που αναγράφεται στο πιστοποιητικό,
- την ημερομηνία λήξης του πιστοποιητικού,
- τον σειριακό αριθμό,

- την ψηφιακή υπογραφή του εκδοτικού οργανισμού.

Η τυποποιημένη τώρα μορφή ενός πιστοποιητικού ακολουθεί το πρωτόκολλο X 509. Το πιστοποιητικό μεταφέρεται, συνήθως, μαζί με την ψηφιακή υπογραφή. Για να μπορεί όμως να επαληθευθεί η ψηφιακή υπογραφή, θα πρέπει ο παραλήπτης να έχει το σωστό δημόσιο κλειδί του αποστολέα. Το πιστοποιητικό δεν χρειάζεται να αποστέλλεται κάθε φορά που ξεκινά μια συναλλαγή, αρκεί όμως να σταλεί μια φορά κατά την έναρξη της σύνδεσης.

6.4.2 Είδη Πιστοποιητικών

Υπάρχουν τέσσερις διαφορετικοί τύποι ψηφιακών πιστοποιητικών για την χρήση στο internet:

Πιστοποιητικά Αρχών Πιστοποίησης

Αυτά είναι πιστοποιητικά τα οποία περιλαμβάνουν το όνομα και το δημόσιο κλειδί της αρχής πιστοποίησης και μπορούν να υπογραφούν από μόνα τους. Αυτό σημαίνει ότι η αρχή πιστοποίησης μας λέει ότι το κλειδί της είναι καλό και πρέπει να το εμπιστευτούμε. Διαφορετικά, τα πιστοποιητικά μπορούν να υπογραφούν από μια άλλη αρχή. Τα πιστοποιητικά αυτά διανέμονται με την προοπτική να τα εμπιστευτούμε όπως είναι, και αυτό φαίνεται από το γεγονός ότι ενσωματώνονται απευθείας στους web browsers.

Πιστοποιητικά server

Κάθε SSL server πρέπει να έχει ένα SSL πιστοποιητικό server. Όταν ένας browser συνδέεται σε ένα web server χρησιμοποιώντας το SSL πρωτόκολλο, ο server στέλνει στον browser το δημόσιο κλειδί του σε ένα X 509 v3 πιστοποιητικό. Το πιστοποιητικό χρησιμεύει για να αποδείξει την ταυτότητα του server και για να διανέμει το δημόσιο κλειδί του server, το οποίο χρησιμοποιείται για να κρυπτογραφήσει την αρχική πληροφορία που στέλνεται στον server από τον client.

Προσωπικά πιστοποιητικά

Αυτά περιλαμβάνουν το όνομα ενός ατόμου και το δημόσιο κλειδί του. Επίσης μπορούν να έχουν και άλλες πληροφορίες, όπως την ηλεκτρονική διεύθυνση του ατόμου, την ταχυδρομική του διεύθυνση ή οτιδήποτε άλλο.

Πιστοποιητικά εκδοτών λογισμικού

Χρησιμοποιούνται για να υπογράφουν προγράμματα που πρόκειται να διανεμηθούν.

6.4.3 Απόκτηση Πιστοποιητικών για έναν Server

Για να αποκτηθεί ένα πιστοποιητικό για τον server μας, θα χρειαστεί να ακολουθηθούν τα παρακάτω βήματα:

- δημιουργία ενός RSA ζεύγους κλειδιών, δημόσιου και ιδιωτικού, χρησιμοποιώντας ένα πρόγραμμα που θα προμηθευτούμε από τον πωλητή του server.
- αποστολή του δημόσιου κλειδιού, το διακεκριμένο καθώς και το κοινό όνομα στην CA που επιθυμούμε να χρησιμοποιήσουμε. Η αποστολή αυτή γίνεται με την χρήση email.

- θα πρέπει να ακολουθήσουμε την διαδικασία πιστοποίησης της CA. Συμπλήρωση διάφορων στοιχείων στο site της CA, αποστολή εγγράφων με email-fax ή και με ηλεκτρονικό ταχυδρομείο.
- αναμονή για την επεξεργασία της αίτησης από την CA.
- όταν η CA πειστεί ότι η αίτηση πληροί τις προϋποθέσεις, θα εκδώσει ένα πιστοποιητικό αποτελούμενο από το δημόσιο κλειδί και το διακεκριμένο όνομά μας, άλλες πληροφορίες και την ψηφιακή υπογραφή του. Η αποστολή της αίτησης γίνεται με την χρήση email.
- εγκατάσταση του κλειδιού χρησιμοποιώντας ένα πρόγραμμα που θα το προμηθευτούμε από τον πωλητή του server.

Βέβαια τα X 509 v3 πιστοποιητικά, κάποια στιγμή λήγουν και χρειάζονται την κατάλληλη ανανέωση, η οποία εκτελείται από τις CA. Η ημερομηνία λήξης είναι από 3 έως 12 μήνες, για λόγους ασφαλείας.

6.4.4 Ψηφιακά πιστοποιητικά από την μεριά του χρήστη

Πιστοποιητικά Πελάτη (Client)

Τα client πιστοποιητικά, είναι ψηφιακά πιστοποιητικά που είναι σχεδιασμένα για να πιστοποιούν την ταυτότητα κάποιου ατόμου. Τα client πιστοποιητικά συνδέουν ένα συγκεκριμένο μυστικό κλειδί και εκδίδονται από τις CAs Αρχές Πιστοποίησης. Αυτά τα πιστοποιητικά έχουν πολλές χρήσεις και οφέλη:

- μπορούν να απομακρύνουν την ανάγκη απομνημόνευσης των usernames και passwords
- οι οργανισμοί μπορούν να χρησιμοποιήσουν ένα πιστοποιητικό που έχει εκδοθεί από μια ειδική CA, σαν απόδειξη της ταυτότητάς τους
- είναι πιο εύκολο μια ομάδα ανθρώπων να μοιραστούν ένα ζεύγος username-password παρά ένα ψηφιακό ID. Αυτό γίνεται επειδή η υπογραφή του ονόματός μας απαιτεί πρόσβαση σε ένα μυστικό κλειδί.
- επειδή τα ψηφιακά πιστοποιητικά παρέχουν ένα δημόσιο κλειδί, εμείς μπορούμε να χρησιμοποιήσουμε το ψηφιακό πιστοποιητικό κάποιου για να του στείλουμε κρυπτογραφημένο email.
- τα πιστοποιητικά που δείχνουν την ηλικία ενός προσώπου, μπορούν να χρησιμοποιηθούν για περιορισμούς σε πονηρού περιεχομένου δεδομένα ή και chat groups
- αυτά που δείχνουν το φύλο ενός προσώπου, μπορούν να χρησιμοποιηθούν για ελεύθερη πρόσβαση σε χώρους μόνο για άνδρες ή μόνο για γυναίκες

Τα πιστοποιητικά βοηθούν για την αναγνώριση της ταυτότητας των χρηστών, και την αντιμετώπιση της ανωνυμίας. Επειδή ελαχιστοποιούν την ανωνυμία πολλοί είναι αντίθετοι με την χρήση τους, όμως δεν στέλνονται ποτέ από έναν web browser χωρίς την γνώση και την άδεια του χρήστη.

Υποστήριξη για Client-Side ψηφιακά πιστοποιητικά

Τα client-side ψηφιακά πιστοποιητικά υποστηρίζονται από τον Internet Explorer, τον Netscape Navigator, και άλλες εφαρμογές βασισμένες στο SSL. Η υποστήριξη αποτελείται από τέσσερα συστατικά κλειδιά:

- δημιουργία κλειδιού,
- απόκτηση πιστοποιητικού,
- κλήση/ανταπόκριση,
- ασφαλής αποθήκευση

Ανάκτηση ψηφιακών πιστοποιητικών/ Υπογραφής

Για να γίνει αυτό θα πρέπει να ακολουθήσουμε τις εξής ενέργειες:

- επισκεπτόμαστε έναν από τους γνωστούς τόπους (site) παροχής πιστοποιητικών
- συμπληρώνουμε την on line φόρμα εγγραφής και υποβάλλουμε ηλεκτρονικά το αίτημά μας, για την παροχή ενός πιστοποιητικού
- λαμβάνουμε ένα μήνυμα που περιλαμβάνει έναν σύνδεσμο (link) για το αυτόματο κατέβασμα του πιστοποιητικού
- εξάγουμε την ψηφιακή υπογραφή μας την οποία και αποθηκεύουμε σε μία συσκευή αποθήκευσης.
- χρησιμοποιούμε τη συσκευή αποθήκευσης για να εισάγουμε την ψηφιακή υπογραφή μας σε άλλους υπολογιστές στο σπίτι ή σε φορητό Η/Υ.

6.4.5 Ψηφιακές Υπογραφές

Ένας εύκολος, αποδοτικός καθώς και ένας ασφαλής τρόπος υπογραφής ηλεκτρονικών εγγράφων, είναι οι ψηφιακές υπογραφές. Στην ουσία οι ψηφιακές υπογραφές είναι ψηφιακά δεδομένα τα οποία βρίσκονται μαζί με άλλα ηλεκτρονικά δεδομένα σε μια λογική συσχέτιση και αποδεικνύουν έτσι την γνησιότητά τους.

Οι ψηφιακές υπογραφές, για να υλοποιηθούν, χρησιμοποιούν την κρυπτογραφία δημόσιου κλειδιού. Ο κάθε χρήστης έχει δύο κλειδιά, που σχετίζονται με μια μαθηματική σχέση μεταξύ τους. Με το ένα κλειδί δημιουργεί την υπογραφή και με το άλλο κάνει την επαλήθευσή της. Οι ψηφιακές υπογραφές διαφέρουν από την κρυπτογράφηση, στο γεγονός ότι για να δημιουργηθεί η υπογραφή ο αποστολέας κάνει χρήση του ιδιωτικού του κλειδιού, ενώ για να κάνει την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιό κλειδί του αποστολέα.

Στην διαδικασία για την δημιουργία καθώς και για την επαλήθευση μιας ψηφιακής υπογραφής, μπαίνει και η έννοια της συνάρτησης κατακερματισμού. Αφού εφαρμοστεί αυτή η συνάρτηση, από ένα ανεξαρτήτου μεγέθους μήνυμα, παράγεται η σύνοψη του μηνύματος, η οποία είναι μια σειρά από bits που έχουν ένα συγκεκριμένο μέγεθος (π.χ. 128 ή 160 bits κλπ). Η σύνοψη του κάθε μηνύματος είναι μοναδική και το αντιπροσωπεύει.

Ας σημειωθεί ότι μια συνάρτηση κατακερματισμού είναι μονόδρομη, διότι από την σύνοψη ενός μηνύματος, την οποία δημιουργεί, είναι σχεδόν αδύνατο υπολογιστικά κάποιος να βγάλει το αρχικό

μήνυμα. Ακόμη υπάρχει πολύ μικρή πιθανότητα δύο μηνύματα να τύχει να έχουν την ίδια σύνοψη και τέλος η κάθε αλλαγή σε κάποιο μήνυμα σημαίνει ότι δημιουργείται και διαφορετική σύνοψη.

Ηλεκτρονική υπογραφή είναι λοιπόν μία σύνοψη ενός μηνύματος από την πλευρά του αποστολέα, η οποία μάλιστα έχει υποστεί κρυπτογράφηση με το ιδιωτικό κλειδί του. Να θεωρηθεί ότι ο αποστολέας ενός μηνύματος, έχει κάποιο συγκεκριμένο ζεύγος κλειδιών και το ιδιωτικό το κατέχει πλήρως. Ακολούθως ο αποστολέας χρησιμοποιώντας το ιδιωτικό του κλειδί, για να κρυπτογραφήσει το μήνυμα, πιστοποιεί στον παραλήπτη, (ο οποίος κάνει αποκρυπτογράφηση με το αντίστοιχο δημόσιο κλειδί του αποστολέα), την ταυτότητά του. Είναι δηλαδή η ψηφιακή υπογραφή ένας τρόπος με τον οποίο πιστοποιείται η ταυτότητα του αποστολέα κάποιου μηνύματος.

Για να δημιουργηθεί μια υπογραφή ο κάθε αποστολέας μηνυμάτων θα πρέπει κάνει τις ενέργειες που ακολουθούν:

- Χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού, δημιουργεί την σύνοψη του μηνύματος που θέλει να στείλει. Αυτό που θα παραχθεί θα είναι μια συγκεκριμένου μήκους σειρά ψηφίων.
- Χρησιμοποιεί το ιδιωτικό κλειδί του για να κρυπτογραφήσει το αποτέλεσμα που προέκυψε από την εφαρμογή της συνάρτησης κατακερματισμού και έτσι δημιουργεί την ψηφιακή υπογραφή του μηνύματος.
- Το αρχικό μήνυμα κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη και μαζί με την ψηφιακή υπογραφή αποστέλλεται στον επιθυμητό παραλήπτη.

Ο παραλήπτης τώρα για να επιβεβαιώσει την ακεραιότητα του μηνύματος και την ταυτότητα του αποστολέα κάνει τις παρακάτω ενέργειες:

- Χρησιμοποιεί το δημόσιο κλειδί του αποστολέα, ώστε να αποκρυπτογραφήσει την ψηφιακή υπογραφή που βρίσκεται στα ηλεκτρονικά δεδομένα του μηνύματος. Έτσι αποκαλύπτει την τιμή της σύνοψης.
- Αν το μήνυμα είχε κρυπτογραφηθεί, τότε χρησιμοποιεί το ιδιωτικό κλειδί για να το αποκρυπτογραφήσει.
- Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, δημιουργεί την σύνοψη του μηνύματος. Αν τώρα οι τιμές των δύο συνόψεων είναι ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι αχέραιο.

Κεφάλαιο 7

PGP (Pretty Good Privacy)

7.1 Εισαγωγή

Ένα από τα συστήματα κρυπτογράφησης δημόσιου κλειδιού είναι το PGP Pretty Good Privacy που το έτος 1991 αναπτύχθηκε στις Ηνωμένες πολιτείες Αμερικής από τον ερευνητή Phil Zimmerman. Κάποια στιγμή, μετά από την χαλάρωση των περιορισμών που υπήρχαν στις ΗΠΑ, μπορούσε να εξαχθεί πλέον το PGP και σε ηλεκτρονική μορφή. Παρόλα αυτά όμως το project PGPi, συνέχισε να έχει τον απόλυτο έλεγχο της διακίνησης και της διανομής των διάφορων εκδόσεων αυτού του προγράμματος, μαζί με τον πηγαίο κώδικα, σε όλο τον κόσμο.

Το PGP, όταν πρόκειται για προσωπική χρήση, διατίθεται δωρεάν, ενώ όταν πρόκειται να εκτελεστούν συναλλαγές, χρειάζεται κάποια άδεια, ώστε να μπορεί να χρησιμοποιηθεί. Ο σκοπός του PGP ήταν να χρησιμοποιηθεί, σε συνδυασμό με το σύστημα που γίνονται επικοινωνίες μέσω του ηλεκτρονικού ταχυδρομείου, το οποίο προϋπήρχε και το οποίο συμβαίνει να είναι συμβατό με κάθε πλατφόρμα, και το μόνο που μένει είναι να υπάρξει προστασία για τις πληροφορίες ή τα δεδομένα που διακινούνται μέσω του Ίντερνετ, δηλαδή να είναι εξασφαλισμένο ότι αυτά πιθανόν να παρακολουθούνται και για τον λόγο αυτό, θα πρέπει να είναι ακατανόητα, σε όλους πέραν αυτών που είναι οι νόμιμοι παραλήπτες τους. Αυτό επιτυγχάνεται μόνο με ισχυρή κρυπτογράφηση τους, ώστε κανείς κακόβουλος να μην μπορεί να τα υποκλέψει.

7.2 Συστατικά στοιχεία του PGP

Το PGP αποτελείται από τέσσερα στοιχεία κρυπτογράφησης και έναν αριθμό συστατικών μερών λογισμικού, συμβατών μεταξύ τους. Ο πυρήνας των μηχανισμών ασφάλειας είναι:

- Ο αλγόριθμος κρυπτογράφησης δεδομένων IDEA.
- Το σύστημα κρυπτογράφησης δημόσιου κλειδιού RSA για την διαχείριση κλειδιών.
- Η συνάρτηση κατακερματισμού MD5.
- Η γεννήτρια τυχαίων αριθμών.

Τα άλλα συστατικά του PGP υλοποιούν τυπικές λειτουργίες όπως π.χ την αλληλεπίδραση με το χρήστη, τη διαχείριση αρχείων και τη συμπίεση των δεδομένων.

7.3 Η γεννήτρια Τυχαίων Αριθμών

Η γεννήτρια των Τυχαίων Αριθμών είναι ένα από τα συστατικά που έχει το PGP και το οποίο χρησιμοποιείται για να δημιουργηθεί ένα τυχαίο και επιλεγμένο κλειδί συνόδου, που χρησιμοποιείται για να εκτελεστεί η κρυπτογράφηση μηνυμάτων με την βοήθεια του αλγορίθμου IDEA. Έστω τώρα ότι κάποιος επιτιθέμενος αποκτά ένα κλειδί τέτοιας μορφής, το μόνο που θα μπορεί να κάνει είναι να το χρησιμοποιήσει μόνο για ανάγνωση του μηνύματος.

Η γεννήτρια αυτού του είδους παρουσιάζει αρκετές διαφορές σε σχέση με τις γεννήτριες που έχουν την κλασική μορφή. Στις γεννήτριες τυχαίων αριθμών απαιτείται περισσότερος χρόνος για την παραγωγή τυχαίου αριθμού, ο οποίος μπορεί να προβλεφθεί. Οι κλασικές γεννήτριες παράγουν γνωστές ακολουθίες τυχαίων αριθμών, και είναι εύκολο να συμπεράνει κανείς την εσωτερική κατάσταση τους όταν εξεταστεί μια μικρή ακολουθία αριθμών στην έξοδο. Άρα για να είναι δυνατή η αντιμετώπιση τέτοιας μορφής επιθέσεων, το PGP συγκεντρώνει όλους τους χρόνους άφιξης δύο χαρακτήρων, οι οποίοι είναι διαδοχικοί, και πληκτρολογούνται σε αυτό. Η απόσταση που υπάρχει ανάμεσα σε αυτούς τους δύο χρόνους άφιξης των δύο χαρακτήρων, έχει έναν τυχαίο παράγοντα που είναι εύκολο να προβλεφθεί. Κατόπιν το κομμάτι το οποίο είναι απρόβλεπτο, υπόκειται σε φιλτράρισμα και ύστερα χρησιμοποιείται στην ανατροφοδότηση της γεννήτριας. Στην συνέχεια αυτοί οι τυχαίοι αριθμοί χρησιμοποιούνται σαν κλειδιά συνόδου ή σε άλλες χρήσεις οι οποίες είναι παρόμοιες.

7.4 Η Λειτουργία του PGP

Θεωρούμε ότι ένας χρήστης A θέλει να στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου P, στον B. Οι δυο χρήστες έχουν τα δικά τους ιδιωτικά (D_x) και δημόσια (E_x) κλειδιά RSA και θεωρούμε ότι ο ένας γνωρίζει το δημόσιο κλειδί του άλλου.

- Αρχικά το πρόγραμμα PGP στον υπολογιστή του A περνάει το μήνυμα P, από την συνάρτηση κατακερματισμού MD5.
- Μετά το hash κρυπτογραφείται με το ιδιωτικό κλειδί RSA του A, D_A . Όταν ο B τελικά πάρει το μήνυμα, τότε θα μπορέσει να αποκρυπτογραφήσει το hash με το δημόσιο κλειδί E_A , και να επιβεβαιώσει ότι είναι το σωστό.
- Μετά το κρυπτογραφημένο hash και το αρχικό μήνυμα διατάσσονται σε ένα νέο μήνυμα PI και συμπιέζονται ώστε να παραχθεί το PI.ZIP.
- Στην συνέχεια παράγεται τυχαία ένα κλειδί K_M για τον αλγόριθμο IDEA, και το οποίο ισχύει μόνο για την συγκεκριμένη αποστολή ηλεκτρονικού ταχυδρομείου. Το κλειδί αυτό χρησιμοποιείται για την κρυπτογράφηση με το PI.ZIP με το IDEA.
- Επιπλέον το κλειδί κρυπτογραφείται με το δημόσιο κλειδί του B.
- Τα δύο αυτά τμήματα διατάσσονται και αποστέλλονται στο δίκτυο.
- Όταν ο B πάρει το μήνυμα, αποκρυπτογραφεί το κλειδί K_M , χρησιμοποιώντας το ιδιωτικό κλειδί RSA (D_B).
- Χρησιμοποιώντας το K_M αποκρυπτογραφεί το μήνυμα που είναι κρυπτογραφημένο με τον αλγόριθμο IDEA και λαμβάνει το PI.ZIP.

- Μετά την αποσυμπίεση ο Β ξεχωρίζει το hash από το καθαρό μήνυμα και το αποκρυπτογραφεί χρησιμοποιώντας το δημόσιο κλειδί του Α.
- Αν το hash συμφωνεί με τον υπολογισμό MD5 που εκτελεί ο ίδιος, τότε γνωρίζει ότι το μήνυμα είναι αυτό που έστειλε ο Α.

7.5 Τα χαρακτηριστικά του PGP

Εξακρίβωση γνησιότητας

Για να εξακριβωθεί η γνησιότητα ακολουθούνται τα ακόλουθα βήματα:

Πρώτα ο αποστολέας στέλνει το μήνυμα και μετά ο MD5 χρησιμοποιείται για να παράγει ένα 128-bit hash code μήνυμα, ο οποίος κώδικας στην συνέχεια κρυπτογραφείται χρησιμοποιώντας τον RSA και το ιδιωτικό κλειδί του αποστολέα, το δε αποτέλεσμα προσκολλάται στο μήνυμα.

Ακολούθως ο παραλήπτης χρησιμοποιεί με την σειρά τον RSA με το δημόσιο κλειδί του αποστολέα, για να αποκρυπτογραφήσει και να βρει τον hash code.

Τέλος ο παραλήπτης παράγει ένα νέο hash code για το μήνυμα και το συγκρίνει με το αποκρυπτογραφημένο hash code που έχει βρει. Αν ταιριάζουν, τότε δέχεται το μήνυμα σαν αυθεντικό.

Εμπιστευτικότητα

Αυτή παρέχεται με την κρυπτογράφηση των μηνυμάτων πριν σταλούν ή αποθηκευτούν σαν αρχεία. Και για τις δύο αυτές περιπτώσεις χρησιμοποιείται ο IDEA και πιο συγκεκριμένα η 64-bit cipher feedback mode του IDEA με πίνακα αρχικοποίησης όλα μηδέν.

Στο PGP κάθε συμβατικό κλειδί χρησιμοποιείται μόνο μια φορά, και άρα για κάθε μήνυμα παράγεται με τυχαίο τρόπο ένα κλειδί 128-bits. Για την προστασία του, το κλειδί αυτό πριν μεταδοθεί, κρυπτογραφείται με βάση το δημόσιο κλειδί του παραλήπτη. Η σειρά των γεγονότων έχει ως εξής:

Ο αποστολέας παράγει ένα μήνυμα και έναν τυχαίο 128-bit αριθμό, ο οποίος θα χρησιμοποιηθεί σαν session key μόνο για το μήνυμα αυτό. Μετά το μήνυμα κρυπτογραφείται με IDEA μαζί με το session key. Κατόπιν το session key κωδικοποιείται με RSA χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη και προσαρτάται στο μήνυμα. Τέλος ο παραλήπτης χρησιμοποιεί RSA με το δικό του ιδιωτικό κλειδί για να βρει το session key, το οποίο θα χρησιμοποιήσει ώστε να μπορέσει να αποκρυπτογραφήσει το μήνυμα. Το μέγεθος του κλειδιού που θα χρησιμοποιήσει ο RSA μπορεί να είναι 384,512 και 1024 bits.

Εμπιστευτικότητα και εξακρίβωση γνησιότητας

Όταν και οι δύο υπηρεσίες χρησιμοποιούνται, αρχικά, ο αποστολέας παράγει μια ηλεκτρονική υπογραφή, με βάση το ιδιωτικό κλειδί του, και την τοποθετεί στο τέλος του μηνύματος. Στην συνέχεια το μήνυμα μαζί με την υπογραφή κρυπτογραφείται χρησιμοποιώντας το IDEA και ένα session key. Το session key κρυπτογραφείται χρησιμοποιώντας τον RSA και το δημόσιο κλειδί του παραλήπτη.

Συμπίεση

Το PGP συμπιέζει από μόνο του το μήνυμα αφού τοποθετηθεί η υπογραφή και πριν κρυπτογραφηθεί. Έτσι κερδίζουμε χώρο και κατά την μετάδοση και κατά την αποθήκευση του μηνύματος. Ο αλγόριθμος που χρησιμοποιείται είναι ο ZIP.

Συμβατότητα ηλεκτρονικού ταχυδρομείου

Όταν χρησιμοποιείται PGP σε ολόκληρο ή μέρος του block που αποστέλλεται, είναι κρυπτογραφημένο και αποτελείται από μια σειρά από τυχαία 8-bit octets. Λόγω του περιορισμού που υπάρχει σε ορισμένα συστήματα ηλεκτρονικού ταχυδρομείου, για μόνο ASCII text μηνύματα, το PGP παρέχει μια υπηρεσία που μετατρέπει τη σειρά αυτή σε εκτυπώσιμους ASCII χαρακτήρες. Για τον σκοπό αυτό χρησιμοποιείται η radix-64 μετατροπή, την οποία παίρνει κάθε ομάδα τριών octets και τα μετατρέπει σε 4 χαρακτήρες ASCII, καθώς επίσης προσθέτει στο τέλος ένα CRC για την ανίχνευση λαθών. Το PGP επιπλέον, μπορεί να μετατρέπει, σε radix-64 μορφή, μόνο το μέρος όπου υπάρχει η υπογραφή, ώστε ο αποστολέας να μπορεί διαβάσει τα μηνύματα, χωρίς να χρησιμοποιεί PGP, και μόνο αν θέλει να πιστοποιήσει την υπογραφή να το χρησιμοποιεί.

Τμηματοποίηση και συναρμολόγηση

Το PGP μπορεί να υποδιαιρεί ένα μήνυμα που είναι πολύ μεγάλο, σε μικρότερα τμήματα, ώστε να γίνεται κατάλληλο για αποστολή και σε ορισμένες περιπτώσεις που το μέγεθος των μηνυμάτων, τα οποία μπορούν να αποσταλούν, είναι περιορισμένο. Η τμηματοποίηση γίνεται μετά από τις άλλες επεξεργασίες.

7.6 Αλυσίδες κλειδιών (Key Rings)

Όλα τα δημόσια κλειδιά θα πρέπει να κρατούνται και να φυλάσσονται σε ξεχωριστά πιστοποιητικά κλειδιών. Αυτά τα πιστοποιητικά περιλαμβάνουν την ταυτότητα του χρήστη στον οποίο ανήκουν, μια σφραγίδα με το χρόνο δημιουργίας του ζεύγους κλειδιών και τέλος το υλικό του κλειδιού. Το κάθε μυστικό κλειδί κρυπτογραφείται με τον κωδικό του, για τον κίνδυνο απώλειάς του. Ένα οποιοδήποτε αρχείο κλειδιών ή κάποια αλυσίδα από αυτά περιέχει ένα ή πιο πολλά πιστοποιητικά κλειδιών.

Τα κλειδιά έχουν από ένα key id το καθένα, που είναι μια συντομογραφία του δημόσιου κλειδιού. Για πολλά από τα κλειδιά υπάρχει η δυνατότητα να μοιράζονται το ίδιο user id, για λόγους πρακτικούς κυρίως, κανένα όμως δεν μοιράζεται με άλλο κλειδί το ίδιο key id.

Το PGP χρησιμοποιεί περιλήψεις μηνυμάτων ώστε να μπορεί να δημιουργήσει ψηφιακές υπογραφές. Η περιλήψη του κάθε μηνύματος, είναι κρυπτογραφικά μια πολύ ισχυρή και μονόδρομη συνάρτηση, των 128 bits του μηνύματος. Η ψηφιακή υπογραφή σχηματίζεται όταν η περιλήψη του μηνύματος κρυπτογραφηθεί με το μυστικό κλειδί.

Η χρήση του key id γίνεται από τον παραλήπτη, για να βρει το δημόσιο κλειδί του αποστολέα, έτσι ώστε να μπορεί να εκτελεί τους ελέγχους στις ψηφιακές υπογραφές. Το λογισμικό του παραλήπτη είναι αυτό το οποίο αναζητά με αυτόματο τρόπο το δημόσιο κλειδί του αποστολέα καθώς και το user id του, που είναι στο μπρελόκ των δημόσιων κλειδιών, τα οποία έχει στην κατοχή του ο παραλήπτης.

Αυτοί οι δύο τύποι μπρελόκ κλειδιών είναι η κύρια μέθοδος της αποθήκευσης και διαχείρισης των δημόσιων και ιδιωτικών κλειδιών.

7.7 Προστασία Δημόσιου Κλειδιού

Σε ένα κρυπτογραφικό σύστημα δημόσιου κλειδιού, δεν είναι αναγκαία η προστασία των δημόσιων κλειδιών, γιατί αυτό που επιδιώκεται είναι η όσο γίνεται μεγαλύτερη διάδοσή τους. Αυτό που πρέπει να διασφαλίζεται και είναι και αρκετά σημαντικό είναι ότι πρέπει οι χρήστες που επικοινωνούν να είναι σίγουροι ότι ένα δημόσιο κλειδί το οποίο φαίνεται να ανήκει σε κάποιον, πράγματι ανήκει σε

αυτόν. Αυτό είναι ένα από τα σημαντικά μειονεκτήματα του συστήματος κρυπτογράφησης δημόσιων κλειδιών.

Θα μπορούσε να οριστεί ένα άτομο, ευρείας εμπιστοσύνης, το οποίο να ειδικευτεί στο να παρέχει ψηφιακές υπογραφές στα πιστοποιητικά των δημόσιων κλειδιών που ανήκουν σε άλλους χρήστες. Αυτό το άτομο θα μπορούσε να είναι ένας key server ή κάποια υπηρεσία πιστοποίησης. Έτσι το οποιοδήποτε πιστοποιητικό δημόσιου κλειδιού το οποίο έχει την υπογραφή αυτού του key server, θα θεωρείται ότι είναι γνήσιο και άξιο εμπιστοσύνης.

Το πιο σπουδαίο και δύσκολο πρόβλημα στις εφαρμογές της κρυπτογράφησης δημόσιων κλειδιών, είναι η διαδικασία προστασίας αυτών των κλειδιών. Αυτό είναι και το αδύνατο σημείο της κρυπτογράφησης δημόσιων κλειδιών, και η προσπάθεια που καταβάλλεται για να αντιμετωπιστεί το πρόβλημα αυτό είναι αρκετά μεγάλη.

Το PGP κρατάει κάποια στοιχεία, και για τον λόγο αυτό γνωρίζει ποια από τα δημόσια κλειδιά που είναι στην κατοχή κάποιου χρήστη, είναι πιστοποιημένα με υπογραφές. Επίσης με το κλειδί του αυτός ο χρήστης πρέπει να πιστοποιήσει τα κλειδιά των άλλων. Το PGP αμέσως μετά αναλαμβάνει να κρίνει αυτομάτως αν κάποιο δημόσιο κλειδί είναι έγκυρο ή όχι. Θα πρέπει επιπροσθέτως να διασφαλιστεί ότι κανένας δεν υπάρχει περίπτωση να αλλοιώσει το μπρελόκ με τα κλειδιά. Το PGP μπορεί αυτόματα να εκτελέσει σύγκριση στο δημόσιο κλειδί απέναντι σε ένα αντίγραφο του σε κάποιο προστατευμένο φυσικό μέσο.

Άλλος τρόπος για την προστασία του μπρελόκ με τα κλειδιά είναι να υπογραφεί ψηφιακά ολόκληρο, με το μυστικό κλειδί κάποιου χρήστη. Θα πρέπει όμως να υπάρχει και κάπου αλλού προστατευμένο ένα αντίγραφο του δημόσιου κλειδιού του εν λόγω χρήστη, ώστε να μπορεί να κάνει έλεγχο στην υπογραφή του.

7.8 Διαδικασία αναγνώρισης έγκυρων κλειδιών

Το PGP θα πρέπει να παρακολουθεί συνεχώς ποια από τα κλειδιά του μπρελόκ είναι πιστοποιημένα και ποια όχι. Αυτά τα κλειδιά θα πρέπει να είναι υπογεγραμμένα από χρήστες για τους οποίους υπάρχει εμπιστοσύνη. Το μόνο το οποίο πρέπει να κάνει κάποιος χρήστης είναι να ρωτήσει το PGP για το ποιοι χρήστες είναι εμπιστοσύνης σαν μεσάζοντες και να πιστοποιήσει τα κλειδιά των άλλων με το δικό του κλειδί.

Το PGP αναλαμβάνει την υποχρέωση να ξεκινήσει αυτόματα τις διαδικασίες για έλεγχο στην εγκυρότητα των κλειδιών, τα οποία είναι υπογεγραμμένα από τους μεσάζοντες που έχουν οριστεί από κάποιον χρήστη. Μπορεί βέβαια να υπογράψει και ο ίδιος κλειδιά.

Υπάρχουν δύο κριτήρια με βάση τα οποία το PGP κρίνει την χρησιμότητα των κλειδιών και για τα οποία δεν πρέπει να υπάρχει σύγχυση:

- Το κλειδί ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει.
- Το κλειδί ανήκει σε κάποιον που μπορούμε να εμπιστευτούμε για την πιστοποίηση άλλων κλειδιών.

Έγκυρα είναι μόνο τα κλειδιά τα οποία έχουν πιστοποιηθεί από κάποιον που έχει οριστεί σαν έμπιστος. Τα κλειδιά τα οποία ανήκουν σε μεσάζοντες οι οποίοι είναι έμπιστοι, θα πρέπει να έχουν πιστοποιηθεί ή από τους ίδιους τους χρήστες ή από κάποιον άλλον ο οποίος έχει οριστεί σαν έμπιστος. Το PGP δίνει επιπλέον την δυνατότητα να οριστούν διαφορετικά επίπεδα εμπιστοσύνης για διαφορετικούς μεσάζοντες. Όταν ελεγχθεί η εγκυρότητα ενός κλειδιού από το PGP ακολουθεί ο έλεγχος για τον βαθμό εμπιστοσύνης όλων των συνημμένων υπογραφών πιστοποίησης. Το σχεπτικό με το οποίο λειτουργεί το PGP μπορεί να προσαρμόζεται στις απαιτήσεις που έχει ο κάθε χρήστης και επιπλέον μπορεί να ρυθμίζεται ανάλογα.

Το κλειδί που έχει στην κατοχή του ο κάθε χρήστης θεωρείται έγκυρο από το PGP και έτσι δεν χρειάζεται να πιστοποιηθεί από κανέναν. Το PGP έχει τη γνώση για το ποια δημόσια κλειδιά ανήκουν σε ποιόν και κοιτάζει να βρει τα αντίστοιχα μυστικά κλειδιά στο μπρελόκ τους. Το PGP θεωρεί ότι ο καθένας θα πρέπει να εμπιστεύεται τον εαυτό του, ώστε να πιστοποιεί άλλα κλειδιά. Το PGP επιτρέπει στον οποιονδήποτε να μπορεί να καθορίσει ο ίδιος την πολιτική του σε θέματα διαχείρισης των κλειδιών του. Έτσι τέλος το PGP βάζει τους χρήστες, και όχι το σύστημα, στην κορυφή της διαδικασίας της πιστοποίησης αφού αυτοί έχουν τον πρώτο λόγο.

7.9 Προστασία του μυστικού κλειδιού

Η προστασία του μυστικού κλειδιού, είναι κάτι το αυτονόητο, στο οποίο πρέπει να δοθεί μεγάλη προσοχή. Αν κάποια στιγμή πέσει σε λάθος χέρια, τότε θα πρέπει πολύ γρήγορα να ενημερωθούν όλοι, πριν κάποιος αρχίσει να υπογράφει με το όνομα αυτού του οποίου είναι το κλειδί. Το μυστικό κλειδί μπορεί να φυλάσσεται σε κάποιον υπολογιστή στο σπίτι ή σε ένα laptop, αφού βέβαια αυτά είναι υπό συνεχή επίβλεψη. Άρα θα πρέπει το μυστικό κλειδί να χρησιμοποιείται μόνο από συστήματα στα οποία υπάρχει φυσικός έλεγχος.

Πρέπει να υπάρχει μεγάλη προσοχή στην διαδικασία, καθώς και στο χώρο τον οποίο θα αποθηκευτούν το μυστικό κλειδί καθώς και το password, ποτέ δεν γίνεται αποθήκευση και των δύο στον ίδιο χώρο αφενός και να γίνεται backup στο μυστικό μπρελόκ αφετέρου. Σε περιπτώσεις απώλειας θα πρέπει να αχρηστευτούν όλα τα δημόσια κλειδιά.

Το σύστημα PGP εκτός από τα πλεονεκτήματα που έχει στην διαχείριση των κλειδιών, έχει και τα μειονεκτήματά του. Δεν υπάρχει μία κεντρική λίστα που να περιέχει τα μη έγκυρα κλειδιά κάνοντας πιο δύσκολη την γνώση τους. Έτσι αν κάτι πάει στραβά η διαδικασία γνωστοποίησής του είναι επίπονη. Εάν τελικά το μυστικό κλειδί και η μυστική φράση πέσουν στα χέρια άλλων θα πρέπει να φτιάξουμε και να διανείμουμε ένα “πιστοποιητικό απολεσθέντος κλειδιού” (key compromise certificate). Αυτός ο τύπος πιστοποιητικού χρησιμοποιείται για να προειδοποιεί άλλους χρήστες να σταματήσουν να χρησιμοποιούν το αντίστοιχο δημόσιο κλειδί μας. Για την δημιουργία του εν λόγω πιστοποιητικού μπορεί να χρησιμοποιηθεί το PGP και μετά να σταλεί σε όλους τους φίλους και συνεργάτες σε όλον τον κόσμο. Το PGP επιπλέον θα αναλάβει να κάνει την εγκατάσταση του πιστοποιητικού απολεσθέντος κλειδιού στα δημόσια μπρελόκ και από την στιγμή εκείνη και μετά, θα αποτρέπεται αυτομάτως η επαναχρησιμοποίηση του κλειδιού. Ακολούθως θα πρέπει δημιουργηθεί καινούργιο ζευγάρι κλειδιών, μυστικού και δημόσιου και τα οποία θα χρησιμοποιούνται στο μέλλον.

7.10 Δουλεύοντας με το PGP

Η διαδικασία εγκατάστασης του προγράμματος PGP είναι απλή και μετά άμεσα μπορεί να αρχίσει η χρήση του. Η πρώτη κίνηση είναι η δημιουργία του ζεύγους των κλειδιών (ιδιωτικό και δημόσιο). Η μεγαλύτερη προσοχή χρειάζεται τη στιγμή κατά την οποία δίνεται το password, το οποίο δίνει πρόσβαση στο ιδιωτικό κλειδί. Μετά μπορεί αποφασιστεί εάν θα σταλεί το δημόσιο κλειδί σε κάποιον διακομιστή κλειδιών και έτσι οι υπόλοιποι χρήστες να έχουν τη δυνατότητα εύκολα να το παίρνουν και να αποστέλλουν μηνύματα ή δεδομένα τα οποία θα είναι κρυπτογραφημένα.

Για διευκόλυνση στην διανομή του δημόσιου κλειδιού σε άτομα που ενδιαφέρουν, υπάρχει η ευχέρεια να επισυνάπτεται σε e-mail τα οποία στέλνονται. Για να είναι δυνατή η διανομή του ζεύγους των κλειδιών, μπορεί να εξαχθεί το δημόσιο κλειδί σε ένα αρχείο κειμένου, αρκεί να γίνει επιλογή του χρήστη που ενδιαφέρει.

Στην διαδικασία εξαγωγής του ζεύγους κλειδιών γίνεται λόγος για δύο δακτυλίους κλειδιών:

- τον ιδιωτικό, όπου κρατούνται όλα τα ιδιωτικά κλειδιά που έχει κάποιος στην κατοχή του,
- και τον δημόσιο, όπου κρατούνται όλα τα δημόσια.

Κάποιες φορές είναι ανάγκη να διατίθενται περισσότερα από ένα ζεύγος κλειδιών, το ένα ζεύγος χρησιμοποιείται για την προσωπική αλληλογραφία και το άλλο για επαγγελματική χρήση, για την οποία χρήση τα κλειδιά θα είναι μεγαλύτερου μεγέθους και άρα δυσκολότερο να παραβιαστούν.

Όταν ολοκληρωθεί πλέον η εισαγωγή στο PGP, το πρόγραμμα έρχεται με το κατάλληλο plugin, ώστε να υπάρξει συνεργασία με το Outlook. Έτσι αφού συμπληρωθεί και συνταχθεί ένα e-mail και επισυναφθούν κάποια αρχεία, υπάρχουν οι εξής επιλογές, ή να κρυπτογραφηθούν ή να υπογραφεί κάποιο μήνυμα, θα πρέπει όμως να είναι στην διάθεση το δημόσιο κλειδί του παραλήπτη.

Κεφάλαιο 8

Πρωτόκολλο PEM (Privacy Enhanced Mail)

8.1 Εισαγωγή

Ένα μήνυμα ή ένα mail στο Internet το οποίο στέλνεται από έναν αποστολέα προς έναν παραλήπτη, κατά την πορεία του διανύει διάφορα συστήματα και δίκτυα, τα οποία βρίσκονται μέσα σε αυτή την διαδρομή. Δεν μπορεί να βασίζεται κάποιος στο ότι όλα αυτά τα συστήματα και τα δίκτυα που θα χρησιμοποιηθούν παρουσιάζουν αξιοπιστία. Ένας επιτιθέμενος μπορεί να κρυφτεί οπουδήποτε, και τα μηνύματα ή δεδομένα τα οποία ανταλλάσσονται μεταξύ οντοτήτων, είναι πολύ εύκολο από αυτόν να διαβαστούν, να τροποποιηθούν ή ακόμη και να εμποδιστούν στο να φθάσουν στον τελικό τους προορισμό.

Για να μπορέσει να αντιμετωπιστεί αυτή η αδυναμία, την οποία έχει το ηλεκτρονικό ταχυδρομείο του Internet, υπάρχει το πρωτόκολλο PEM Privacy Enhanced Mail, το οποίο προσθέτει την εφαρμογή των υπηρεσιών της απορρήτου συναλλαγής πιστοποίησης της ταυτότητας, της ακεραιότητας των μηνυμάτων και της μη αποκήρυξης της πηγής, για να το πετύχει. Όλες αυτές οι υπηρεσίες προσφέρονται μέσα από την χρήση της απ' άκρη σε άκρη κρυπτογράφησης μεταξύ δύο χρηστών.

8.2 Οι αρχές του PEM

Το σημαντικότερο για το πρωτόκολλο PEM είναι ότι οι υπηρεσίες ασφάλειας εφαρμόζονται σε όλο το μήνυμα και όχι σε ένα μέρος αυτού αφού δεν επιτρέπεται αλλά ούτε και υποστηρίζεται η επιλεκτική χρήση των υπηρεσιών του σε τμήματα των μηνυμάτων.

Η ανάπτυξη του πρωτοκόλλου στηρίχθηκε σε κάποιες βασικές αρχές:

- Όλες οι προσθήκες ασφάλειας εφαρμόζονται στο Application Layer του OSI και είναι ανεξάρτητες από οποιαδήποτε χαρακτηριστικά ασφάλειας χαμηλότερων επιπέδων.
- Οι προσθήκες ασφάλειας εφαρμόζονται μόνο από τον αποστολέα και τους τελικούς αποδέκτες των μηνυμάτων. Ο αποστολέας είναι απαραίτητο να γνωρίζει κατά πόσο ο προοριζόμενος παραλήπτης του μηνύματος εφαρμόζει τις υπηρεσίες ασφάλειας του PEM, ώστε να αποφευχθεί η άσκοπη κρυπτογράφηση και κωδικοποίηση του μηνύματος.
- Οι καθορισμένοι μηχανισμοί είναι συμβατοί με μεγάλη ποικιλία προγραμμάτων ηλεκτρονικού ταχυδρομείου και επιπλέον οι μηχανισμοί του PEM διαλέγονται έτσι ώστε να μπορούν να χρησιμοποιηθούν στα περισσότερα προγράμματα χρηστών.

- Με το πρωτόκολλο PEM υποστηρίζεται μεγάλη ποικιλία τεχνικών διαχείρισης κλειδιών και διαφορετικές τεχνικές χρησιμοποιούνται με διαφορετικούς παραλήπτες. Διαφορετικές τεχνικές μπορούν να οριστούν ακόμα και με τους διαφορετικούς παραλήπτες ενός multicast-μηνύματος.

8.3 Είδη κλειδιών και διαχείριση αυτών για το πρωτόκολλο PEM

Η περιγραφή του πρωτοκόλλου PEM στο RFC 1421 καθορίζει δύο τύπους κλειδιών οι οποίοι είναι:

- Τα **Data Encrypting Keys, (DEK)**, τα οποία είναι κλειδιά τα οποία χρησιμοποιούνται για να γίνεται η κρυπτογράφηση μηνυμάτων ή κειμένων. Στην διαχείριση ασύμμετρων κλειδιών, στα PEM μηνύματα στα οποία εφαρμόζεται η υπηρεσία με την οποία προστατεύεται το απόρρητο τα DEK κλειδιά χρειάζονται για την επιπλέον κρυπτογράφηση των Message Integrity Checks (MIC). Τα MIC είναι τα αποτελέσματα που λαμβάνονται στην έξοδο ενός digest ή ένας hash algorithm, όταν εισαχθεί στην είσοδο το μήνυμα. Τα κλειδιά DEK παράγονται εκ νέου κάθε φορά που πρέπει να μεταδοθεί νέο μήνυμα.
- Τα **Interchange Keys, (IK)**, είναι κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση των DEK και MIC, τα οποία μεταφέρονται μέσα σε κάποιο μήνυμα. Σημειωτέον ότι το ίδιο IK κλειδί χρησιμοποιείται σε όλα τα μηνύματα που ανταλλάσσουν δύο οντότητες, για μικρό όμως χρονικό διάστημα. Η κρυπτογράφηση των DEK και MIC γίνεται και με συμμετρική κρυπτογράφηση αλλά και με ασύμμετρη. Στην πρώτη περίπτωση το κλειδί IK είναι το ίδιο και για τους δύο χρήστες. Στην δεύτερη περίπτωση η κρυπτογράφηση του DEK γίνεται με το δημόσιο κλειδί του παραλήπτη και για την κρυπτογράφηση των MIC γίνεται με το ιδιωτικό κλειδί του αποστολέα.

Όταν κάποιο μήνυμα είναι υπό εξέταση από το PEM παράγεται ένα DEK για να μπορέσει να κρυπτογραφηθεί το μήνυμα, όπως επίσης και οι παράμετροι που είναι αναγκαίες. Τέτοιες παράμετροι π.χ. είναι Initialization Vectors οι οποίες εξαρτώνται από τους αλγορίθμους που έχουν επιλεγεί. Στην περίπτωση των ασύμμετρων IK κλειδιών που χρησιμοποιούνται είναι διαφορετικά, για τον καθένα παραλήπτη του μηνύματος, ώστε να προετοιμαστούν προς κρυπτογράφηση τα DEK και τα MIC. Αντίθετα στην περίπτωση των ασύμμετρων IK κλειδιών, (επειδή ο αποστολέας έχει στην κατοχή του ένα ζευγάρι κλειδιών), η κρυπτογράφηση των DEK και MIC γίνεται για τον κάθε παραλήπτη μηνυμάτων με το ίδιο κλειδί. Στην ασύμμετρη διαχείριση κλειδιών, επιπλέον, υπάρχει η δυνατότητα να συνδυαστεί με χρήση πιστοποιητικών με τα οποία θα επαληθευτεί η ταυτότητα του αποστολέα κάποιου μηνύματος. Το πιστοποιητικό αυτό εκτός από τις πληροφορίες που είναι σχετικές με τον εκδότη κάποιου Certificate Authority (CA), περιέχει και το κλειδί του αποστολέα.

Υπάρχει περίπτωση, ένα σύστημα Key Distribution System, να δημιουργεί κάποια τυχαία DEK. Τέτοια συστήματα έχουν την δυνατότητα να εφαρμόζουν ισχυρότερους αλγορίθμους για να παράγονται τυχαία DEK, παρόλα αυτά όμως, η αποκέντρωση της παραγωγής, επιτρέπει στα συστήματα τα οποία χρησιμοποιούν οι διάφοροι χρήστες, να συντηρούνται μόνα τους και επίσης να απαλείφει την εμπιστοσύνη σε τρίτους χρήστες.

8.4 Περιληπτική Διαχείριση Μηνυμάτων

Για να μπορούν τα κρυπτογραφημένα μηνύματα να είναι αναγνωρίσιμα από όλους και να μεταφέρονται στο κάθε περιβάλλον, χρειάζεται ένας μετασχηματισμός που να περνάει από διάφορες φάσεις.

Η διαδικασία που ακολουθείται είναι η ακόλουθη. Αρχικά τα μηνύματα συντάσσονται με βάση τοπικούς κανόνες, κάνοντας χρήση του συνόλου χαρακτήρων καθώς και τους χαρακτήρες ελέγχου του τοπικού συστήματος. Η μορφή αυτή μετατρέπεται ακολουθώντας σε κανονική, η οποία αποτελεί την είσοδο στις διαδικασίες της κρυπτογράφησης και της παραγωγής MIC. Το αποτέλεσμα που βγαίνει από την κρυπτογράφηση και την παραγωγή του MIC κωδικοποιείται με βάση έναν κατάλληλο μηχανισμό. Η έξοδος του τελευταίου βήματος συνδυάζεται με κάποιες κατάλληλες επικεφαλίδες που μεταφέρουν πληροφορίες για τον έλεγχο της κρυπτογράφησης. Το PEM μήνυμα που εξάγεται από την διαδικασία, συμπεριλαμβάνεται στα περιεχόμενα ενός μηνύματος το οποίο είναι να μεταδοθεί. Στα περιεχόμενα μπορεί να υπάρχει και ένα απλό κείμενο το οποίο δεν προστατεύεται. Στην συνέχεια ο κάθε παραλήπτης του μηνύματος, αφού πρώτα αφαιρέσει την κωδικοποίηση, αμέσως μετά εξετάζει τα πεδία ελέγχου της κρυπτογράφησης, τα οποία δίδουν τις πληροφορίες που χρειάζονται ώστε να επαληθευθούν η εγκυρότητα του MIC και ακολουθώντας να αποκρυπτογραφηθεί το κείμενο. Σαν τελευταίο βήμα είναι ότι το μήνυμα μετατρέπεται από την κανονική μορφή στην μορφή η οποία αντιστοιχεί στα χαρακτηριστικά του τοπικού συστήματος του παραλήπτη. Εδώ θα πρέπει να σημειωθεί ότι τα άκυρα PEM μηνύματα θα πρέπει να αναφερθούν μαζί με την συλλογή διαγνωστικών πληροφοριών, ώστε να αντιμετωπίζονται προβλήματα ασυμβατότητας ή κάποιων άλλων αιτιών. Τα δε έγκυρα PEM μηνύματα, που όμως έχουν πρόβλημα όσο αφορά στην επαλήθευση, (η οποία είναι αποτυχημένη), του MIC, θα πρέπει να αντιμετωπίζονται με αρκετή προσοχή. Επίσης οι χρήστες είναι αναγκαίο να ειδοποιούνται, ότι δεν μπορεί να είναι εγγυημένη η αυθεντικότητα και η ακεραιότητα των μηνυμάτων.

8.5 Μηχανισμός Ενθυλάκωσης

Το τελικό αποτέλεσμα το οποίο προκύπτει από την αμέσως προηγούμενη διαδικασία, μπορεί να συνδυαστεί με κάποιες πληροφορίες που είναι σχετικές με την προστασία του εγγράφου. Μετά από αυτόν τον συνδυασμό το αποτέλεσμα ενθυλακώνεται στο σώμα του μηνύματος, το οποίο και μεταδίδεται. Στις επικεφαλίδες και πριν από τα προστατευμένα δεδομένα, τοποθετούνται τα πεδία τα οποία αναφέρονται στην κρυπτογράφηση αφενός και στα MIC αφετέρου. Όλο το PEM μήνυμα περικλείεται από τις κατάλληλες γραμμές διαχωρισμού.

Η διαδικασία της ενθυλάκωσης παρέχει γενίκευση στον τρόπο με τον οποίο εκτελείται η επεξεργασία του μηνύματος που παρελήφθη. Ακολουθώντας η ενθυλάκωση διαχωρίζει τα πεδία, που είναι χρήσιμα στην αποκρυπτογράφηση και επαλήθευση του μηνύματος, από αυτά που αλλάζουν στην μεταφορά. Η τεχνική της ενθυλάκωσης είναι δυνατόν να χρησιμοποιηθεί και στην ενθυλάκωση πολλαπλών PEM μηνυμάτων, καθώς και στην συνοδεία του PEM μηνύματος από ένα απλό κείμενο. Οι διαχωριστικές γραμμές, που αναφέρθηκαν, χρειάζονται για τον διαχωρισμό των PEM μηνυμάτων, καθώς και στην διάκριση στα μη κρυπτογραφημένα μηνύματα.

8.6 Τύποι μηνυμάτων των PEM

Ανάλογα με το είδος της παρεχόμενης προστασίας και της εφαρμοζόμενης υπηρεσίας τα PEM μηνύματα διακρίνονται σε τέσσερα είδη:

- **Encrypted:** αναπαριστά ένα PEM μήνυμα στο οποίο έχουν εφαρμοστεί οι υπηρεσίες της διαφύλαξης του απορρήτου της συναλλαγής, της εξασφάλισης της ακεραιότητας των δεδομένων, της πιστοποίησης ταυτότητας και της εξασφάλισης της μη αποκήρυξης της πηγής.
- **MIC-Only:** αναπαριστά ένα PEM μήνυμα στο οποίο παράγονται όλες οι προηγούμενες υπηρεσίες εκτός της διαφύλαξης του απορρήτου. Μόνο τα UA (είναι προγράμματα ηλεκτρο-

νικού ταχυδρομείου) που ενσωματώνουν το PEM μπορούν να παρουσιάσουν το μήνυμα για ανάγνωση.

- **MIC-Clear:** το μήνυμα είναι το ίδιο με προηγουμένως με την διαφορά ότι όλα τα UA μπορούν να παρουσιάσουν το μήνυμα, αλλά μόνο οι συμβατοί με το PEM μπορούν να επαληθεύσουν την αυθεντικότητα και την ακεραιότητα του μηνύματος.
- **Certificate Revocation:** είναι το μήνυμα που περιέχει μια ή περισσότερες λίστες ανάκλησης πιστοποιητικών.

8.7 Ταχυδρομικές Λίστες

Όταν ένα μήνυμα απευθύνεται σε ταχυδρομικές λίστες, δύο διαφορετικές μέθοδοι μπορούν να εφαρμοστούν για προστασία και αφορούν τα κλειδιά ΙΚ.

Η πρώτη μέθοδος είναι το ΙΚ ανά λίστα, κατά την οποία ο αποστολέας επιλέγει να μην κάνει ανάλυση της ταχυδρομικής λίστας στα μέλη της και να χρησιμοποιήσει κοινό ΙΚ κλειδί για όλους τους παραλήπτες της λίστας. Στην περίπτωση αυτής της μεθόδου το ίδιο ΙΚ κλειδί, πρέπει να είναι στην διάθεση όλων των μελών της ταχυδρομικής λίστας, πράγμα που σημαίνει ότι γίνεται εύκολη η επεξεργασία του μηνύματος.

Όταν χρησιμοποιείται αυτή η μέθοδος, υπάρχει πιθανή και σε μεγάλο βαθμό έκθεση, καθώς και ανάκληση, του ΙΚ κλειδιού, που σημαίνει ότι δημιουργείται πρόβλημα μεταξύ των μελών της λίστας. Ειδικά για τα συμμετρικά κλειδιά, ο κάθε χρήστης που κατέχει το ΙΚ κλειδί, μπορεί να κάνει ότι είναι ο αυθεντικός αποστολέας. Όμως και κατά την διαχείριση ασύμμετρων κλειδιών, υπάρχει ένα μειονέκτημα, αφού δεν γίνεται να εφαρμοστούν όλες οι υπηρασίες ασφάλειας.

Η δεύτερη μέθοδος είναι το ΙΚ ανά παραλήπτη, κατά την οποία το κλειδί για την κρυπτογράφηση των δεδομένων του DEK μηνύματος, κρυπτογραφείται με κάθε ένα κλειδί ΙΚ, για τον κάθε παραλήπτη. Μεταφέρονται έτσι με το μήνυμα όλες οι παρουσιάσεις των DEK. Η κρυπτογράφηση ανά χρήστη δεν εκτελείται στο προστατευμένο κείμενο αλλά μόνο στα DEK και στα MIC.

Η μέθοδος αυτή έχει ένα μειονέκτημα, που είναι η χρήση πολλαπλών ΙΚ κλειδιών τα οποία περιπλέκουν την επεξεργασία του μηνύματος καθώς και την διαχείριση των κλειδιών. Όμως η υποκλοπή ενός κλειδιού, το οποίο δεν μοιράζεται σε πολλούς χρήστες, είναι δυσκολότερη και η ανάκληση σε ένα ζεύγος ΙΚ κλειδιών, δεν δημιουργεί προβλήματα σε όλα τα μέλη της λίστας.

Το καταληκτικό συμπέρασμα είναι ότι, μια υβριδική προσέγγιση είναι προτιμότερη, για την διαδρομή από τον αποστολέα προς τον MLA (mail List Agent) όπου εφαρμόζεται η πρώτη μέθοδος που αναφέρθηκε (δηλαδή η ΙΚ ανά λίστα). Στην αντίστροφη όμως διαδρομή δηλαδή από τον MLA (mail List Agent) προς τους τελικούς αποδέκτες, εφαρμόζεται η δεύτερη μέθοδος (δηλαδή η ΙΚ ανά παραλήπτη).

8.8 Περίληψη Ενθυλακωμένων Επικεφαλίδων

Στο σημείο αυτό θα αναπτυχθούν οι περιπτώσεις των πιο σημαντικών επικεφαλίδων οι οποίες ενθυλακώνονται στο PEM μήνυμα και περιέχουν χρήσιμες και απαραίτητες πληροφορίες, για την προστασία που παρέχεται στους αλγορίθμους κρυπτογράφησης και παραγωγής των MIC. Στην ενθυλάκωση αυτή περιλαμβάνονται και στοιχεία τα οποία είναι απαραίτητα για να πιστοποιηθεί η ταυτότητα της πηγής.

Οι επικεφαλίδες αυτές είναι:

- **Proc-Type:** απαιτείται σε όλα τα PEM μηνύματα, απαντάται μόνο μια φορά και είναι η πρώτη ενθυλακωμένη επικεφαλίδα. Υποδηλώνει τον τύπο του PEM μηνύματος και η τιμή που μπορεί να πάρει είναι Encrypted, MIC-Only, MIC-Clear και CRL.
- **Content-Domain:** περιγράφει το είδος των περιεχομένων που μεταφέρονται ενθυλακωμένα και στα οποία εφαρμόζονται οι υπηρεσίες ασφάλειας του PEM. Η μόνη προκαθορισμένη τιμή είναι η RFC 822.
- **DEK-Info:** περιγράφει τον αλγόριθμο κρυπτογράφησης των περιεχομένων και μεταφέρει κατάλληλες παραμέτρους για συγκεκριμένους αλγορίθμους. Υπάρχει και μια τιμή DEK-Info ανά μήνυμα και απαιτείται για όλα τα Encrypted μηνύματα.
- **Originator-ID:** προσδιορίζει την ταυτότητα του αποστολέα και καθορίζει το IK κλειδί που χρησιμοποιείται. Η επικεφαλίδα αυτή έχει δύο διαφορετικές μορφές, ανάλογα με την τεχνική διαχείρισης κλειδιών: η Originator-ID-Asymmetric η οποία απαιτείται για όλα τα PEM μηνύματα με ασύμμετρη διαχείριση κλειδιών και η Originator-ID-Symmetric η οποία απαιτείται για το PEM μηνύματα με συμμετρική διαχείριση κλειδιών.
- **Originator-Certificate:** χρησιμοποιείται μόνο στην ασύμμετρη διαχείριση κλειδιών. Μεταφέρει το πιστοποιητικό του αποστολέα κωδικοποιημένο σύμφωνα με τον μηχανισμό Base 64.
- **MIC-Info:** χρησιμοποιείται μόνο με την ασύμμετρη διαχείριση κλειδιών και περιέχει στοιχεία που υποδηλώνουν τον αλγόριθμο που παρήγαγε το MIC, τον αλγόριθμο που κρυπτογράφησε το MIC και τέλος περιέχει την υπογραφή του μηνύματος από το ιδιωτικό κλειδί του αποστολέα. Για την περίπτωση Encrypted PEM μηνυμάτων, το κρυπτογραφημένο MIC ξανά κρυπτογραφείται με το ίδιο DEK και τον ίδιο αλγόριθμο που χρησιμοποιήθηκε στα προστατευόμενα περιεχόμενα.
- **Recipient-ID:** η επικεφαλίδα αυτή προσδιορίζει την ταυτότητα του παραλήπτη ή και παραληπτών. Συγχρόνως παρέχει το IK κλειδί και παρουσιάζεται με δύο διαφορετικές μορφές: την Recipient-ID-Asymmetric και την Recipient-ID-Symmetric ανάλογα με την τεχνική διαχείρισης των κλειδιών.
- **Key-Info:** οι πληροφορίες που περιέχει εξαρτώνται από την διαχείριση των κλειδιών. Στην συμμετρική διαχείριση των κλειδιών περιλαμβάνεται ο αλγόριθμος που χρησιμοποιήθηκε για την κρυπτογράφηση των DEK και MIC από το IK, καθώς και τα ίδια τα DEK και MIC από το IK. Στην ασύμμετρη διαχείριση κλειδιών περιλαμβάνονται ο αλγόριθμος κρυπτογράφησης του DEK από το δημόσιο κλειδί του αποστολέα και επίσης το κρυπτογραφημένο DEK από το δημόσιο κλειδί του αποστολέα.

8.9 Υποστηριζόμενοι Αλγόριθμοι

Ο μόνος αλγόριθμος για κρυπτογράφηση περιεχομένων είναι ο DES σε μορφή Cipher Block Chaining (CBC) mode. Η είσοδος στην περίπτωση αυτού του αλγορίθμου, μπορεί να χρειάζεται το κατάλληλο συμπλήρωμα, ώστε το μέγεθός του να είναι πολλαπλάσιο των 8 bytes. Επίσης χρειάζεται έναν 64 bits Initialization Vector, ο οποίος διαφέρει για κάθε ένα Encrypted PEM μήνυμα. Ο DES CBC χρειάζεται ένα κλειδί κρυπτογράφησης των 64 bits. Από τα 64 bits τα 56 bits μπορούν

να χρησιμοποιηθούν απευθείας για τον DES CBC, ενώ τα υπόλοιπα 8 bits είναι bits περιττής ισοτιμίας. Για το κάθε Encrypted PEM μήνυμα παράγεται ένα νέο τυχαίο κλειδί.

Για να παραχθούν MIC, υπάρχουν δύο αλγόριθμοι ο MD2 και ο MD5. Και οι δύο δέχονται σαν είσοδο, μήνυμα οποιουδήποτε μήκους και παράγουν στην έξοδο μία ακολουθία των 16 bytes. Όταν χρησιμοποιείται η διαχείριση συμμετρικών κλειδιών, το αποτέλεσμα χωρίζεται σε δύο ίσα κομμάτια των 8 bytes, τα οποία κρυπτογραφούνται ξεχωριστά και κατόπιν ενώνονται πάλι.

Οι αλγόριθμοι που χρησιμοποιούνται για την διαχείριση συμμετρικών κλειδιών, τα οποία χρησιμοποιούνται για να κρυπτογραφηθούν οι DEK και MIC είναι δύο παραλλαγές του DES, ο DES σε ECB (Electronic Code Book) mode, καθώς και ο DES σε EDE (Encrypt-Decrypt-Encrypt) mode. Και οι δύο αλγόριθμοι χρειάζονται IK κλειδιά που έχουν μέγεθος 64 bits.

Οι αλγόριθμοι που χρησιμοποιούνται για την διαχείριση ασύμμετρου ζευγαριού IK κλειδιών (δημόσιο και ιδιωτικό), έχουν την μορφή η οποία καθορίζεται από τον μηχανισμό RSA. Έτσι για την κρυπτογράφηση των DEK και MIC ο μηχανισμός RSA εφαρμόζεται με τέτοιο τρόπο που το ιδιωτικό κλειδί να κρυπτογραφεί το MIC (και έτσι να παράγονται ψηφιακές υπογραφές των μηνυμάτων), το δε δημόσιο κλειδί κρυπτογραφεί τον DEK. Χρησιμοποιώντας επιπλέον τον αλγόριθμο MD2 σε συνδυασμό με τον RSA, δημιουργούνται οι προϋποθέσεις ώστε να υπογράφονται τα πιστοποιητικά CRL.

Κεφάλαιο 9

Εφαρμογές της Κρυπτογραφίας

9.1 Γενικά

Η χρήση της κρυπτογραφίας, με την ραγδαία εξέλιξη που είχε, αυξάνεται συνεχώς και αυτό καθιστά αξιόπιστη την οποιαδήποτε μεταφορά πληροφοριών ή δεδομένων μέσω του διαδικτύου. Η σύγχρονη κρυπτογραφία παρέχει πολλές εφαρμογές, οι οποίες βοηθάνε, σε μεγάλο βαθμό, τον κάθε τομέα της καθημερινότητας των ανθρώπων. Πολύ σύντομα θα προσφέρονται συναρπαστικές εφαρμογές της κρυπτογραφίας, όπως είναι η αναγνώριση αντικειμένων μέσω ραδιοσυχνοτήτων (RFID). Ακολούθως αναφέρεται ένας συνοπτικός κατάλογος των εφαρμογών της κρυπτογραφίας:

- Ασφάλεια των συναλλαγών σε τράπεζες, δίκτυα- ATM.
- Κινητή τηλεφωνία (TETRA-TETRAPOL-GSM).
- Σταθερή τηλεφωνία (Crypto phones).
- Διασφάλιση εταιρικών πληροφοριών.
- Στρατιωτικά δίκτυα (Τακτικά Συστήματα Επικοινωνιών Μάχης).
- Διπλωματικά δίκτυα.
- Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές).
- Ηλεκτρονική ψηφοφορία.
- Ηλεκτρονική δημοπρασία.
- Ηλεκτρονικό γραμματοκιβώτιο.
- Συστήματα συναγερμών.
- Συστήματα βιομετρικής αναγνώρισης.
- Έξυπνες κάρτες.
- Ιδιωτικά δίκτυα (VPN).
- Word Wide Web.
- Δορυφορικές εφαρμογές (δορυφορική τηλεόραση).

- Ασύρματα δίκτυα (Hipperion, Bluetooth, 802.11x).
- Τηλεδιάσκεψη-τηλεφωνία μέσω διαδικτύου VOIP.
- Διάφορα πρωτόκολλα.
- Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων.

Ακολούθως θα αναπτυχθούν εν συντομία ορισμένες από τις παραπάνω εφαρμογές.

9.2 Πρωτόκολλα

Τα συστήματα κρυπτογραφίας τα οποία χρησιμοποιούνται από το WEB, και ικανοποιούν τις τέσσερες βασικές απαιτήσεις ασφάλειας, (οι οποίες είναι η αρχή της εμπιστευτικότητας, η αρχή της ακεραιότητας, της επίδειξης γνησιότητας και η αρχή της μη αποκήρυξης), χρησιμοποιούν τα ακόλουθα πρωτόκολλα: PEM (Privacy Enhanced Mail), S/MIME (Secure/Multipurpose Internet Mail Extensions), S-HTTP (Secure-Hyper Text Transfer Protocol), IP Sec (IP Security Protocol), SET (Secure Electronic Transactions), SSH (Secure Shell) και IKE (Internet Key Exchange). Τα πρωτόκολλα αυτά θα αναλυθούν εν συντομία ακολούθως.

9.2.1 PEM (Privacy Enhanced Mail)

Το πρωτόκολλο αυτό έχει σκοπό να αντιμετωπίσει τα προβλήματα και τις αδυναμίες του ηλεκτρονικού ταχυδρομείου στο Ιντερνέτ, οι οποίες παρουσιάζονται. Για να συμβεί αυτό, προστίθεται κάποια εφαρμογή, ώστε να εξασφαλίζεται το απόρρητο στις διάφορες συναλλαγές, η πιστοποίηση της ταυτότητας, η ακεραιότητα των δεδομένων ή μηνυμάτων, καθώς και η μη αποκήρυξη της πηγής. Η εξασφάλιση όλων αυτών γίνεται με την χρήση, από το ένα έως το άλλο άκρο, κρυπτογράφησης μεταξύ δύο οντοτήτων.

9.2.2 S/MIME (Secure/Multipurpose Internet Mail Extensions)

Αν κάποιος θέλει να ανταλλάξει, σε γλώσσες πλην της αγγλικής, μηνύματα μέσα από διαφορετικά υπολογιστικά συστήματα, χρησιμοποιεί αυτό το πρωτόκολλο. Χρησιμοποιείται κυρίως από προγράμματα ηλεκτρονικού ταχυδρομείου, τα οποία θέλουν να εφαρμόσουν κρυπτογράφηση σε μηνύματα που αποστέλλονται αφενός και για να επεξεργαστούν προστατευμένα μηνύματα που έχουν παραληφθεί αφετέρου. Επιπλέον δίνει την δυνατότητα σε εταιρείες που σχεδιάζουν λογισμικά, να αναπτύσσουν τέτοια, ώστε ένα μήνυμα αν κρυπτογραφείται με ένα συγκεκριμένο πρόγραμμα να μπορεί να αποκρυπτογραφηθεί από ένα άλλο.

9.2.3 S-HTTP(Secure Hyper –Text-Transfer-Protocol)

Είναι το πιο βασικό και το περισσότερο χρησιμοποιούμενο από τα πρωτόκολλα που υπάρχουν σε δραστηριότητες μεταξύ ενός client και ενός server στο WWW. Το πρωτόκολλο αυτό παρέχει, τέτοιους ασφαλείς μηχανισμούς μεταξύ ενός client και ενός server, ώστε να επιτρέπονται ασφαλείς και αυθόρμητες συναλλαγές μεταξύ τους. Στόχος στη σχεδίαση αυτού του πρωτοκόλλου, ήταν να είναι ευέλικτο και να διαθέτει πολλαπλούς μηχανισμούς από αλγορίθμους. Παρέχει ακόμη συμμετρικές δυνατότητες, σε δύο οντότητες που επικοινωνούν μεταξύ τους, πράγμα που σημαίνει ότι τα μηνύματα και οι προτιμήσεις και των δύο πλευρών, τα χρησιμοποιούν με τον ίδιο τρόπο και παράλληλα διατηρείται το μοντέλο συναλλαγής καθώς και διατηρούνται τα χαρακτηριστικά επικοινωνίας

του εν λόγω πρωτοκόλλου. Αυτό το πρωτόκολλο δεν χρειάζεται πιστοποιητικά δημόσιων κλειδιών από την μεριά ενός client, αφού υποστηρίζει και τα συμμετρικά κλειδιά. Αυτό είναι αρκετά σημαντικό, επειδή οι ανυθόρμητες ιδιωτικές συναλλαγές μπορούν να εκτελούνται, χωρίς να απαιτείται από του χρήστες να έχουν ένα έγκυρο ζευγάρι κλειδιών.

9.2.4 IP Sec (IP Security Protocol)

Το πρωτόκολλο αυτό περιλαμβάνει ένα σύνολο από μηχανισμούς οι οποίοι είναι σχεδιασμένοι, έτσι ώστε να προστατεύουν την κίνηση IP. Προστατεύει δε τις ακόλουθες υπηρεσίες, την χωρίς σύνδεση ακεραιότητα των πληροφοριών και δεδομένων, την εξακρίβωση για την γνησιότητα της προέλευσής τους, την προστασία έναντι των επαναλήψεων και τέλος την διασφάλιση της εμπιστευτικότητας.

9.2.5 SET (Secure Electronic Transactions)

Είναι ένα κρυπτογραφικό πρωτόκολλο, το οποίο αναπτύχθηκε από την Visa, την Master Card, την Netscape και την Microsoft. Έχει κάποια εξειδίκευση και για τον λόγο αυτό χρησιμοποιείται μόνο για την ασφαλή συναλλαγή με πιστωτικές κάρτες και επιταγές μεταξύ πελατών και εμπόρων. Δημιουργήθηκε με βάση συγκεκριμένες προδιαγραφές, οι οποίες προήλθαν από τις ανάγκες των επιχειρήσεων για ασφαλείς συναλλαγές.

9.2.6 SSH (Secure Shell)

Το πρωτόκολλο SSH (Secure Shell), παρέχει ασφαλή απομακρυσμένη σύνδεση, σε έναν υπολογιστή, πάνω από ένα δίκτυο που δεν είναι ασφαλές και επιπλέον επιτρέπει την διαπραγμάτευση όλων των αλγορίθμων που χρησιμοποιούνται. Κύριος στόχος του είναι να παραμένει όσο γίνεται πιο απλό, με όσο το δυνατόν λιγότερους αλγορίθμους. Υπάρχει όμως και ένας άλλος στόχος, ο οποίος αποβλέπει στην βελτίωση της ασφάλειας στο Ιντερνέτ. Όλες οι εφαρμογές του πρωτοκόλλου πρέπει να υποστηρίζουν ένα ελάχιστο σύνολο αλγορίθμων, έτσι ώστε να εξασφαλιστεί η διαλειτουργικότητά του. Για να γίνει γρήγορη ανάπτυξη και υιοθέτηση του πρωτοκόλλου, έχουν υπάρξει κάποιες παραχωρήσεις, όπως είναι η καθιέρωση στην υποχρεωτική επαλήθευση των κλειδιών, πράγμα όμως το οποίο δεν συνιστάται. Οι αλγόριθμοι κρυπτογράφησης, ανταλλαγής των κλειδιών, συμπίεσης, η παροχή ακεραιότητας καθώς και οι μηχανισμοί ασύμμετρων κλειδιών, μπορεί να επιλεγούν από λίστες. Οι λίστες αυτές δίνονται από τον client στον server και αντίστροφα και μάλιστα διαφορετικοί για την κάθε κατεύθυνση.

9.2.7 Το πρωτόκολλο ανταλλαγής κλειδιών (IKE-Internet Key Exchange)

Για την υποστήριξη αυτοματοποιημένων διαπραγματεύσεων της CA, καθώς και για την αυτοματοποιημένη δημιουργία και ανανέωση κλειδιών κρυπτογράφησης, σχεδιάστηκε το πρωτόκολλο IKE (Internet Key Exchange). Χρησιμοποιεί κάποιες πολύπλοκες διαδικασίες κρυπτογράφησης και εξακρίβωσης της γνησιότητας, γιατί μέσω αυτής γίνονται οι ανταλλαγές πληροφοριών και κλειδιών τα οποία απαιτούνται για να διαφυλάσσεται η ασφάλεια των επικοινωνιών.

9.3 Συστήματα ψηφιακών πληρωμών

9.3.1 First Virtual

Το οποιοδήποτε σύστημα πληρωμών στηρίζεται επάνω στην ανταλλαγή των e-mail καθώς και στην εντιμότητα των καταναλωτών. Το σύστημα First Virtual παίζει τον ρόλο του μεσολαβητή σε συναλλαγές πιστωτικών καρτών ανάμεσα σε καταναλωτές και σε εμπόρους. Το σύστημα αυτό δεν χρησιμοποιεί κρυπτογραφία ή ασφαλή μέσα επικοινωνίας και για να το χρησιμοποιήσει κάποιος καταναλωτής, θα πρέπει πρώτα να εγκαταστήσει έναν λογαριασμό First Virtual. Ο λογαριασμός αυτός ασφαλίζεται με πιστωτικές κάρτες Visa και Master Card. Μετά την υπογραφή First Virtual, δίνεται στον καταναλωτή ένα PIN. Το πλεονέκτημα που έχει το σύστημα First Virtual, είναι ότι παρέχεται ασφάλεια απέναντι σε απάτες.

9.3.2 Cyber Cash

Χρησιμοποιεί εξειδικευμένο λογισμικό από την πλευρά του πελάτη και του πωλητή, για να εξασφαλίσει ασφαλείς ηλεκτρονικές συναλλαγές μέσω του διαδικτύου. Υποστηρίζει πληρωμές τόσο με πιστωτικές κάρτες όσο και με ηλεκτρονικά εμβάσματα (checks). Χρησιμοποιεί κρυπτογράφηση 3DES κατά την μετάδοση της πληροφορίας που αφορά την πληρωμή. Επίσης δεν είναι απαραίτητο οι πωλητές να αποθηκεύουν, στην βάση δεδομένων ή σε οποιαδήποτε άλλη μορφή στατικής μνήμης, τους αριθμούς των πιστωτικών καρτών των πελατών τους. Αυτό ελαχιστοποιεί τον κίνδυνο να κλαπεί κάποια σημαντική πληροφορία, που αφορά την ηλεκτρονική συναλλαγή, από άτομα που μπορεί να παραβιάσουν τα συστήματα ασφαλείας στους υπολογιστές του πωλητή.

9.3.3 Digicash

Στις Digicash οι καταναλωτές έχουν την δυνατότητα να κρατάνε τη νομισματική αξία μέσα σε μια φόρμα ηλεκτρονικών εμβλημάτων (tokens). Καταναλωτές και έμποροι ανταλλάσσουν tokens, πράγμα το οποίο επιβεβαιώνεται από μια τράπεζα που πιστοποιεί ότι οι υπογραφές οι οποίες υπάρχουν πάνω στα tokens είναι έγκυρες και ότι επιπλέον τα tokens δεν έχουν ξοδευτεί. Με τις Digicash παρέχεται ένα αρκετά υψηλό σύστημα ασφαλείας. Τέλος ο έμπορος ο οποίος χρησιμοποιεί Digicash έχει την πληροφόρηση την οποία χρειάζεται, ώστε να διασφαλίσει την πληρωμή του, ενώ αντίθετα η τράπεζα για κάποια συναλλαγή της έχει πληροφόρηση μόνο για να κάνει πίστωση ή χρέωση σε κάποιον λογαριασμό.

9.3.4 Millicent

Τα Millicent χρησιμοποιούνται κυρίως για μικρές ηλεκτρονικές αγορές αγαθών. Η καινοτομία αυτής της εφαρμογής είναι η χρήση των κτηματομεσιτών (brokers) και των χαρτονομισμάτων scrips. Ένα scrip έχει μικρή ονομαστική αξία και εξαργυρώνεται μόνο σε συγκεκριμένα εμπορικά καταστήματα. Στο scrip η αρίθμηση γίνεται συριακά και επιπλέον υπογράφεται με ψηφιακό τρόπο. Τα scrips αγοράζονται σε ποσότητες μεγάλες, σε χονδρική τιμή από τους brokers, οι οποίοι στη συνέχεια τα μεταπωλούν σε διάφορους πελάτες. Τέλος το σύστημα των Millicent αφού διαχειρίζεται μικροποσά δεν χρειάζεται ισχυρή κρυπτογραφία αλλά ούτε και κάποια υποδομή δημόσιου κλειδιού για τη πιστοποίηση της αυθεντικότητας.

9.3.5 Μαγνητικές Κάρτες

Οι περιπτώσεις κατά τις οποίες γίνεται χρήση των μαγνητικών καρτών είναι, για την αναγνώριση των χρηστών από τερματικά ATM και POS, καθώς και σε σημεία πώλησης σε καταστήματα. Με τις μαγνητικές κάρτες μπορεί να γίνεται και έλεγχος στην πρόσβαση, ιδιαίτερα σε ασφαλείς τοποθεσίες (Zone Access Control). Η χρήση τέτοιων καρτών συνήθως συνδυάζεται μαζί με κάποιον κωδικό, ώστε να επιβεβαιώνεται η ταυτότητα του χρήστη ο οποίος είναι νόμιμος.

9.3.6 Έξυπνες Κάρτες (Smart Card)

Οι έξυπνες κάρτες διαθέτουν μικροεπεξεργαστές, καθώς και μνήμες ROM και RAM. Είναι κάρτες οι οποίες διαθέτουν πιο μεγάλη μνήμη από τις μαγνητικές κάρτες και έχουν πλεονέκτημα αφού διαθέτουν ενσωματωμένη υπολογιστική ισχύ. Ένα άλλο σπουδαίο πλεονέκτημα των έξυπνων καρτών είναι ότι πολύ δύσκολα μπορεί να γίνει αντιγραφή τους. Επίσης παρέχουν φυσική προστασία των δεδομένων τα οποία είναι αποθηκευμένα.

9.4 Σύστημα Κέρβερος

Το σύστημα Κέρβερος είναι μια αξιόπιστη τριμερής υπηρεσία η οποία πιστοποιεί τις ταυτότητες των χρηστών και βασίστηκε σε ένα μοντέλο το οποίο παρουσιάστηκε από τους Needham και Schroeder. Βασίζεται στην απόκτηση από τους χρήστες κουπονιών (tokens) από έμπιστους και ασφαλείς servers, τα οποία ισχύουν για ένα συγκεκριμένο χρονικό διάστημα και μόνο με αυτά μπορεί κάποιος να αποκτήσει άδεια για να μπορεί να έχει πρόσβαση σε αρχεία ή υπηρεσίες. Το σύστημα Κέρβερος κρατάει σε μια βάση δεδομένων όλους τους πελάτες μαζί με τα κλειδιά τους. Το ιδιωτικό κλειδί του κάθε χρήστη είναι ένας κρυπτογραφημένος κωδικός πρόσβασης, ο οποίος είναι γνωστός μόνο στον ιδιοκτήτη του και στον Κέρβερο. Αφού λοιπόν ο Κέρβερος γνωρίζει τα ιδιωτικά κλειδιά των χρηστών, έχει την δυνατότητα να δημιουργήσει μηνύματα με τα οποία μπορεί να πειστεί ο κάθε εξυπηρετούμενος ότι αυτός με τον οποίο είναι σε επικοινωνία είναι αυτός που ισχυρίζεται ότι είναι. Ακόμη ο Κέρβερος μπορεί να δώσει κάποια προσωρινά κλειδιά συνόδου σε δύο χρήστες και μόνο σε αυτούς. Με το κλειδί συνόδου μπορούν να κρυπτογραφηθούν μηνύματα που ανταλλάσσονται ανάμεσα σε δύο οντότητες. Τέλος στον Κέρβερο καταχωρούνται δικτυακές υπηρεσίες, οι οποίες απαιτούν πιστοποίηση, όπως επίσης καταχωρούνται και οι εξυπηρετούμενοι, οι οποίοι θέλουν να χρησιμοποιήσουν αυτές τις υπηρεσίες και όλα τα ιδιωτικά κλειδιά διαπραγματεύονται όταν γίνεται η καταχώρηση.

9.5 Συστήματα βάσης βιομετρήσεων

Μια από τις πιο σύγχρονες εφαρμογές της κρυπτογράφησης είναι οι βιομετρήσεις. Ως γνωστόν το ανθρώπινο σώμα έχει πληθώρα μοναδικών γνωρισμάτων, τα οποία μπορούν να χρησιμοποιηθούν για την αναγνώριση της ταυτότητας κάποιου χρήστη. Παραδείγματα τέτοιων γνωρισμάτων είναι τα δακτυλικά αποτυπώματα, η ίριδα του ματιού, το σχήμα του προσώπου ή του χεριού, η φωνή, η φλεβική δομή, η γεωμετρία του αυτιού, το DNA, η μυρωδιά του σώματος κλπ. Όλα αυτά αφορούν τα φυσικά χαρακτηριστικά του κάθε ατόμου. Το τελευταίο διάστημα αναπτύσσονται και κάποιες μέθοδοι οι οποίες βασίζονται στην συμπεριφορά του ατόμου όπως είναι ο ρυθμός πληκτρολόγησης ενός κειμένου, η υπογραφή του χρήστη κλπ. Οι βιομετρικές μέθοδοι θεωρούνται οι πιο ασφαλείς και μάλιστα τις χρησιμοποιούν αρκετοί οργανισμοί όπως κρατικές υπηρεσίες, τράπεζες κλπ με σκοπό πάντα να παρέχουν αυξημένη ασφάλεια στα συστήματά τους και καλύτερη εξυπηρέτηση των

πελατών τους. Περιπτώσεις που εφαρμόζονται οι βιομετρικές μέθοδοι είναι τα PIN, οι διάφορες κάρτες καθώς και τα συνθηματικά.

9.6 Ιδιωτικά δίκτυα VPN (Virtual Private Network)

Τα δίκτυα αυτά είναι μια εξαιρετικά σημαντική τεχνολογία η οποία τα τελευταία χρόνια έχει γνωρίσει μεγάλη ανάπτυξη. Τις πιο πολλές φορές και ιδιαίτερα για απομακρυσμένους χρήστες, απαιτεί πιστοποίηση και επιπλέον ασφαλίζει τα διάφορα δεδομένα με τεχνολογίες κρυπτογράφησης, με τέτοιον τρόπο ώστε να μην είναι δυνατή η διάδοση ιδιωτικών πληροφοριών σε άτομα τα οποία δεν είναι εξουσιοδοτημένα. Σημαντικό πλεονέκτημα αυτών των δικτύων είναι το μειωμένο κόστος τους, αφού δεν είναι απαραίτητη κάποια φυσική μισθωμένη γραμμή που συνδέει απομακρυσμένους χρήστες σε ένα δίκτυο Intranet. Η αιτία για την οποία δημιουργήθηκαν τέτοια δίκτυα είναι η ασφάλεια που παρέχουν, αφού κάποιος τρίτος μη εξουσιοδοτημένος, δεν μπορεί να υποκλέψει συνομιλίες και δεδομένα, έτσι υπάρχει εκτεταμένη χρήση από τον στρατό. Στα δίκτυα αυτά ο εκάστοτε δρομολογητής δεν είναι αυτός που επιλέγει το που θα σταλούν τα διάφορα μηνύματα. Τέλος δημιουργείται ένα κανάλι μέσα από το οποίο γίνεται ασφαλής η επικοινωνία μεταξύ χρηστών.

9.7 Ηλεκτρονική ψηφοφορία

Για τις ηλεκτρονικές ψηφοφορίες είναι απαραίτητο να υπάρχει κάποια εγγύηση, ώστε η κάθε ψήφος να μην έχει υποστεί τροποποίηση μετά από την υποβολή της. Στη περίπτωση της ψηφοφορίας από απόσταση υπεισέρχονται κάποιες παράμετροι, οι οποίες έχουν άμεση σχέση με την διαδικασία της ψηφοφορίας, και που παραβιάζουν την ιδιωτικότητα. Παραδείγματα τέτοιων παραμέτρων είναι το διαδίκτυο, κάποιο κακόβουλο λογισμικό κλπ. Τα θεμελιώδη στοιχεία τα οποία συνθέτουν την διαδικασία της ηλεκτρονικής ψηφοφορίας είναι, κατά πρώτον η άσκηση του εκλογικού δικαιώματος από απόσταση και η χρήση κάποιου υπολογιστικού συστήματος ώστε να οργανωθεί και να διεξαχθεί κανονικά η όλη εκλογική διαδικασία. Ένα τέτοιο σύστημα μπορεί να περιλαμβάνει σύστημα υλικού και λογισμικού όπως επί παραδείγματι εξυπηρετητές, σταθμούς εργασίας, πρωτόκολλα κρυπτογράφησης κλπ. Ακόμη τέτοια συστήματα είναι δυνατόν να περιλαμβάνουν κάποια σύνολα από οντότητες οι οποίες είναι εξουσιοδοτημένες και που εμπλέκονται στην όλη διαδικασία της ψηφοφορίας, επιπλέον ενσωματώνουν ένα σύνολο από κάποιους κανόνες και ορισμένες διαδικασίες, στοιχεία τα οποία καθορίζουν τον τρόπο με τον οποίο θα διεξαχθεί η διαδικασία της ψηφοφορίας. Και τέλος γίνεται έλεγχος σε όλα τα επιμέρους στάδια, ώστε να είναι δυνατή η εξασφάλιση της ακεραιότητας καθώς και της εγκυρότητας της ηλεκτρονικής ψηφοφορίας.

9.8 Ηλεκτρονική δημοπρασία

Είναι διαδικασία την οποία χρησιμοποιούν επιχειρήσεις και οργανισμοί, με μεγάλη ποικιλία αποτελεσμάτων. Σε κάποιες από αυτές τις δημοπρασίες επιτυγχάνονται μειωμένες τιμές, αλλά και μπορεί να χρησιμοποιηθούν σαν εργαλεία έρευνας για τις τιμές καθώς και για να λαμβάνονται γνώσεις οι οποίες αφορούν την αγορά γενικότερα. Βασικά οι ηλεκτρονικές δημοπρασίες είναι μια on line διαδικασία δυναμικής διαπραγμάτευσης σε πραγματικό χρόνο, μεταξύ κάποιας επιχείρησης ή οργανισμού από την μια μεριά και μιας ομάδας προμηθευτών οι οποίοι είναι προεγκεκριμένοι από την άλλη. Οι προμηθευτές είναι σε έναν συνεχή ανταγωνισμό μεταξύ τους, κάνοντας τις προσφορές τους μέσω του διαδικτύου, χρησιμοποιώντας βέβαια κάποιο λογισμικό το οποίο είναι εξειδικευμένο για τέτοιες περιπτώσεις.

9.9 Ηλεκτρονικό γραμματοκιβώτιο (Mail Box)

Το Mail Box είναι η θέση στην οποία αποθηκεύονται τα διάφορα μηνύματα, μέχρι τη στιγμή την οποία θα παραληφθούν με την βοήθεια του προγράμματος του ηλεκτρονικού ταχυδρομείου το οποίο χρησιμοποιεί ο κάθε χρήστης. Παραδείγματα τέτοιων προγραμμάτων είναι το Outlook Express, το Netscape Messenger κλπ. Τα πρωτόκολλα POP και το SMTP είναι αυτά τα οποία αναλαμβάνουν την λήψη και την αποστολή των διαφόρων μηνυμάτων. Με το πρόγραμμα του ηλεκτρονικού ταχυδρομείου υπάρχει η δυνατότητα λήψης των μηνυμάτων ή απευθείας από το Mail Box ή από απόσταση με την βοήθεια εξυπηρετητών οι οποίοι χρησιμοποιούν το πρωτόκολλο POP.

9.10 Τηλεδιάσκεψη

Η τηλεδιάσκεψη είναι ένας από τους τρόπους για να υπάρχει άμεση επικοινωνία μέσα από το Internet, όπου αυτοί οι οποίοι συμμετέχουν συνδέονται με έναν εξυπηρετητή ο οποίος είναι τέτοιος ώστε να μπορούν να συνομιλούν με τους υπόλοιπους. Αυτό μπορεί να γίνει με την υποστήριξη κάποιου κειμένου το οποίο πληκτρολογείται και η ηχητική σύνδεση γίνεται με κάποια μικρόφωνα ενώ η οπτική σύνδεση γίνεται με την χρησιμοποίηση βιντεοκάμερας. Στην τηλεδιάσκεψη το βασικό χαρακτηριστικό είναι ότι οι συμμετέχοντες που συνομιλούν είναι ταυτόχρονα συνδεδεμένοι στο πρόγραμμα το οποίο τους διαχειρίζεται.

9.11 Τηλεφωνία μέσω VOIP

Η τηλεφωνία μέσω VOIP είναι το είδος της επικοινωνίας μέσω του διαδικτύου, το οποίο χαρακτηρίζεται από ένα σύνολο τεχνολογιών και πρωτοκόλλων, με την οποία προσφέρεται συνομιλία φωνής σε πραγματικό χρόνο, με αρκετά καλή ποιότητα και το σπουδαιότερο χωρίς κανένα κόστος.

9.12 Ασφάλεια τραπεζικών συναλλαγών

Για να είναι δυνατή η ασφάλεια στις τραπεζικές συναλλαγές, είναι απαραίτητη η χρήση προηγμένων τεχνολογιών και αναγνωρισμένων πρωτοκόλλων ασφάλειας, με τα οποία εξασφαλίζεται ασφαλής πρόσβαση στις διάφορες υπηρεσίες τις οποίες προσφέρει η κάθε τράπεζα, επιπλέον το απόρρητο των προσωπικών δεδομένων του κάθε πελάτη καθώς και η μεταφορά τους, η αποθήκευσή τους και τέλος η θωράκιση του όλου συστήματος από πιθανές απειλές επιθέσεων πρόσβασης από τρίτα πρόσωπα.

9.13 Δίκτυα ATM

Τα δίκτυα των ATM των τραπεζών, είναι από τις πλέον διαδεδομένες διαδικασίες, μέσω των οποίων εξυπηρετούνται πελάτες, και μάλιστα δεν είναι απαραίτητη η χρήση του Internet. Αυτό όμως το οποίο είναι απαραίτητο, είναι η χρήση κάποιου στοιχείου αυθεντικοποίησης και ταυτοπροσωπίας, όπως επί παραδείγματι κάποια κάρτα, και έτσι παρουσιάζεται η δυνατότητα να διεκπεραιωθούν πάρα πολλές τραπεζικές συναλλαγές, οι οποίες ολοκληρώνονται με ασφάλεια αφού γι' αυτές τις διαδικασίες χρησιμοποιούνται οι τελευταίες εξελιγμένες τεχνολογίες ασφάλειας, όπως είναι η κρυπτογράφηση, οι ψηφιακές υπογραφές και πολλές άλλες.

Κεφάλαιο 10

10.1 Η Έννοια Της Ιδιωτικότητας(Privacy)

Η ιδιωτικότητα είναι σχετική με τις ψηφιακές τεχνολογίες, οι οποίες έχουν μπει σε μεγάλο βαθμό στην ζωή μας, και βρίσκεται χωρίς αμφισβήτηση στην επικαιρότητα. Το τι είναι ιδιωτικό αλλάζει από άτομο σε άτομο και από λαό σε λαό και επιπλέον καθορίζεται από κάποιες αρχές. Πάντα όμως άτομα ή ομάδες ανθρώπων φροντίζουν ώστε οι πληροφορίες ή τα δεδομένα, που διακινούνται στο διαδίκτυο, να είναι προστατευμένα και να φαίνονται μόνο όσα θέλουν αυτοί.

Η ιδιωτικότητα λοιπόν έχει μεγάλη σχέση με την ασφάλεια πληροφοριών και δεδομένων και κάποιες φορές ταυτίζονται, άλλες φορές όμως έρχονται σε σύγκρουση. Από την άποψη της πληροφορικής ιδιωτικότητα δεδομένων και πληροφοριών είναι η σχέση που υπάρχει ανάμεσα στην διάδοση και την συγκέντρωση των διαφόρων πληροφοριών που διακινούνται μέσω του διαδικτύου.

Παραδείγματα δεδομένων τα οποία πρέπει να προστατεύονται, είναι τα προσωπικά δεδομένα και ιδιαίτερα τα λεγόμενα ευαίσθητα προσωπικά δεδομένα. Ενδεικτικά αναφέρονται σαν προσωπικά δεδομένα, οι πληροφορίες για την επικοινωνία (όνομα, τηλέφωνο, email κλπ), διάφορες μορφές ταυτοποίησης (ταυτότητα, δίπλωμα, διαβατήριο κλπ), δημογραφικές πληροφορίες (ηλικία, φίλο, εθνικότητα κλπ), επαγγελματικές πληροφορίες (θέση που κατέχει κάποιος στην εργασία του, σε ποια επιχείρηση εργάζεται κλπ), πληροφορίες υγειονομικού ενδιαφέροντος (κατάσταση της υγείας, φορέας ασφάλισης κλπ), χρηματοοικονομικής φύσεως πληροφορίες (τραπεζικοί λογαριασμοί, ιστορικό αγορών κλπ) και τέλος διάφορες δραστηριότητες στο διαδίκτυο (διεύθυνση IP, αγορές, επαφές, φίλοι κλπ). Σαν ευαίσθητα προσωπικά δεδομένα μπορούν να θεωρηθούν οι πολιτικές και οι θρησκευτικές πεποιθήσεις, πληροφορίες που αφορούν την υγεία, τις σεξουαλικές προτιμήσεις κλπ.

Η προστασία της ιδιωτικότητας είναι ένα πολύ σημαντικό θέμα, το οποίο θα πρέπει να αφορά, εκτός των απλών χρηστών, κυρίως τις επιχειρήσεις, έτσι ώστε να υπάρχει η δυνατότητα διασφάλισης των δεδομένων και των πληροφοριών και άρα να διαφυλάσσεται η εμπιστοσύνη, που είναι απαραίτητο να έχουν οι πελάτες απέναντι στην κάθε επιχείρηση με την οποία συναλλάσσονται ώστε να παρεμποδίζονται π.χ. ύποπτες δραστηριότητες.

Τα τελευταία χρόνια, με την μεγάλη ανάπτυξη του διαδικτύου, η οποία έχει συμβεί, υπεισέρχεται αναγκαστικά το ζήτημα της προστασίας της ιδιωτικότητας. Ένα παράδειγμα με το οποίο απειλείται η ιδιωτικότητα, είναι τα κοινωνικά δίκτυα, όπως το Facebook. Εκτός όμως από τα social media, υπάρχουν και κάποιες άλλες εφαρμογές του διαδικτύου, οι οποίες δεν δίνουν την απόλυτη εξασφάλιση της ιδιωτικότητας για τους διάφορους χρήστες. Μια αυτού του είδους εφαρμογή είναι το cloud computing (το υπολογιστικό νέφος), του οποίου η χρήση έχει εξαπλωθεί τόσο σε μεμονωμένους χρήστες, όσο και σε επιχειρήσεις. Το θέμα του cloud computing θα αναπτυχθεί σε άλλη ενότητα που ακολουθεί.

10.2 ABC 4 Trust

Για να αντιμετωπιστούν τα μεγάλα προβλήματα της ιδιωτικότητας, τα οποία προέκυψαν μετά την εξάπλωση των εφαρμογών του cloud, υπάρχουν τα διαπιστευτήρια, δηλαδή οι νέες μορφές των ηλεκτρονικών ταυτοτήτων. Έχουν υπάρξει πολλές προσπάθειες για να επιτευχθεί αυτός ο στόχος, μια από τις τελευταίες είναι το έργο ABC 4 Trust η οποία στηρίχθηκε στα διαπιστευτήρια που βασίζονται στα χαρακτηριστικά Attribute Based Credentials (ABCs).

10.2.1 Attribute Based Διαπιστευτήρια

Καθημερινά πραγματοποιείται μεγάλο πλήθος από ηλεκτρονικές συναλλαγές, όπως είναι το ηλεκτρονικό εμπόριο, το e-banking, καθώς και διάφορες δοσοληψίες που πιθανώς να έχουν οι πολίτες με κρατικές υπηρεσίες όπως εφορία, ασφαλιστικά ταμεία κλπ. Όλες αυτές οι εφαρμογές πρέπει να στηρίζονται σε κάποιου είδους αυθεντικοποίηση, ώστε με αυτόν τον τρόπο να δημιουργούνται σχέσεις εμπιστοσύνης για όλα τα εμπλεκόμενα μέρη που επικοινωνούν.

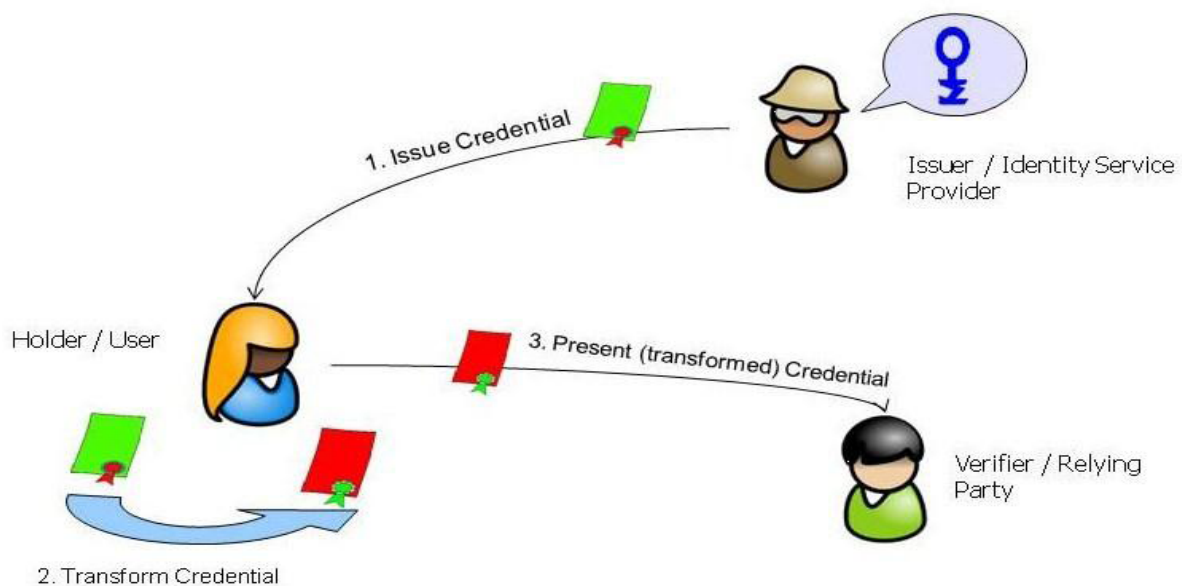
Τα μέσα λοιπόν για την προστασία της ιδιωτικότητας των χρηστών είναι τα ηλεκτρονικά διακριτικά ελέγχου ταυτότητας και ασφάλειας με τα οποία οι χρήστες αποδεικνύουν το ποιοι είναι. Οι μηχανισμοί αυτοί δεν χρησιμοποιούνται μόνο στο διαδίκτυο, αλλά και αλλού, όπως σε περιπτώσεις των ηλεκτρονικών ταυτοτήτων, των κινητών τηλεφώνων καθώς και των RFID διακριτικών (Radio Frequency Identification), δηλαδή την ταυτοποίηση μέσω ραδιοσυχνοτήτων (είναι δηλαδή ένα σύστημα ασύρματης αναγνώρισης αντικειμένων, το οποίο αντικατέστησε τα Bar Code). Αυτοί οι μηχανισμοί αυθεντικοποίησης εξαπλώνονται με μεγάλη ταχύτητα, αλλά παρουσιάζουν δυστυχώς μια αδυναμία, δηλαδή το ότι χρησιμοποιούν μοναδικά αναγνωριστικά, πράγμα το οποίο δημιουργεί σοβαρό κίνδυνο όσο αφορά την ιδιωτικότητα, αφού μπορεί ο ίδιος χρήστης να κάνει διάφορες συναλλαγές.

Ένας άλλος τρόπος για την προστασία των χρηστών του διαδικτύου είναι η αυθεντικοποίηση με την χρήση κωδικών πρόσβασης, μηχανισμός όμως ο οποίος παρουσιάζει πολλά προβλήματα που αφορούν την ιδιωτικότητα. Ακόμα και τα κρυπτογραφικά πιστοποιητικά, τα οποία είναι ένας ακόμα τρόπος προστασίας, δεν καλύπτουν πλήρως τις προϋποθέσεις που απαιτεί και έχει ανάγκη η ιδιωτικότητα, παρά το ότι παρέχουν ασφάλεια η οποία είναι αρκετή για τους διάφορους χρήστες του διαδικτύου, επειδή αφορούν ένα υπαρκτό πρόσωπο. Η χρήση ενός κρυπτογραφικού πιστοποιητικού βάζει σε κίνδυνο την ταυτότητα του χρήστη που το έχει στην κατοχή του, στο σημείο το οποίο ζητά (ο χρήστης) την αυθεντικοποίηση.

Τα κλασικά διαπιστευτήρια δεν προστατεύουν την ιδιωτικότητα, επειδή κυρίως αποκαλύπτουν την ταυτότητα αυτού που έχει στην κατοχή του το διαπιστευτήριο. Σε αντίθεση με τα κλασικά, τα ABCs διαπιστευτήρια επιτρέπουν στον κάτοχό τους να αποκαλύπτει μόνο κάποιο ελάχιστο κομμάτι της πληροφορίας, χωρίς να γίνεται γνωστή η ταυτότητά του. Έχουν γίνει πολλές προσπάθειες για την δημιουργία ABC συστημάτων, ώστε να μπορούν να είναι έμπιστα και παράλληλα να προστατεύουν την ιδιωτικότητα του κατόχου των διαπιστευτηρίων. Τέτοια ABCs διαπιστευτήρια είναι τα κρυπτογραφικά, όπως τα X 509, τα οποία μπορούν να επαληθευτούν με την χρήση δημόσιου κλειδιού του εκδότη και παράλληλα να προσφέρουν την απαιτούμενη ασφάλεια.

Οι τεχνολογίες ABC, που ονομάζονται ανώνυμα συστήματα διαπιστευτηρίων, επιτρέπουν σε κάποιον πάροχο υπηρεσιών ταυτότητας, να εκδίδει διαπιστευτήρια σε οποιονδήποτε χρήστη και μάλιστα παρέχοντας κάποια χαρακτηριστικά του χρήστη, όπως είναι η διεύθυνσή του, η ημερομηνία γέννησής του αλλά και τα δικαιώματα που έχει καθώς και οι ρόλοι του. Χρησιμοποιώντας έτσι ο χρήστης κάποιο διαπιστευτήριο, μπορεί να αποδείξει σε κάποιον τρίτο, ότι το έχει στην κατοχή του και περιέχει κάποιες συγκεκριμένες πληροφορίες αποθηκευμένες. Έτσι λοιπόν τα ανώνυμα διαπιστευτήρια έχουν σκοπό να γίνουν η βάση για την προστασία της ιδιωτικότητας του χρήστη

σε ένα τέτοιο σημερινό ηλεκτρονικό περιβάλλον.



Σχήμα 10.1: Επαλήθευση ενός attribute-based διαπιστευτηρίου

10.2.2 Περιγραφή του έργου ABC4Trust

Όπως είναι γνωστό όλες οι υπηρεσίες και οι εφαρμογές που σχετίζονται και βασίζονται στους ηλεκτρονικούς υπολογιστές, χρειάζονται απαραίτητα την ύπαρξη αυθεντικοποίησης, ώστε να είναι δυνατή η δημιουργία σχέσεων εμπιστοσύνης μεταξύ των χρηστών που έρχονται σε επικοινωνία. Όμως οι παραδοσιακές μορφές διαπιστευτηρίων, όπως έχει αναφερθεί και στην προηγούμενη ενότητα, δεν προσφέρουν απόλυτη προστασία στην ιδιωτικότητα των χρηστών του διαδικτύου και η μόνη πλέον ελπίδα ώστε να καλυφθεί και να αντιμετωπιστεί αυτό το πρόβλημα είναι τα ABCs συστήματα αυθεντικοποίησης.

Υπάρχουν πολλές προτάσεις για τον τρόπο με τον οποίο μπορεί να γίνει η υλοποίηση σε ABCs συστήματα αυθεντικοποίησης, και συγκεκριμένα θα αναφερθούν δύο τέτοιες τεχνολογίες, οι οποίες παρουσιάστηκαν από τις εταιρείες IBM και Microsoft και συγκεκριμένα η τεχνολογία Identity Mixer και η τεχνολογία U-Prove αντίστοιχα για κάθε εταιρεία.

Κατά πρώτον η εταιρεία IBM ανέπτυξε μετά από αρκετές έρευνες ένα ανώνυμο σύστημα διαπιστευτηρίων, το οποίο είναι το Identity Mixer, τεχνολογία η οποία δίνει στους χρήστες και μάλιστα σε μεγάλο βαθμό, την δυνατότητα αυθεντικοποίησης και ιδιωτικότητας, ζητήματα τα οποία είναι απαραίτητα και χρειάζεται να συνυπάρχουν ταυτόχρονα. Με αυτήν την τεχνολογία, στους διάφορους χρήστες, παρουσιάζεται η δυνατότητα να μπορούν να προμηθεύονται από τον εκδότη, διαπιστευτήρια, τα οποία θα περιέχουν όλες τις πληροφορίες που ο κάθε εκδότης, έχει την δυνατότητα να πιστοποιήσει, για λογαριασμό τους. Κατόπιν εάν ο χρήστης θέλει να αποδείξει, σε κάποιον πάροχο υπηρεσιών, έναν ισχυρισμό ο οποίος τον αφορά, θα πρέπει να χρησιμοποιήσει την τεχνολογία της IBM Identity Mixer, ώστε να μπορεί να εκτελέσει κάποιον μετασχηματισμό, με ασφάλεια, στα διαπιστευτήρια τα οποία έχει εκδώσει αυτός ο πάροχος. Μάλιστα αυτά τα διαπιστευτήρια, τα οποία έχουν υποστεί από τον χρήστη τον οποιονδήποτε μετασχηματισμό περιέχουν μόνο τις πληροφορίες, οι οποίες είναι πιστοποιημένες και που ο κάθε χρήστης έχει την διάθεση να αποκαλύψει σε άλλους χρήστες με τους οποίους έρχεται σε επικοινωνία. Επίσης κάθε χρήστης έχει

την δυνατότητα να εκτελέσει κάποιον μετασχηματισμό στα διαπιστευτήρια, όσες φορές θελήσει, χωρίς να υπάρχει επηρεασμός στην διασύνδεση μεταξύ αυτών που επικοινωνούν.

Τώρα κατά δεύτερον η εταιρεία Microsoft, ανέπτυξε μια προηγμένη τεχνολογία κρυπτογράφησης, την U-Prove, η οποία συνδυασμένη με κάποιες από τις γνωστές λύσεις ταυτοποίησης, οι οποίες βασίζονται σε κάποια πρότυπα, ξεπερνάει το πρόβλημα της εξασφάλισης της ταυτότητας και της ιδιωτικότητας του κάθε χρήστη.

Επειδή οι δύο αυτές τεχνολογίες, δηλαδή η Identity Mixer και η U-Prove, υποστηρίζονται από τις δύο κορυφαίες στον κόσμο εταιρίες σε θέματα πληροφορικής, (αναφερόμαστε στην IBM και στην Microsoft), είναι ανάμεσα στις υποψήφιες οι οποίες θα συνεισφέρουν στην διαδικασία της τυποποίησης και η οποία αφορά τον συγκεκριμένο τομέα, δηλαδή την έκδοση τέτοιων διαπιστευτηρίων τα οποία θα εξασφαλίζουν την προστασία της ταυτότητας και της ιδιωτικότητας των χρηστών που επικοινωνούν μεταξύ τους. Όμως εξ' αιτίας της πολυπλοκότητας την οποία παρουσιάζουν τα ABCs συστήματα διαπιστευτηρίων καθώς και οι επιδράσεις τις οποίες έχουν μεταξύ τους οι clients και οι servers, είναι ζητήματα τα οποία αποθαρρύνουν τους διάφορους πιθανούς χρήστες, και έτσι με αυτόν τον τρόπο εμποδίζεται η ανάπτυξη αυτών των τεχνολογιών, να γίνει σε μεγάλη κλίμακα.

Για να μπορέσουμε τώρα να ξεπεράσουμε τα διάφορα εμπόδια που προκύπτουν κατά την εφαρμογή αυτών των τεχνολογιών, θα πρέπει να υπάρξει κάποιου είδους συγκριτική αντίληψη, για τις δύο αυτές τεχνολογίες, έτσι ώστε να έχουν την δυνατότητα μεμονωμένοι χρήστες ή ομάδες χρηστών, να αποφασίζουν για το ποια από τις δύο εφαρμογές (Identity Mixer και U-Prove) τους προσφέρει καλύτερη εξυπηρέτηση. Επιπλέον οι χρήστες να έχουν την δυνατότητα της πρόσβασης σε πιθανές εφαρμογές, οι οποίες ίσως και να χρειάζονται διαφορετικές ABCs τεχνολογίες. Αυτός είναι ο λόγος που είναι αναγκαίο να υπάρχουν μαζί και μάλιστα να εναλλάσσονται, διαφορετικού τύπου ABCs τεχνολογίες, οι οποίες αφορούν τους ίδιους χρήστες καθώς και τις πλατφόρμες κάποιων εφαρμογών. Επειδή δεν υπάρχουν λειτουργίες και χαρακτηριστικά, για τα οποία να υπάρχει η δυνατότητα μέτρησης και σύγκρισης μεταξύ των ABCs τεχνολογιών και έτσι γίνεται δύσκολο αν όχι αδύνατο να εξαχθούν κάποια συμπεράσματα τα οποία να αφορούν τα πλεονεκτήματα ή τα μειονεκτήματα, των εν λόγω δύο τεχνολογιών που έχουν αναφερθεί, ώστε να επιλεγεί η πιο καλή και αποτελεσματική για την αυθεντικοποίηση.

10.2.3 Στόχοι του έργου ABC4Trust

Το έργο, που ονομάζεται ABC4Trust, χρησιμοποιεί τεχνολογίες που μπορούν να προστατέψουν την ιδιωτικότητα του ατόμου. Το έργο αυτό, θα διερευνήσει και θα δοκιμάσει στην πράξη τις τεχνολογίες προστασίας της ιδιωτικότητας με βάση τα Attribute-Based Credentials (ABC) οι οποίες επιτρέπουν στον χρήστη να δώσει μόνο τις προσωπικές πληροφορίες που είναι αναγκαίες χωρίς να αποκαλύψει την πλήρη ταυτότητά του.

Το έργο ABC4Trust ξεκίνησε το Νοέμβριο του 2010 και διήρκεσε τέσσερα χρόνια. Ξεκίνησε πιλοτικά με εφαρμογές και δοκιμές σε Σουηδία και Ελλάδα και συγκεκριμένα, η πρώτη πιλοτική εφαρμογή πραγματοποιήθηκε στο Norrtullskolan, ένα σχολείο της δευτεροβάθμιας εκπαίδευσης στο Söderhamn της Σουηδίας και η δεύτερη πιλοτική εφαρμογή, πραγματοποιήθηκε από το Ερευνητικό Ακαδημαϊκό Ινστιτούτο Τεχνολογίας Υπολογιστών (EAITY) στην Πάτρα.

Το έργο ABC4Trust θα δώσει την δυνατότητα σε κάθε εκπαιδευτικό ίδρυμα να εκδίδει ηλεκτρονικά πιστοποιητικά στους χρήστες, συμπεριλαμβανομένων μαθητών, γονέων, και φοιτητών, επιτρέποντάς τους να αποδεικνύουν διάφορες ιδιότητές τους, όπως είναι το ότι έχουν παρακολουθήσει ένα μάθημα, ότι είναι μέλη μιας συγκεκριμένης τάξης, ότι ανήκουν σε μία συγκεκριμένη ομάδα εργασίας ή αθλητική ομάδα, ή ακόμη και το φύλο ή την ηλικία τους. Το πιστοποιητικό κάθε χρήστη θα είναι αποθηκευμένο σε μία έξυπνη κάρτα ή κινητό τηλέφωνο και θα μπορεί να το χρησιμοποιεί για την ταυτοποίησή του σε διάφορες υπηρεσίες.

Ο στόχος του έργου ABC4Trust είναι να καταστούν κατανοητές πλήρως και σε βάθος οι ABCs τεχνολογίες και έτσι να αναπτυχθούν αποτελεσματικά και αποδοτικά στην πράξη καθώς και να ενοποιηθούν αυτές οι τεχνολογίες σε πολλούς διαφορετικούς τομείς. Για τον λόγο αυτόν το έργο ABC4Trust θα πρέπει αρχικά να προτείνει ένα πλαίσιο, για τις τεχνολογίες ABCs, το οποίο θα επιτρέπει την συνύπαρξη, την εναλλαγή καθώς και την ενοποίηση αυτών των τεχνολογιών. Συγκεκριμένα, κατά πρώτον θα αναγνωρίζει και θα περιγράφει διαφορετικές συνιστώσες αυτών των τεχνολογιών (όπως είναι η αίτηση, αλλά και η έκδοση διαπιστευτηρίων), και κατά δεύτερον θα δημιουργεί τις προδιαγραφές εκείνες που θα έχουν οι διάφορες μορφές των δεδομένων, τις προδιαγραφές των διεπαφών και τέλος τις μορφές που θα έχουν τα πρωτόκολλα για το συγκεκριμένο πλαίσιο. Επίσης θα ορίζει τα κριτήρια με βάση τα οποία θα μπορεί να γίνει η σύγκριση των ιδιοτήτων οι οποίες πραγματοποιούνται στις διαφορετικές τεχνολογίες, γι' αυτές τις συνιστώσες και τέλος θα παρέχει τις σχετικές υλοποιήσεις για την κάθε μία από αυτές τις συνιστώσες.

Κυρίως όμως έξι είναι οι στόχοι του έργου ABC4Trust, οι οποίοι αναφέρονται συνοπτικά ακολούθως:

- θα προτείνει κάποιο πλαίσιο για τις ανεξάρτητες τεχνολογίες, για τα πρωτόκολλα καθώς και για την λειτουργία των ABCs τεχνολογιών, με τέτοιο τρόπο ώστε κάποιες διαφορετικές τεχνολογίες, να μπορούν να συνυπάρχουν και να ανταποκρίνονται στις απαιτήσεις που έχουν οι διάφορες εφαρμογές, οι οποίες τείνουν να εναλλάσσονται καθώς και να ενοποιούνται με την πάροδο του χρόνου ενώ παράλληλα αυτές οι τεχνολογίες εξελίσσονται.
- θα αναλύει και θα συγκρίνει τις νέες τεχνολογίες ABCs, που παρουσιάζονται στην πορεία και έχουν σχέση με την ασφάλεια και την ροή των πληροφοριών και με την επεξεργασία των χαρακτηριστικών και τις επιδόσεις τους.
- θα δημιουργήσει ανάπτυξη σε κάποιες από τις υλοποιήσεις αυτών των τεχνολογιών, έτσι ώστε να είναι δυνατόν να επιτευχθεί η μεταφορά τους σε κάποιες διαφορετικές πλατφόρμες ή σε κάποιους συνδυασμούς πλατφορμών.
- θα έχει την δυνατότητα να προσδιορίσει τις απαιτήσεις τις οποίες έχουν οι διάφορες επιχειρήσεις, ώστε να έχουν την δυνατότητα να ετοιμάσουν κάποιες πιλοτικές εφαρμογές, οι οποίες προκύπτουν από τις ABCs τεχνολογίες.
- θα αναπτύξει κάποιες πιλοτικές εφαρμογές, ώστε να είναι δυνατός ο έλεγχος της αξιοπιστίας της εν λόγω αρχιτεκτονικής πρότασης, θα εξερευνήσει στην πράξη, αυτές τις αρχιτεκτονικές και τέλος θα εκτελέσει αξιολόγηση για την χρησιμότητά τους σε πραγματικά σενάρια εφαρμογών και τα οποία αφορούν κυρίως τις επιχειρήσεις.
- θα αποτελέσει τον κινητήριο μοχλό με την βοήθεια του οποίου, οι διάφορες εταιρείες που συμμετέχουν σε αυτό το έργο θα έχουν την δυνατότητα να στοχεύουν στην τυποποίηση και παράλληλα να γνωστοποιούν τα αποτελέσματα που προκύπτουν, έτσι ώστε ο καθένας να έχει την δυνατότητα πρόσβασης στη γνώση για τις ABCs τεχνολογίες, καθώς και να μαθαίνει πληροφορίες οι οποίες αφορούν τις πιλοτικές εφαρμογές τους.

10.3 Υπολογιστικό Νέφος (cloud computing)

10.3.1 Εισαγωγή στο 'νέφος'

Στην προσπάθεια να ορίσει κάποιος με ακρίβεια τι είναι το cloud computing, γίνεται φανερό ότι δεν υπάρχει ορισμός καθολικά αποδεκτός. Θα αναφερθούν παρακάτω κάποιοι ορισμοί οι οποίοι

είναι αρκετά αντιπροσωπευτικοί: Σύμφωνα με τους Mell Peter, Grance Timothy (2011) το cloud computing είναι ένα μοντέλο που επιτρέπει με εύκολο τρόπο την δυνατότητα πρόσβασης σε μια φάρμα υπολογιστικών πόρων οι οποίοι είναι τα δίκτυα, οι servers, οι αποθηκευτικοί χώροι, κ.λ.π. Η πρόσβαση αυτή γίνεται με πολύ γρήγορο τρόπο και με ελάχιστη προσπάθεια ή επίβλεψη.

Ο Staten James (2008) ορίζει το cloud computing ως την "πηγή" μέσω της οποίας είναι δυνατό να αποκτήσει κανείς δυνατότητα υψηλής επεκτασιμότητας και εύκολη διαχείριση υπολογιστικών πόρων. Επιπλέον παρέχει την δυνατότητα να φιλοξενήσει εφαρμογές τελικού χρήστη και τελικά να χρεώσει σε νομισματικές μονάδες τις διευκολύνσεις αυτές ανάλογα με την χρήση των πόρων πράγμα το οποίο γίνεται απολογιστικά.

Σύμφωνα με τους Plummer D., Bittman T. (2008) το cloud computing είναι η διάσταση της πληροφορικής στην οποία είναι δυνατή η δυναμική επέκταση δυνατοτήτων, που παραδίδονται στον τελικό πελάτη σαν υπηρεσίες με την χρήση τεχνολογιών διαδικτύου, πράγμα το οποίο είναι μια κάπως διαφορετική οπτική για το τι ακριβώς είναι το cloud computing.

Για τους Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal το 2008 το cloud computing είναι ένα τύπος παράλληλου και καταμετρημένου συστήματος το οποίο αποτελείται από ένα σύνολο από διασυνδεδεμένα υπολογιστικά συστήματα, τα οποία και παρουσιάζονται σαν ένας ενιαίος υπολογιστικός πόρος, και τα οποία υλοποιούν με αρκετά δυναμικό τρόπο το επίπεδο υπηρεσιών τα οποία έχουν συμφωνηθεί εκ των προτέρων μεταξύ του παρόχου, που προσφέρει την υπηρεσία και του τελικού χρήστη.

Το NIST (National Institute of Standards and Technology) μετά από έρευνα και βασιζόμενο σε θέματα που αφορούν το cloud, προσπάθησε να δώσει τον ορισμό του με βάση την δική του άποψη. Το cloud αλλάζει συνεχώς, εξελίσσεται και έτσι μετά από εκτεταμένες συζητήσεις μεταξύ φορέων, είτε αυτοί αντιπροσωπεύουν τον ιδιωτικό τομέα είτε τον δημόσιο, ότι θα τελειοποιηθούν κάποιοι παράγοντες, οι οποίοι σχετίζονται με το cloud, όπως είναι οι περιπτώσεις χρήσης του, οι κίνδυνοι οι οποίοι παρουσιάζονται κατά την διάρκεια της χρήσης του, τα οφέλη που αποκομίζονται, καθώς και οι τεχνολογίες που σχετίζονται και χρησιμοποιούνται όταν το εφαρμόζουμε. "Όλα αυτά βέβαια θα έχουν την τάση να εξελίσσονται και να αλλάζουν προς το καλύτερο με την πάροδο του χρόνου.

Όλη η διαδικασία και αυτά που σχετίζονται με το cloud, αντιπροσωπεύουν ένα τεράστιο σύνολο, το οποίο αποτελείται από πωλητές-κατασκευαστές, διάφορα μοντέλα εφαρμογών, καθώς τμήματα της αγοράς, τα οποία έχουν κάποια εξειδίκευση πάνω στα συγκεκριμένα θέματα.

Μετά λοιπόν από αυτά ο ορισμός που δίνει το NIST, προσπαθεί να λάβει υπ' όψιν του όλες τις πιθανές προσεγγίσεις οι οποίες αφορούν το cloud, και βγαίνει από τα ακόλουθα. Το cloud λοιπόν είναι ένα μοντέλο το οποίο επιτρέπει την on-demand πρόσβαση, με την προϋπόθεση βέβαια να υπάρχει δίκτυο (internet), σε μία δεξαμενή, που θα μπορεί να επισκέπτεται ο καθένας, (δεξαμενή στην πληροφορική είναι ένα σύνολο από πόρους, οι οποίοι έχουν αρχικοποιηθεί και φυλάσσονται, ώστε μπορούν να χρησιμοποιηθούν ανά πάσα στιγμή, αντί να κατανέμονται on-demand). Επιπλέον ο χρήστης θα έχει και πρόσβαση στους υπολογιστικούς πόρους, (στα δίκτυα, στους servers, στην μνήμη, τις εφαρμογές και στις υπηρεσίες που μπορεί να προσφερθούν). Έτσι όλα αυτά θα είναι δυνατόν να προσφέρονται εύκολα, πάντα όμως σε συνεννόηση με τον πάροχο που μας εξυπηρετεί.

10.3.2 Ιστορική αναδρομή για το Cloud Computing

Η πρώτη ιδέα, η οποία αφορούσε την διανομή των υπολογιστικών πόρων μέσα από το διαδίκτυο, δημιουργήθηκε το 1960. Ο πρώτος ο οποίος χρησιμοποίησε τον επιστημονικό όρο του cloud computing, είναι ο Ramnath Chellappa, αυτό έγινε το 1997 σε μια διάλεξη που έδωσε. Κάποιοι αποδίδουν την έννοια του cloud στον John Mc Carthy ο οποίος είχε την ιδέα της διανομής των υπολογιστικών πόρων σαν μια υπηρεσία κοινής ωφέλειας όπως είναι η ΔΕΗ ή η ΕΥΔΑΠ. Από την

δεκαετία του 60' αναπτύχθηκε το cloud και μάλιστα σε πολλά επίπεδα, με αργή όμως ανάπτυξη που διατηρήθηκε μέχρι και την δεκαετία του 90' οπότε και το Internet άρχισε να προσφέρει ένα αρκετά σημαντικό εύρος ζώνης.

Όλα τα σύγχρονα χαρακτηριστικά του cloud και οι διαφορετικές μορφές του διερευνήθηκαν και παρουσιάστηκαν σε ένα βιβλίο που εκδόθηκε από τον Douglas Parkhills το 1966. Το βιβλίο αυτό έχει τον τίτλο "The Challenge of the Computer Utility".

Ο όρος cloud προήλθε από την τηλεφωνία, όπου οι διάφοροι τηλεφωνικοί πάροχοι αρχικά και μέχρι το 1990, μπορούσαν να προσφέρουν μόνο point-to-point κυκλώματα. Από εκεί όμως και μετά ανέπτυξαν την δυνατότητα να μπορούν να διαθέτουν στους συνδρομητές τους, υπηρεσίες Εικονικών Ιδιωτικών Δικτύων (τα γνωστά VPN δίκτυα), τα οποία είχαν σε αρκετά μεγάλο βαθμό, ποιότητα υψηλού επιπέδου από την μια μεριά, αλλά από την άλλη το σπουδαιότερο είναι το χαμηλό κόστος.

Το cloud στην αρχή, έβαλε τα όρια που θα υπάρχουν ανάμεσα στο κομμάτι για το οποίο ευθύνεται ο κάθε πάροχος και σε αυτό που την ευθύνη έχουν οι διάφοροι χρήστες. Με την πάροδο του χρόνου, το cloud προσπάθησε να επεκτείνει τα εν λόγω όρια, με τέτοιον τρόπο ώστε να είναι δυνατή η κάλυψη με τους servers και τις υπάρχουσες δικτυακές υποδομές. Η ιδέα του παγκόσμιου δικτύου υπολογιστών ξεκίνησε την δεκαετία του 60' από τον JCR Licklider. Με βάση αυτό το δίκτυο θα μπορούσαν όλοι, από όποιο σημείο πάνω στην γη και αν βρίσκονται, να συνδέονται μεταξύ τους, να ανταλλάσσουν πληροφορίες και δεδομένα, καθώς και να έχουν πρόσβαση σε αυτά. Αυτό λοιπόν το όραμα του JCR Licklider, μοιάζει πολύ με το cloud, πάνω και στο οποίο στηρίχθηκε η ανάπτυξή του.

Υπήρξαν πολλές εταιρείες οι οποίες ασχολήθηκαν και συνέβαλλαν στην εξέλιξη του cloud με πρώτη την εταιρεία του Salesforce το 1999. Αυτή είναι η εταιρεία η οποία πρωτοστάτησε στο να ανοίξει ο δρόμος σε άλλες εταιρείες, οι οποίες είναι εξειδικευμένες ή όχι, στο να παρέχουν εφαρμογές και υπηρεσίες μέσω του διαδικτύου.

Μια από αυτές τις εταιρείες είναι η Amazon, η οποία ξεκίνησε να αναπτύσσει νέα προϊόντα παροχής υπηρεσιών, όπως είναι το Amazon Web Service (AWS) το οποίο εισήγαγε το 2006. Ακολουθώντας την ίδια χρονιά η εν λόγω εταιρεία διέθεσε στην αγορά το Elastic Compute Cloud (EC2), το οποίο ήταν μια υπηρεσία που έδινε την ευκαιρία σε μεμονωμένους ιδιώτες καθώς και μικρές επιχειρήσεις να ενοικιάζουν δικούς τους υπολογιστές και έτσι να χρησιμοποιούν τις δικές τους εφαρμογές.

Το 2007 οι εταιρείες Google και IBM καθώς και κάποια ανώτατα εκπαιδευτικά ιδρύματα, ξεκίνησαν μια έρευνα που αφορούσε το cloud. Αργότερα στις αρχές του 2008, το Eucalyptus το οποίο είναι η πρώτη AWS API πλατφόρμα ανοιχτού κώδικα με την οποία δημιουργείται ανάπτυξη στα ιδιωτικά cloud.

Κατόπιν το 2009 το Web 2.0 έφτασε στο ύψιστο σημείο ανάπτυξής του, ενώ η Google καθώς και πολλές άλλες εταιρείες, άρχισαν να διαθέτουν κάποιες εφαρμογές browser-based, όπως είναι η εφαρμογή Google App. Με βάση την δήλωση του Steve Balmer της Microsoft που έγινε τον Μάρτιο του 2010, φαίνεται η τεράστια ανάπτυξη που θα έχει το cloud που πιθανώς να φτάσει και στο 90%.

10.3.3 Γενικά για το Cloud Computing

Το cloud computing είναι βέβαιο ότι θα έχει το αποκλειστικό ενδιαφέρον όλων των επιστημόνων, που ασχολούνται με την Τεχνολογία της Πληροφορικής, στα χρόνια που ακολουθούν.

Είναι η εξέλιξη από την μια μεριά της Τεχνολογίας Εικονικοποίησης και από την άλλη του μοντέλου Υπολογισμών Ωφέλειας. Το cloud computing είναι τεχνολογία η οποία επιτρέπει στον χρήστη να χρησιμοποιεί λογισμικό, υπηρεσίες και δεδομένα τα οποία δεν βρίσκονται αποθηκευμένα σε δικό

του υπολογιστή. Ένα από τα απολύτως απαραίτητα συστατικά του είναι η ύπαρξη του Internet, μέσα από το οποίο θα έχουν την δυνατότητα οι χρήστες να απολαμβάνουν όλες τις υπηρεσίες που πιθανώς να θέλει, χωρίς να τις αγοράζει αλλά πληρώνοντας ένα μίσθωμα, μπορεί όμως και να χρησιμοποιεί δωρεάν κάποιο χώρο τον οποίο προσφέρουν οι πάροχοι.

Ένα βασικό χαρακτηριστικό του cloud είναι η δυνατότητα κατανομής της υπολογιστικής ισχύος έτσι ώστε ο κάθε χρήστης να έχει στην διάθεσή του πιο μεγάλο μέρος αυτής της ισχύος. Έτσι αλλάζει ο τρόπος διάθεσης των υπολογιστικών πόρων, αφού παρέχεται η δυνατότητα αποθήκευσης και επεξεργασίας των δεδομένων, ενέργειες που γίνονται μέσα από το Internet και μάλιστα από όποιο σημείο και αν βρισκόμαστε. Επιπλέον οι χρήστες μπορούν να χρησιμοποιούν λειτουργικά συστήματα και εφαρμογές χωρίς να τα αγοράζουν, όπως έχει αναφερθεί, και μάλιστα να τα εγκαταστήσουν στον δικό τους υπολογιστή.

Οι υπολογιστικοί πόροι του κάθε παρόχου χρησιμοποιούνται για να εξυπηρετούν πολλούς χρήστες συγχρόνως, χρησιμοποιώντας ένα μοντέλο πολλαπλών μισθωτών. Οι πόροι αυτοί, φυσικοί ή εικονικοί, θα διατίθενται ανάλογα με την ζήτηση των καταναλωτών. Τέτοιοι πόροι είναι η επεξεργασία δεδομένων, η μνήμη, το bandwidth του δικτύου, οι αποθηκευτικοί χώροι και τέλος οι εικονικές μηχανές. Ο κάθε χρήστης μπορεί να δεσμεύει πόρους ανάλογα με τις ανάγκες του και μάλιστα αυτόματα. Οι δυνατότητες που υπάρχουν είναι διαθέσιμες και προσβάσιμες από όλους.

Το πιο σημαντικό στοιχείο του cloud είναι ότι διαθέτει Virtualization (εικονικοποίηση), μια μέθοδος ώστε οι χρήστες να έχουν την δυνατότητα να κατεβάζουν πολλά ανεξάρτητα εικονικά λειτουργικά συστήματα στον υπολογιστή τους. Οι υπολογιστικοί πόροι μπορούν να δεσμεύονται γρήγορα και ελαστικά ώστε να χρησιμοποιούνται, πολλές φορές αυτόματα και επιπλέον να φαίνεται άμεσα αν είναι διαθέσιμοι ή όχι όταν αποδεσμευτούν.

Το πιο σημαντικό πρόβλημα που παρουσιάζεται με την χρήση του cloud, είναι η εξασφάλιση της ιδιωτικότητας των πληροφοριών και των δεδομένων, έτσι ώστε να μην είναι προσβάσιμα από άτομα τα οποία δεν είναι εξουσιοδοτημένα. Απειλές βέβαια της ασφάλειας είναι δυνατόν να προκύψουν κατά την διάρκεια που εκτελούνται κάποιες εφαρμογές. Έτσι το cloud θα διαδοθεί, και μάλιστα σε μεγάλη κλίμακα, όταν θα υπάρξει από την πλευρά των χρηστών η σιγουριά, ότι εξασφαλίζονται στον μέγιστο βαθμό, η ιδιωτικότητα των πληροφοριών καθώς και των δεδομένων.

10.3.4 Αρχιτεκτονική του Cloud Computing

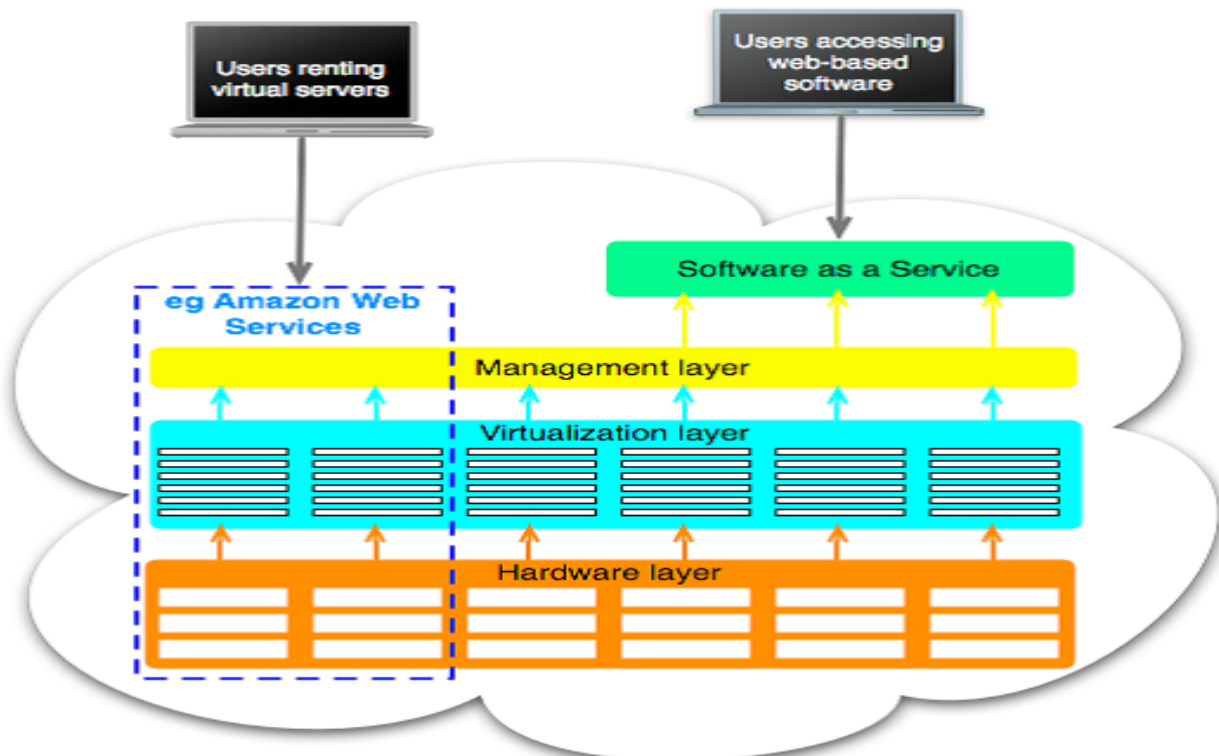
Τα βασικά αλλά και τα πιο σημαντικά μέρη πάνω στα οποία στηρίζεται η αρχιτεκτονική του cloud είναι δύο. Το πρώτο είναι το μέρος το οποίο μπορεί να βλέπει ο κάθε χρήστης και το οποίο περιλαμβάνει το δίκτυό του, τον υπολογιστή του και τις εφαρμογές τις οποίες μπορεί να χρησιμοποιεί, έτσι ώστε να έχει την επιθυμητή πρόσβαση στο cloud. Το δεύτερο μέρος είναι το ίδιο το cloud, το οποίο για να μπορεί να προσφέρει τις υπηρεσίες που επιθυμούν οι χρήστες, περιλαμβάνει μια ποικιλία από υπολογιστές, από servers καθώς και από συσκευές στα οποία υπάρχει η δυνατότητα αποθήκευσης δεδομένων.

Η κάθε υπηρεσία που προσφέρει το cloud παρέχεται ανάλογα με την χρήση που κάνει ο κάθε χρήστης (δηλαδή pay-per-use). Η διαδικασία σχετίζεται με την ανάγκη on demand συστημάτων, επειδή υπάρχει το πλεονέκτημα του να μπορεί κάποιος να έχει πρόσβαση σε δεδομένα και πληροφορίες όταν είναι συνδεδεμένος στο διαδίκτυο.

Υπάρχουν τρία επίπεδα τα οποία έχουν σχέση με την αρχιτεκτονική του cloud computing:

- Το κατώτερο επίπεδο περιλαμβάνει τα υλικά δηλαδή οι servers, οι οποίοι υπάρχουν σε κέντρα δεδομένων είτε αυτά ανήκουν σε κάποια εταιρεία, όπως είναι η Amazon και η Google και είναι δημόσια προσβάσιμα, είτε αυτά ανήκουν σε κάποιο εκπαιδευτικό ίδρυμα μόνο όμως για εσωτερική χρήση.

- Το αμέσως επόμενο επίπεδο περιλαμβάνει την τεχνολογία Virtualization (εικονικοποίησης), με την οποία έχουμε έναν server να “τρέχει” πολλούς άλλους εικονικούς και ανεξάρτητους servers.
- Το cloud όμως δεν σταματάει εδώ. Σε τελικούς χρήστες, μέσω του διαδικτύου, παρέχεται λογισμικό το οποίο ονομάζουμε SoftWare as a Service (δηλαδή λογισμικό σαν Υπηρεσία). Έτσι λοιπόν το λογισμικό είναι ένα ακόμα επίπεδο στο οποίο οι χρήστες μπορούν να έχουν πρόσβαση μέσω ενός Web browser ή μέσα από ένα εργαλείο το οποίο θα πρέπει να είναι συμβατό με το Web.



Σχήμα 10.2: Ένα απλό μοντέλο επιπέδων του «cloud»

10.3.5 Τι είναι το cloud computing

Το cloud είναι ένα μοντέλο το οποίο επιτρέπει μια on demand ευέλικτη πρόσβαση σε ένα σύνολο από υπολογιστικούς πόρους, το οποίο μπορεί να τροφοδοτείται γρήγορα και με ελάχιστη προσπάθεια διαχείρισης.

Το cloud computing προσφέρει διαρκή διαθεσιμότητα και αποτελείται από πέντε θεμελιώδη χαρακτηριστικά, τέσσερα μοντέλα πρακτικής εφαρμογής και τέλος τρία μοντέλα παροχής υπηρεσιών.

Τα πέντε θεμελιώδη χαρακτηριστικά:

- η ικανοποίηση της ζήτησης (on demand self service), με την οποία προσφέρονται από τους παρόχους υπηρεσιών, μονομερώς, σε καταναλωτές υπολογιστικοί πόροι για όσο διάστημα τους χρειάζονται.
- ένα άλλο χαρακτηριστικό είναι η ευρεία πρόσβαση στο δίκτυο (broad network access), στο οποίο οι υπηρεσίες που προσφέρονται είναι διαθέσιμες μέσω του διαδικτύου χρησιμοποιώντας διάφορες συσκευές όπως κινητά τηλέφωνα, laptops, PDAs κλπ.
- ακολουθεί η διαθεσιμότητα των πόρων (resource pooling), με την οποία οι υπολογιστικοί πόροι των παρόχων συγκεντρώνονται, ώστε να μπορούν να εξυπηρετήσουν πολλούς χρήστες, χρησιμοποιώντας ένα μοντέλο multi-tenant και διατίθενται αναλόγως με την ζήτηση που θα υπάρχει.
- το τέταρτο χαρακτηριστικό είναι η ευελιξία της επεκτασιμότητας (rapid elasticity), με την οποία οι υπηρεσίες που προσφέρονται από το cloud διατίθενται γρήγορα και με μεγάλη προσαρμοστικότητα και σε κάποιες περιπτώσεις αυτό γίνεται αυτόματα.
- τέλος το τελευταίο χαρακτηριστικό είναι η τιμολόγηση βάσει της χρήσης (a measured service), με την οποία τα συστήματα του cloud ελέγχουν αυτόματα και βελτιώνουν, όταν χρειάζεται, την χρήση των υπολογιστικών πόρων, χρησιμοποιώντας δυνατότητες μέτρησης. Την χρήση των πόρων μπορούμε να την παρακολουθήσουμε, να την ελέγξουμε και να την καταγράψουμε, παρέχοντας έτσι την απαιτούμενη διαφάνεια για τον χρήστη αλλά και για τον πάροχο, όσον αφορά την χρησιμοποιούμενη υπηρεσία.

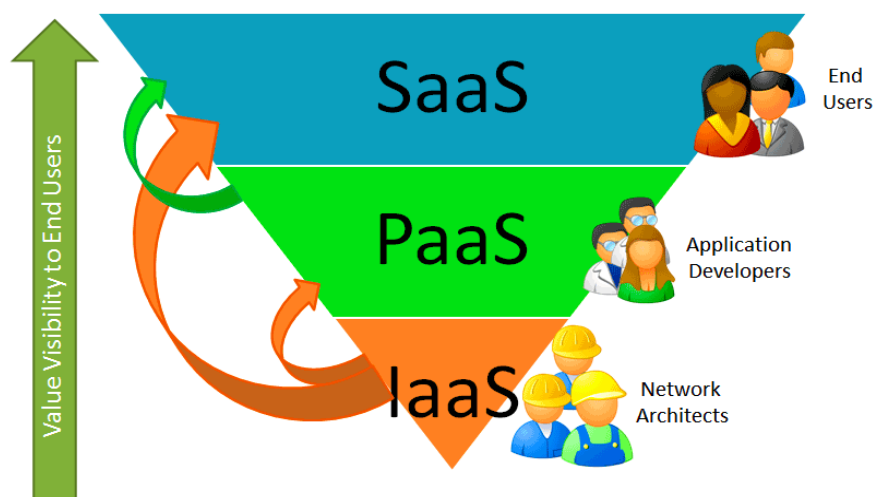
Τα τέσσερα μοντέλα πρακτικής εφαρμογής (ανάπτυξης):

- Private cloud (ιδιωτικό): είναι το cloud το οποίο έχει δημιουργηθεί για την χρήση αποκλειστικά και μόνο από τους χρήστες. Υπάρχουν αρκετές παραλλαγές, αυτού του μοντέλου ανάπτυξης, ανάλογα με το καθεστώς που ισχύει στον κάθε πάροχο, καθώς και τα χαρακτηριστικά της λειτουργίας του. Στο κάθε ιδιωτικό cloud υπάρχει περίπτωση να ανήκει στην ιδιοκτησία του κάθε χρήστη, ενώ η εγκατάσταση, η λειτουργία και η συντήρηση είναι θέματα που αφορούν τους παρόχους. Κάποιες από τις υπάρχουσες υποδομές, όπως π.χ. οι servers, μπορεί να βρίσκονται ή στην πλευρά των πελατών ή στην πλευρά των παρόχων.
- Community cloud (κοινοτικό): είναι το cloud στο οποίο κάποιοι από τους χρήστες, οι οποίοι όμως έχουν ίδιες ανάγκες, αποφασίζουν, για δικούς τους λόγους (π.χ. οικονομικούς), να μοιράζονται τις υποδομές, τις παραμετροποιήσεις, αλλά και αποκλειστική ευθύνη της διαχείρισης των υποδομών του cloud. Ας σημειωθεί ότι η διαχείριση σε αυτό το μοντέλο ανάπτυξης γίνεται είτε από κάποιο μέλος που ανήκει στην ίδια κοινότητα είτε ακόμα και από κάποιον τρίτο για τον οποίο υπάρχει συμφωνία μεταξύ των μελών της κάθε κοινότητας.

- Public cloud (δημόσιο): είναι το cloud στο οποίο η ιδιοκτησία ανήκει αποκλειστικά στον κάθε πάροχο υπηρεσιών. Το δημόσιο cloud στηρίζει αρκετές εφαρμογές, τις οποίες μπορούν να χρησιμοποιούν οι χρήστες, με αντάλλαγμα όμως κάποιο είδος ενοικίου, το οποίο έχει συμφωνηθεί, ανάλογα βέβαια με την χρήση των υπηρεσιών που κάνουν.
- Hybrid cloud (υβριδικό): είναι το cloud το οποίο αποτελείται από την σύνθεση πολλών cloud (δύο και άνω), τα οποία όμως παραμένουν αυτόνομα και συνδέονται μεταξύ τους με τέτοια τεχνολογία, η οποία επιτρέπει την φορητότητα στα δεδομένα και στις διάφορες εφαρμογές. Μπορεί βέβαια να θεωρηθεί σαν υβριδικό cloud και οποιοσδήποτε συνδυασμός μεταξύ των τριών μοντέλων ανάπτυξης τα οποία αναφέρθηκαν προηγούμενα.

Μοντέλα παροχής υπηρεσιών:

- Cloud Software as a Service (SaaS): σε αυτό το μοντέλο, δίνεται η δυνατότητα στους χρήστες, να χρησιμοποιούν τις διάφορες εφαρμογές που προσφέρει ο κάθε πάροχος. Σε αυτές τις εφαρμογές οι πελάτες των παρόχων, έχουν πρόσβαση χρησιμοποιώντας διάφορες client συσκευές, μέσα από ένα πρόγραμμα περιήγησης, (ένα thin client interface), όπως είναι το Web. Στην περίπτωση αυτή οι χρήστες δεν έχουν τον έλεγχο και την διαχείριση των διάφορων υποδομών cloud που χρησιμοποιεί.
- Cloud Platform as a Service (PaaS): στην συγκεκριμένη περίπτωση προσφέρεται η δυνατότητα στους πελάτες των παρόχων, να αναπτύσσουν καθώς και να έχουν τον έλεγχο των διάφορων εφαρμογών cloud, τις οποίες είτε έχουν αποκτήσει είτε έχουν δημιουργήσει οι ίδιοι, χωρίς όμως να ασκούν τον έλεγχο και την διαχείριση των υποδομών cloud.
- Cloud Infrastructure as a Service (IAAS): τέλος σε αυτό το μοντέλο παροχής υπηρεσιών δίνεται η δυνατότητα ώστε να μπορούν οι χρήστες να δεσμεύουν για να χρησιμοποιήσουν την επεξεργαστική ισχύ που είναι προς διάθεση, καθώς και αποθηκευτικά μέσα, δίκτυα αλλά και κάποιους άλλους υπολογιστικούς πόρους. Επιπλέον οι καταναλωτές μπορούν να εκτελούν και να αναπτύσσουν δικό τους λογισμικό, το οποίο μπορεί να περιέχει εφαρμογές, ακόμα και λειτουργικά συστήματα. Όμως οι χρήστες δεν μπορούν να ελέγχουν και να διαχειρίζονται τις cloud υποδομές, μπορούν όμως να ελέγχουν τους αποθηκευτικούς χώρους, τις εφαρμογές που έχουν αναπτυχθεί καθώς και τα διάφορα λειτουργικά συστήματα. Εκτός αυτών πιθανώς να μπορεί και να ελέγχει, σε περιορισμένο όμως βαθμό, κάποιον δικτυακό εξοπλισμό όπως είναι το Firewalls.



Σχήμα 10.3: Μοντέλα υπηρεσιών του «cloud»

10.3.6 Σημαντικές Έννοιες

Εικονικοποίηση Virtualization

Ο εν λόγω όρος πρωτοεμφανίστηκε την δεκαετία του 1960. Η πλατφόρμα αυτή εκτελείται σε ένα συγκεκριμένο υπολογιστή, από ένα λογισμικό που λέγεται control program. Η μέθοδος αυτή σε υπολογιστές ή λειτουργικά συστήματα αποκρύπτει από τους χρήστες τα χαρακτηριστικά μιας πλατφόρμας. Επιπλέον αποτελεί μια βάση για όλες τις αρχιτεκτονικές cloud και δίνει την δυνατότητα να μπορούν να συγκεντρώνονται οι υπολογιστικοί πόροι και τα κέντρα δεδομένων και έτσι να δημιουργείται ένας πόρος για τον οποίο υπάρχει η δυνατότητα να διαμοιράζεται σε όλες τις εφαρμογές.

Η μέθοδος virtualization επιτρέπει πιο μεγάλη αποτελεσματικότητα και ευελιξία, χωρίς βέβαια να υπάρχει κάποια επίπτωση στην παραγωγικότητα του διαχειριστή του συστήματος ή στα εργαλεία και στις διαδικασίες. Τώρα παρά το ότι πολλοί από τους παρόχους στρέφονται στην χρήση της μεθόδου της εικονικοποίησης, ώστε να μειώνουν τις κεφαλαιακές και τις λειτουργικές τους δαπάνες, στόχος τελικά του cloud είναι να υπάρξει ένας διαχωρισμός μεταξύ των εφαρμογών και των υποδομών του.

Κατά ζήτηση (On-demand)

Η on demand διάθεση των πόρων είναι μια από τις βασικές προϋποθέσεις, που θα πρέπει να ικανοποιεί ο κάθε πάροχος υπηρεσιών cloud ώστε να μπορεί να διαθέτει στους πελάτες του υπολογιστικούς πόρους όταν τους χρειάζονται. Επιπλέον είναι μια από τις βασικές παροχές τις οποίες επιθυμούν να έχουν οι επιχειρήσεις κυρίως, από τους παρόχους, ώστε να αποφεύγουν μια περιττή επένδυση που αφορά τους υπολογιστικούς πόρους, αφού σε αντίθεση με το παραδοσιακό μοντέλο, στο cloud δεν χρειάζεται να διατηρούν δικούς τους πόρους. Με αυτόν τον τρόπο μειώνουν το κόστος επειδή κάποιοι από τους πόρους δεν θα χρησιμοποιούνται σε μεγάλη έκταση. Συνέπεια αυτού είναι ότι οι προμηθευτές λογισμικού θα μπορούν να αναπτύσσουν κάποιες εφαρμογές χωρίς να χρειάζεται από προηγουμένως να έχουν ένα συγκεκριμένο αριθμό πελατών.

Πληρωμή ανάλογα με την χρήση (pay-per-use)

Η δυνατότητα pay-per-use είναι μία από τις πολλές πτυχές του cloud, η οποία βασίζεται στην χρέωση. Οι χρήστες πληρώνουν μόνο όταν χρησιμοποιούν τους υπολογιστικούς πόρους και φυσικά αυτή η χρήση είναι μετρήσιμη π.χ. σε ώρες, ημέρες κλπ, μετατρέποντας έτσι τις κεφαλαιακές σε λειτουργικές δαπάνες. Οι πόροι που διατίθενται βρίσκονται κάπου μέσα στο cloud και όχι σε κάποια φυσική τοποθεσία. Αυτό βέβαια το οποίο συμφέρει τους παρόχους υπηρεσιών είναι ότι οι επιχειρήσεις κυρίως πρέπει να αξιοποιούν ολόκληρη ή σχεδόν ολόκληρη την επεξεργαστική ισχύ.

Υπολογισμοί ωφέλειας (Utility computing)

Οι υπολογισμοί ωφέλειας γίνονται από μια υπηρεσία που μετράει τους υπολογιστικούς πόρους και λειτουργεί όπως οι εταιρείες παροχής ηλεκτρικού ρεύματος, νερού, φυσικού αερίου ή τηλεφωνίας. Αυτό έχει ένα πλεονέκτημα ότι το κόστος αρχικά, για να αποκτηθούν οι πόροι, είναι πολύ χαμηλό έως και μηδενικό. Το έτος 2002 είναι το έτος κατά το οποίο ξεκίνησαν πολλές εταιρείες, όπως είναι η IBM, η HP και η Microsoft να καθιερώνουν την χρήση των υπολογισμών ωφέλειας. Το 2008 όμως οι εταιρείες Google και Amazon πήραν την πρωτοπορία και καθιέρωσαν τις δικές τους Utility εφαρμογές και υπηρεσίες. Το Utility Computing ενσωματώνει και ένα είδος εικονικοποίησης (virtualization), έτσι ώστε η μνήμη και η υπολογιστική ισχύς που είναι προς διάθεση, να έχουν την δυνατότητα να είναι κατά πολύ μεγαλύτερες από αυτές που έχουν μεμονωμένοι υπολογιστές, διαμοιράζοντας τον χρόνο. Έτσι δημιουργείται η ανάγκη για την ύπαρξη πολλών servers, οι οποίοι μπορεί να είναι μια ομάδα από υπολογιστές, οι οποίοι είναι εξειδικευμένοι, η οποία δημιουργήθηκε αποκλειστικά για τον σκοπό της εκμίσθωσης.

10.3.7 Εναλλακτικοί και χρήσιμοι τρόποι χρήσης των cloud υπηρεσιών

Το cloud δεν το χρησιμοποιούμε μόνο για αποθήκευση, διαμοιρασμό και back up, αλλά και για πολλές καθημερινές χρήσεις όπως οι δικτυακές εφαρμογές και υπηρεσίες π.χ. διάφορες μορφές mail (gmail, hotmail, yahoo! κλπ).

Άλλη υπηρεσία είναι αυτή που αφορά μουσική με χαρακτηριστικά παραδείγματα το Sound cloud, το iTunes κλπ.

Οι διάφορες δικτυακές σουίτες γραφείου όπως το Zoho, το Google Docs, το Office-365 κλπ.

Οι διάφορες εφαρμογές παιχνιδιών τα οποία αναπτύσσονται με την λογική του cloud. Την ανάπτυξη τους βέβαια την βοήθησε πολύ η ταχεία ανάπτυξη των φορητών συσκευών (Smartphone).

Μεγάλη εφαρμογή του cloud συναντάμε στην εκπαίδευση όπου μπορούν να χρησιμοποιούνται πλήθος από εκπαιδευτικά λογισμικά, από καθηγητές και μαθητές, χρησιμοποιώντας οποιονδήποτε ηλεκτρονικό υπολογιστή, αρκεί να έχει πρόσβαση στο δίκτυο. Όλοι έχουν πρόσβαση σε αποθηκευτικούς χώρους και ισχύ τα οποία είναι ανεξάντλητα.

10.3.8 Πλεονεκτήματα της χρήσης της τεχνολογίας cloud

Πολλά πλεονεκτήματα της χρήσης της τεχνολογίας του cloud αναφέρονται ακολούθως:

- Μείωση του χρόνου που χρειάζεται για την εγκατάσταση, την αναβάθμιση και την ενημέρωση των λογισμικών αφού όλα αυτά τα αναλαμβάνει το cloud.
- Δεν χρειάζεται να διατηρείται και να συντηρείται οποιαδήποτε υψηλή τεχνολογία σε υψηλό επίπεδο.

- Υπάρχει στην διάθεση του καθενός και οποιαδήποτε στιγμή, λογισμικό και δεδομένα, από κάθε φορητή συσκευή, η οποία μπορεί να έχει πρόσβαση στο διαδίκτυο.
- Η ασφάλεια των δεδομένων είναι εξασφαλισμένη αφού αποθηκεύονται σε πολλά αντίγραφα και σε διαφορετικές τοποθεσίες.
- Τέλος το cloud συμβάλλει σε μεγάλο βαθμό στην προστασία του περιβάλλοντος αφού μειώνεται κατά πολύ η χρήση των υλικών υπολογιστικών πόρων και η απαιτούμενη ενέργεια άρα έχουμε λιγότερες εκπομπές ρύπων.

10.3.9 Πάροχοι υπηρεσιών cloud

Σήμερα υπάρχουν πολλές εταιρείες, οι οποίες δραστηριοποιούνται στον χώρο κυρίως της πληροφορικής, που προσφέρουν σε απλούς χρήστες, αλλά και επιχειρήσεις, διάφορες υπηρεσίες cloud. Θα ακολουθήσει ένας συγκεντρωτικός πίνακας στον οποίο αναφέρονται οι κυριότεροι από τους εν λόγω παρόχους υπηρεσιών cloud:

Cloud computing	Cloud storage
Amazon	Amazon S3
Microsoft	Intermap XIPCloud Storage
Flexiant	Nirvanix
Google	Windows Azure
OneNet	PhoneKlone
Joyent	Dropbox
Rackspase Cloud	Box.net
Salesforce	
Skytap	
Jitscale	
Tata IAAS	
DedicatedNow	

Σχήμα 10.4: Συγκεντρωτικός πίνακας παρόχων υπηρεσιών «νέφους»

10.3.10 Υπηρεσίες cloud της Google

Η εταιρεία Google είναι μια από τις πρώτες εταιρείες στην προσφορά υπηρεσιών cloud και γι' αυτό έχουν καθιερωθεί στον χώρο. Οι υπηρεσίες που μπορεί να προσφέρει είναι η Google Apps και η Google App Engine.

Η Google Apps είναι μια σουίτα η οποία προσφέρει πολλές υπηρεσίες όπως είναι το Google Groups όπου ο κάθε χρήστης μπορεί να διαχειρίζεται ομάδες χρηστών, να ελέγχει ποιος έχει πρόσβαση. Τα μέλη της ομάδας μπορούν να μετέχουν σε συζητήσεις μεταξύ τους.

Επίσης το Google Docs είναι μια δωρεάν υπηρεσία, η οποία επιτρέπει στους χρήστες να διαμοιράζονται έγγραφα και υπολογιστικά φύλλα καθώς και να συνεργάζονται σε παρουσιάσεις.

Το Google Sites είναι ένας τρόπος για να μπορεί μα δημιουργήσει κάποιος εύκολα ασφαλείς ιστοσελίδες για intranet και ομαδικά έργα.

Εκτός από τα παραπάνω η Google Apps προσφέρει το Google Calendar, ένα ημερολόγιο με ραντεβού όμοιο με αυτό του Outlook. Τέλος με το Google Video οι εργαζόμενοι μπορούν να μοιραστούν Video με τους συναδέλφους τους, πάντα βέβαια με ασφάλεια, χωρίς να αποκαλύπτονται εμπιστευτικές πληροφορίες.

Η Google App Engine υπηρεσία επιτρέπει στους χρήστες να κατεβάζουν Web εφαρμογές στους server της Google. Υποστηρίζει Java και Python εφαρμογές. Προσφέρει ταχεία ανάπτυξη, εγκατάσταση, απλή διαχείριση καθώς και προσαρμοστικότητα, χωρίς ο χρήστης να καταβάλλει ιδιαίτερη προσπάθεια και να χρειάζεται να ασχοληθεί με το υλικό, τα patches ή τα backup.

10.3.11 Πιθανά οφέλη από τη χρήση του cloud και ζητήματα προς επίλυση

Υπάρχουν πάρα πολλά οφέλη από την χρήση του cloud, τα οποία αναφέρονται συνοπτικά στον πίνακα που ακολουθεί:

ΟΦΕΛΗ	ΠΕΡΙΓΡΑΦΗ
Τιμολόγηση υπηρεσίας	Οι χρήστες πληρώνουν μόνο για όσο χρησιμοποιούν τις υπηρεσίες
Προσαρμοστικότητα	Οι χρήστες μπορούν να αυξήσουν ή να μειώσουν το επίπεδο χρήσης των υπολογιστικών πόρων και των υπηρεσιών εύκολα και εύκολα
Virtualized πόροι	Εξαιτίας της ανάγκης για multi-tenancy το «νέφος» δεν θα ήταν εφικτό χωρίς την μέθοδο virtualization
Αυτοματοποίηση της διαχείρισης	Οι πλατφόρμες «νέφους» διαφέρουν από τα παραδοσιακά κέντρα δεδομένων στην ύπαρξη τυποποίησης.
Self-service παροχή υπηρεσιών	Δυνατότητα παροχής υπηρεσιών χωρίς βοήθεια
Ιδιοκτησιακό καθεστώς από τρίτους	Μεταβίβαση της ιδιοκτησίας πόρων σε τρίτους που ειδικεύονται στην διαχείρισή τους
Διαχειρίσιμες λειτουργίες	Η διαχείριση της υποδομής γίνεται από “τρίτα μέρη”
Πρόσβαση	Πρόσβαση σε πόρους για οποιονδήποτε διαθέτει μια συσκευή με πρόσβαση στο Διαδίκτυο
Συνεργασία	Προάγει την συνεργασία και προωθεί την ευρύτερη ανταλλαγή πληροφοριών
Αυξημένη υπολογιστική ισχύς	Ο χρήστης μπορεί να εκτελέσει δυσκολότερες υπολογιστικές εργασίες χρησιμοποιώντας την υπολογιστική ισχύ χιλιάδων υπολογιστών και server
Απεριόριστη αποθηκευτική χωρητικότητα	Το «νέφος» προσφέρει σχεδόν απεριόριστη αποθηκευτική χωρητικότητα.
Αποδέσμευση από συγκεκριμένες συσκευές	Αποδέσμευση από έναν μόνο υπολογιστή ή δίκτυο, από συγκεκριμένη έκδοση ενός προγράμματος για κάποια συσκευή ή αποθήκευση κάποιου έγγραφου σε μια συγκεκριμένη μορφή ώστε να είναι συμβατό με μια συσκευή
Διαθεσιμότητα	Οι πάροχοι έχουν την υποδομή και το εύρος ζώνης να καλύψουν τις απαιτήσεις των χρηστών για πρόσβαση υψηλής ταχύτητας, μνήμη και εφαρμογές
Ειδίκευση	Γνώσεις ειδικευμένων διαμοιράζονται μεταξύ πολλών πελατών

Σχήμα 10.5: Οφέλη από την χρήση του cloud

Τα ζητήματα που προκύπτουν από την χρήση του cloud και τα οποία πρέπει να επιλυθούν αναφέρονται συνοπτικά στον παρακάτω πίνακα:

ΖΗΤΗΜΑΤΑ ΠΡΟΣ ΕΠΙΛΥΣΗ	ΠΕΡΙΓΡΑΦΗ
Έλλειψη προτύπων αγοράς	Δεν υπάρχουν κοινά πρότυπα αγοράς για όλους του παρόχους υπηρεσιών, τα «νέφη» δεν είναι διαλειτουργικά
Ποιότητα υπηρεσιών	Κάποια από τα ζητημάτων είναι: α) εξαρτάται πλήρως από την σύνδεση που διαθέτουμε β) η δέσμευση μ' έναν πάροχο μπορεί να δημιουργήσει θέματα αξιοπιστίας γ) ελλιπής νομοθεσία

Σχήμα 10.6: Ζητήματα προς επίλυση του cloud

Πιο αναλυτικά όμως τα ζητήματα αυτά θα αναφερθούν ακολούθως:

Έλλειψη προτύπων αγοράς

Το cloud στα αρχικά στάδια της ανάπτυξής του, είχε πρόβλημα λόγω της έλλειψης προτύπων αγοράς. Η αγορά τότε ήταν πολύ ρευστή και έτσι η πιθανή δέσμευση κάποιου χρήστη με οποιονδήποτε πάροχο υπηρεσιών, ενδέχεται να είχε αρνητικές συνέπειες. Ο κάθε πάροχος χρησιμοποιεί διαφορετικές τεχνολογίες με αποτέλεσμα να μην είναι δυνατή η μεταφορά εφαρμογών στο cloud και απλά να αναμένει ο κάθε χρήστης απλά να εκτελεστούν.

Ποιότητα υπηρεσιών (Quality of Service- QoS)

Ένα άλλο θέμα για επίλυση είναι η ποιότητα των υπηρεσιών του cloud. Το πρώτο βασικό ζήτημα είναι ότι χωρίς Internet, cloud δεν υφίσταται, όπως και με χαμηλές ευρυζωνικές ταχύτητες, γιατί τότε προκύπτουν προβλήματα στην απόδοση. Έχουν υπάρξει κάποια προβλήματα πρόσβασης στο cloud από κάποιες μεγάλες εταιρείες, όπως η Google και η Amazon, μόνο όμως προσωρινά για λίγες ώρες. Επίσης δεν προσαρμόζονται εύκολα οι διάφορες Συμφωνίες Επιπέδου Υπηρεσιών με τις ιδιαίτερες ανάγκες που έχει η κάθε επιχείρηση-πελάτης και οι αποζημιώσεις για τους νεκρούς χρόνος πιθανόν να είναι ανεπαρκείς. Τέλος η υπάρχουσα νομοθεσία, η οποία αφορά το cloud, είναι ελλιπής και γι' αυτό είναι σημαντικό στο συμβόλαιο μεταξύ παρόχων και χρηστών, (ιδιαίτερα επιχειρήσεων), να είναι εμφανή τα θέματα για τα οποία ο κάθε πάροχος φέρει ευθύνη και είναι υπόλογος.

Ασφάλεια-Ιδιωτικότητα

Είναι δύο από τα πιο σοβαρά ζητήματα που αφορούν τα cloud, σχετίζονται με την αποθήκευση και την ασφάλεια των δεδομένων και επιπλέον αφορούν την παρακολούθηση στην χρήση του cloud, από την πλευρά των παρόχων. Για να υπάρξει ανάπτυξη του cloud θα πρέπει να υπάρχουν εγγυήσεις οι οποίες να εξασφαλίζουν και ασφάλεια και ιδιωτικότητα.

Απειλές που αφορούν την ασφάλεια καθώς και την ιδιωτικότητα μπορούν να είναι κάποιες από αυτές που αναφέρονται ακολούθως:

Οι πελάτες των πιο πολλών παρόχων υπηρεσιών IaaS, έχουν ανωνυμία, πράγμα που εκμεταλλεύονται οι διάφοροι Spammers, οι οποίοι μπορούν να δρουν χωρίς να τιμωρούνται.

Οι διάφοροι πάροχοι, οι οποίοι παρέχουν στους χρήστες ένα σύνολο από διεπαφές λογισμικού ή API, από την ασφάλεια των οποίων, εξαρτάται η ασφάλεια και η διαθεσιμότητα των υπηρεσιών που προσφέρονται.

Ένα άλλο πρόβλημα είναι η απώλεια και η διαρροή δεδομένων που βρίσκονται στο cloud και τα οποία μπορεί να χαθούν, όταν δεν υπάρχουν τοπικά αντίγραφα. Αυτά τα προβλήματα επιδεινώνονται επειδή τα διάφορα μέρη μιας εφαρμογής μπορεί να βρίσκονται σε διαφορετικά σημεία μέσα στο cloud, επιπλέον τα εργαλεία διαχείρισης των συστημάτων του cloud δεν είναι ενοποιημένα και τέλος οι χρήστες υπάρχει περίπτωση να χάσουν τον έλεγχο των δεδομένων τους επειδή δεν υπάρχουν επαρκή εργαλεία που να μπορούν να το εξασφαλίσουν.

10.3.12 Η υπηρεσία Pithos

Η υπηρεσία Pithos είναι ένα παράδειγμα το οποίο στηρίζεται κυρίως στο cloud. Ανήκει στο υπουργείο Παιδείας και ιδιαίτερα στο τμήμα Έρευνας και Τεχνολογίας του Υπουργείου. Η διαχείριση της εφαρμογής γίνεται από το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ). Η Pithos, διαθέτει στον κάθε χρήστη μέχρι 50 Gbytes αποθηκευτικού χώρου, ο οποίος μπορεί να χρησιμοποιηθεί on line, με ασφαλή πρόσβαση από οπουδήποτε.

Η υπηρεσία Pithos διατίθεται δωρεάν, σε φοιτητές αλλά και σε άλλα μέλη της Πανεπιστημιακής Κοινότητας. Πιο συγκεκριμένα προσφέρονται οι εξής δυνατότητες:

- Για τον προσωπικό χώρο αποθήκευσης των χρηστών υπάρχει η δυνατότητα οργάνωσής του με την μορφή καταλόγων-υποκαταλόγων.
- Μπορεί ακόμη το κάθε αρχείο να σχετίζεται με ένα ή και περισσότερα Tags (ετικέτες).
- Δύναται να εκτελεστεί κάποια αναζήτηση κειμένου, κάποιου περιεχομένου αυτού καθώς και των Tags των αρχείων.
- Υπάρχει κάδος αρχείων, με την ευχέρεια ανάκτησης σβησμένων αρχείων.
- Για κάθε αρχείο υφίσταται αρχείο, για το ιστορικό των αλλαγών που πιθανόν γίνονται.
- Το κάθε αρχείο μπορεί να είναι προς διάθεση σε άλλους χρήστες της υπηρεσίας Pithos, με το δικαίωμα να το διαβάζουν ή να το τροποποιούν ή ακόμα και να κάνουν τροποποίηση δικαιωμάτων.
- Οποιοδήποτε αρχείο μπορεί να είναι προς διάθεση για να ανακτηθεί εκτός συστήματος (unauthenticated download).

Προϋπόθεση για την πρόσβαση χρηστών στην υπηρεσία Pithos, είναι να έχουν λογαριασμό σε κάποιο Ανώτερο ή Ανώτατο Εκπαιδευτικό Ίδρυμα. Η πρόσβαση στην Pithos μπορεί να γίνει με

τρεις τρόπους: μέσα από έναν browser, μέσα από μια ανεξάρτητη εφαρμογή και τέλος μέσα από ένα πρόγραμμα Firefox Plugin (ένα σύστημα συστατικών κάποιου λογισμικού, το οποίο προσθέτει δυνατότητες στο μεγαλύτερο λογισμικό του Firefox, για την επίδειξη π.χ. κάποιων νέων αρχείων).

Από την πλευρά των Εκπαιδευτικών Ιδρυμάτων, η μοναδική απαίτηση είναι οι χρήστες να είναι συνδεδεμένοι με την υποδομή Shibboleth του Ε.Δ.Ε.Τ. ΑΕ.

10.3.13 Το Chromebook

Το Chromebook είναι μια απόδειξη ότι το cloud μετέχει ενεργά στις διάφορες εφαρμογές της πληροφορικής. Είναι ένας φορητός υπολογιστής ο οποίος χρησιμοποιεί το λειτουργικό σύστημα Crome OS της Google, έχει μεγάλες ταχύτητες, ασφάλεια και μεγάλη αυτονομία. Κάποια χαρακτηριστικά του είναι ότι άμεσα μετά την εκκίνηση μπορεί να συνδεθεί με κάποιο ασύρματο δίκτυο. Επιπλέον οι εφαρμογές, οι ρυθμίσεις και τα έγγραφα είναι αποθηκευμένα στο cloud και έτσι αν ο χρήστης χάσει ή αν ακόμα χαλάσει το Chromebook του, δεν έχει πρόβλημα γιατί μπορεί να χρησιμοποιήσει κάποιο άλλο χωρίς πρόβλημα, γιατί θα έχει πρόσβαση στα αρχεία του και στα δεδομένα του. Οι διάφορες ενημερώσεις εκτελούνται αυτόματα χωρίς να υπάρχει παρέμβαση του κάθε χρήστη. Έχει όμως και ένα μειονέκτημα, ότι δεν μπορεί να χρησιμοποιηθεί στην περίπτωση που δεν υπάρχει δίκτυο, είναι δηλαδή ουσιαστικά ένα είδος Laptop το οποίο είναι συνεχώς συνδεδεμένο με το διαδίκτυο. Μπορούν να συνδεθούν στο διαδίκτυο μέσω Wi-Fi και 3 G. Για το θέμα της ασφάλειας που είναι σοβαρό, η εταιρεία κατασκευής εγγυάται πως το λειτουργικό σύστημα του Chromebook, έχει κατασκευαστεί με τέτοιο τρόπο ώστε να αμύνεται σε απειλές από malware και ιούς και επίσης έχει πολλά επίπεδα προστασίας γιατί χρησιμοποιεί ανάμεσα σε άλλα και κρυπτογράφηση σε δεδομένα και εκτός αυτού ζητά επαλήθευση όταν είναι στο στάδιο της εκκίνησης. Είναι έτοιμο να χρησιμοποιηθεί μόλις μετά 8 sec από την στιγμή που θα πατηθεί το κουμπί της έναρξης και τέλος έχει αυτονομία ενέργειας από 6 έως 8,5 ώρες, σε αντίθεση με τα συμβατικά laptops, τα οποία έχουν από 3 έως 4 ώρες αυτονομία. Ένα βασικό μειονέκτημα των Chromebooks, είναι ότι τα πιο ακριβά, τα οποία είναι και καλύτερης ποιότητας, όμως οι τιμές τους είναι τέτοιες που δεν βοηθάνε στις πωλήσεις τους.

10.4 Internet of Things

10.4.1 Εισαγωγή

Το Internet of Things (IoT) είναι ένα σύνολο από διάφορα αντικείμενα ή υποδομές όπως είναι συσκευές, οχήματα, κτίρια καθώς και λειτουργικά συστήματα τα οποία είναι διασυνδεδεμένα με το διαδίκτυο λειτουργούν ανεξάρτητα, αυτόνομα και μπορούν να συγκεντρώνουν καθώς και να ανταλλάσσουν δεδομένα και πληροφορίες μεταξύ τους.

Στην συνέχεια όλες οι εφαρμογές και τα πρότυπα που θα χρησιμοποιηθούν, θα πρέπει να έχουν συμβατότητα με το ήδη υπάρχων δίκτυο που λειτουργεί σήμερα. Επιπλέον έχουν δημιουργηθεί καινούργια πρωτόκολλα τα οποία υποστηρίζουν το IoT, αφού τα ήδη υπάρχοντα δεν είναι αρκετά.

Στο IoT υπάρχει η ευχέρεια, να γίνεται έλεγχος, διασυνδεδεμένων αντικειμένων, συσκευών, οχημάτων, κτιρίων κλπ, από μακριά, με απαραίτητη προϋπόθεση την ύπαρξη της ανάλογης δικτυακής υποδομής. Αυτός είναι ο λόγος που αυτά είναι εξοπλισμένα με αισθητήρες και ενεργοποιητές. Το IoT είναι ένα σύνολο από έξυπνα συστήματα, τα οποία γνωρίζουν μεγάλη ανάπτυξη και εξέλιξη με πολλά παραδείγματα όπως είναι τα έξυπνα σπίτια, οχήματα αλλά και πόλεις. Το καθένα σύστημα ή αντικείμενο που είναι διασυνδεδεμένο έχει το δικό του μοναδικό αναγνωριστικό καθώς και ένα ενσωματωμένο υπολογιστικό σύστημα το οποίο μπορεί να λειτουργεί αυτόνομα ή ακόμα και σε συνεργασία με όλη την δικτυακή υποδομή.

Το IoT γνώρισε μεγάλη ανάπτυξη λόγω της διάδοσης του ασύρματου Internet και των αισθητήρων. Από το 1991 άρχισε η συζήτηση που αφορούσε το IoT, αλλά ουσιαστικά αυτό που πρώτος έθεσε αυτόν τον όρο (του IoT) ήταν ο Kevin Ashton το 1999, αυτός ήταν και ο πρώτος που βρήκε τον τρόπο ώστε να μπορούν να συνδεθούν αντικείμενα με το διαδίκτυο μέσω των RFID, που είναι προϋπόθεση για την λειτουργία του IoT. Οι RFID είναι ετικέτες ραδιοσυχνότητας και μάλιστα είναι η εξέλιξη των Barcode.

Σύμφωνα με το Gartner, θα υπάρξει τεράστια ανάπτυξη του IoT, τέτοια που μέχρι το 2020 θα υπάρχουν διασυνδεδεμένες σχεδόν 20 δις συσκευές, αριθμό που το ABI Research τις ανεβάζει στις 30 δις. Η σύνδεσή τους θα γίνεται με το διαδίκτυο, χρησιμοποιώντας χαμηλής ισχύος ραδιοσήματα, τα οποία δεν έχουν την χρήση Wi-Fi ή Bluetooth.

10.4.2 Κύρια Χαρακτηριστικά του IoT

Το IoT βασίζεται σε μεγάλο βαθμό στο υπολογιστικό νέφος (cloud), στα μεγάλα ή μεγάλου όγκου δεδομένα (BigData) και τέλος στην κινητή τηλεφωνία πέμπτης γενιάς (5G).

Από τεχνικής άποψης το IoT δεν είναι το αποτέλεσμα μιας μόνο πρωτότυπης τεχνολογίας. Σε αντίθεση, διάφορες συμπληρωματικές τεχνικές εξέλιξης παρέχουν δυνατότητες, οι οποίες συνεργάζονται ώστε να βοηθήσουν να γεφυρωθεί το χάσμα που υπάρχει μεταξύ εικονικού και φυσικού κόσμου. Οι δυνατότητες αυτές περιλαμβάνουν:

- Επικοινωνία και συνεργασία μεταξύ των αντικειμένων.
- Διευθυνσιοδότηση: στο IoT τα αντικείμενα μπορούν να τοποθετούνται και να διευθυνσιοδοτούνται και έτσι έχουν την δυνατότητα να επιβεβαιώνονται ή και να ρυθμίζονται από απόσταση.
- Ταυτοποίηση: τα αντικείμενα είναι μοναδικά αναγνωρίσιμα. Οι τεχνολογίες RFID, NFC (NearFieldCommunication) και barcode, είναι παραδείγματα τεχνολογιών με τις οποίες μπορούν να εντοπιστούν.
- Ανίχνευση: τα αντικείμενα έχουν αισθητήρες που με την βοήθεια της συλλογής πληροφοριών που είναι σχετικές με το περιβάλλον τους, καταγράφοντας, διαβιβάζοντας ή αντιδρώντας άμεσα σε αυτό.
- Ενεργοποίηση: τα αντικείμενα περιέχουν ενεργοποιητές προκειμένου να χειριστούν το περιβάλλον τους.
- Ενεργοποίηση και Επεξεργασία πληροφοριών: έξυπνα αντικείμενα διαθέτουν έναν επεξεργαστή ή μικροελεγκτή, καθώς και την ικανότητα αποθήκευσης.
- Εντοπισμός: τα έξυπνα αντικείμενα έχουν επίγνωση της φυσικής τους θέσης ή μπορούν να εντοπίζονται. Το GPS ή το κινητό τηλέφωνο, οι ραδιοφάροι και οι οπτικές ίνες είναι τεχνολογίες μέσω των οποίων επιτυγχάνεται ο στόχος του εντοπισμού.
- Διεπαφές χρήστη: τα έξυπνα αντικείμενα μπορούν να επικοινωνούν με τους ανθρώπους με κατάλληλο τρόπο.

10.4.3 Κατηγορίες Εφαρμογών του IoT

Υπάρχουν διάφορες κατηγορίες σχετικές με τις IoT εφαρμογές. Ενώ υπάρχουν κυριολεκτικά εκατοντάδες εφαρμογές που αναγνωρίζονται από διάφορες βιομηχανίες, είναι εφικτό να ταξινομηθούν με έναν απλό και λογικό τρόπο σε δύο κυρίως κατηγορίες.

Πρώτη κατηγορία εφαρμογών είναι αυτή που περιλαμβάνει την ιδέα πληθώρας ετερογενών, έξυπνων και διασυνδεδεμένων συσκευών με μοναδικά αναγνωριστικά ID, τα οποία αλληλεπιδρούν με άλλα μηχανήματα/αντικείμενα, υποδομές και το φυσικό περιβάλλον. Σε αυτήν την κατηγορία το IoT, παίζει κατά πολύ τον ρόλο της διοίκησης, του ελέγχου και της διαδρομής. Σε όλες τις πτυχές του IoT πολύ μεγάλη σημασία έχει η ασφάλεια και η προστασία.

Η δεύτερη κατηγορία εφαρμογών σχετίζεται με την επεξεργασία των δεδομένων που συλλέγονται από τους τελικούς κόμβους και την εύρεση των δεδομένων για τις τάσεις και τις συμπεριφορές, οι οποίες μπορούν να παράγουν χρήσιμες πληροφορίες σχετικές με το marketing, προκειμένου να δημιουργηθεί επιπλέον εμπόριο.

10.4.4 Συγκεκριμένα παραδείγματα εφαρμογών

Όταν συνδέονται περισσότερα αντικείμενα από ότι άνθρωποι στο διαδίκτυο, ανοίγει ένα παράθυρο στο να δημιουργηθούν εφαρμογές σε τομείς όπως αυτοματισμός και η επικοινωνία μηχανής προς μηχανή. Όμως στην πραγματικότητα οι δυνατότητες είναι ατελείωτες. Υπάρχουν πολλά παραδείγματα που τονίζουν μερικούς από τους τρόπους που το IoT αλλάζει προς το καλύτερο την ζωή των ανθρώπων όπως: εφαρμογές στην εκπαίδευση, το έξυπνο σπίτι, οι έξυπνες πόλεις, η έξυπνη βιομηχανία, το έξυπνο περιβάλλον, οι μεταφορές και οι εφοδιασμοί, η λιανική πώληση, η ιατρική παρακολούθηση από απόσταση, η έξυπνη ενέργεια, η έξυπνη μέτρηση, η έξυπνη κτηνοτροφία και η έξυπνη γεωργία. Ακολουθώντας θα αναπτυχθούν εν συντομία τα παραδείγματα των εν λόγω εφαρμογών.

Εφαρμογές στην εκπαίδευση

Οι δυνατότητες αυτής της εφαρμογής αφορούν κυρίως την ασφάλεια των μαθητών, αλλά και την καλύτερη εκμετάλλευση των εκπαιδευτικών πόρων, όπως π.χ. σε μια βιβλιοθήκη. Στις βιβλιοθήκες οι υπάρχουσες ετικέτες, barcode, στα βιβλία δίνουν την θέση τους σε ολοκληρωμένα κυκλώματα τεχνολογίας ταυτοποίησης μέσω ραδιοσυχνότητας (RFID).

Το έξυπνο σπίτι

Τα μελλοντικά έξυπνα σπίτια θα μπορούν να καταλαβαίνουν το τι συμβαίνει μέσα στο κτίριο, κυρίως επηρεαζόμενα από τρεις πτυχές: την χρήση των πόρων, την ασφάλεια και την άνεση. Ο στόχος είναι η μείωση της συνολικής δαπάνης και τα καλύτερα επίπεδα άνεσης. Αυτά τα οποία μπορούν να υπάρχουν σε ένα έξυπνο σπίτι είναι:

- συσκευές ελέγχου στην χρήση της ενέργειας και του νερού
- διάφορες συσκευές ελέγχου από απόσταση
- συστήματα περιμετρικού ελέγχου σε διάφορες ζώνες περιορισμένης πρόσβασης και εντοπισμός εισβολέων

Οι έξυπνες πόλεις

Είναι αστικές περιοχές που δημιουργούν βιώσιμη ανάπτυξη και υψηλή ποιότητα ζωής. Τα χαρακτηριστικά μιας έξυπνης πόλης περιλαμβάνουν: την οικονομία, τους ανθρώπους, την διακυβέρνηση, την κινητικότητα, το περιβάλλον και την διαβίωση. Τελικά πολλοί είναι οι τομείς και οι κλάδοι οι οποίοι θα επωφεληθούν από πιο ψηφιοποιημένες και έξυπνες πόλεις. Αυτά που μπορούν να υπάρχουν, και αφορούν διάφορους τομείς σε μια έξυπνη πόλη είναι:

- η μελέτη κατάστασης παρακολουθώντας δονήσεις και υλικές συνθήκες , σε κτίρια, γέφυρες και ιστορικά μνημεία
- οι χάρτες αστικού θορύβου για την παρακολούθηση του ήχου σε περιοχές π.χ. όπου υπάρχουν μπαρ
- η ανίχνευση Smartphone για τον εντοπισμό συσκευών που λειτουργούν με Wi-Fi ή bluetooth διεπαφές
- ο έξυπνος φωτισμός στα φώτα των δρόμων με βάση τις καιρικές συνθήκες
- η διαχείριση απορριμμάτων για την βελτιστοποίηση των δρομολογίων περισυλλογής
- οι έξυπνοι δρόμοι με προειδοποιητικά σήματα και εκτροπές

Η έξυπνη βιομηχανία

Σε μια παγκόσμια αλυσίδα ανεφοδιασμού, οι εταιρείες θα μπορούν να παρακολουθούν τα προϊόντα τους μέσα από ετικέτες αναγνώρισης ραδιοσυχνότητας, έτσι θα μειώσουν τα λειτουργικά τους έξοδα και θα βελτιώσουν την παραγωγικότητά τους. Επίσης θα υπάρχουν αισθητήρες στα μηχανήματα, οι οποίοι θα διευκολύνουν την συντήρησή τους και θα επιτρέπουν την καλή λειτουργία και απόδοση γενικά του εξοπλισμού. Αυτά που πρέπει να παρακολουθούνται και να ελέγχονται στο χώρο ενός εργοστασίου είναι:

- η ποιότητα του εσωτερικού αέρα, παρακολουθώντας τα τοξικά επίπεδα, για να είναι ασφαλείς οι εργαζόμενοι και τα εμπορεύματα
- παρακολούθηση θερμοκρασίας ιδιαίτερα σε χώρους (ψυγεία) όπου υπάρχουν ευαίσθητα προϊόντα
- παρακολούθηση των επιπέδων του όζοντος (π.χ. στην ξήρανση κρέατος σε εργοστάσια τροφίμων)
- παρακολούθηση και αξιολόγηση εσωτερικού χώρου με χρήση παθητικών ετικετών (RFID/NFC) και με χρήση Zig Bee το οποίο είναι ένα τυποποιημένο πρωτόκολλο επικοινωνίας που δημιουργήθηκε για χρήση σε ασύρματα προσωπικά δίκτυα

Το έξυπνο περιβάλλον

Πρωτεύει την ιδέα ενός φυσικού κόσμου ο οποίος θα είναι πλούσιος και ορατά συνυφασμένος με αισθητήρες, ενεργοποιητές, οθόνες και υπολογιστικά στοιχεία. Αυτά θα συνδέονται μέσω ενός συνεχούς δικτύου. Έτσι θα μπορεί να υπάρχει:

- παρακολούθηση με συσκευές πυρανίχνευσης δασικών περιοχών

- έλεγχος της ατμοσφαιρικής ρύπανσης για τις εκπομπές CO₂ και άλλων ρύπων από εργοστάσια και αυτοκίνητα
- παρακολούθηση της στάθμης και της ποιότητας του χιονιού, σε χιονοδρομικές πίστες καθώς και για τον κίνδυνο χιονοστιβάδων.
- πρόληψη κατολισθήσεων παρακολουθώντας την υγρασία του εδάφους, τις δονήσεις και την πυκνότητα της γης
- πρόωμη ανίχνευση σεισμών με κατανεμημένο έλεγχο σε περιοχές δονήσεων

Οι μεταφορές και οι εφοδιασμοί

Για αυτά το IoT δεν θα βελτιώνει μόνο τα συστήματα ροής υλικών αλλά και το παγκόσμιο σύστημα εντοπισμού στίγματος, και αυτόματης αναγνώρισης εμπορευμάτων. Αυτά θα μπορούν να γίνουν με:

- την αποφυγή της κυκλοφοριακής συμφόρησης με την παρακολούθηση οχημάτων και πεζών
- την έξυπνη στάθμευση παρακολουθώντας τους χώρους στάθμευσης για την ύπαρξη ή όχι ελεύθερων θέσεων σε αυτά
- την ποιότητα στις συνθήκες φόρτωσης
- την γνώση της θέσης μεμονωμένων αντικειμένων σε λιμάνια και αποθήκες
- την προειδοποίηση για πιθανές εκπομπές στην μεταφορά εύφλεκτων εμπορευμάτων και απομόνωση των επικίνδυνων (π.χ. εκρηκτικά)
- την παρακολούθηση των διαδρομών ευαίσθητων προϊόντων, όπως φαρμάκων κοσμημάτων ή επικίνδυνων εμπορευμάτων

Η λιανική πώληση

Το IoT αντιλαμβάνεται τόσο τις ανάγκες των πελατών όσο και τις ανάγκες των επιχειρήσεων. Αυτό το κάνει συγκρίνοντας τις τιμές ενός προϊόντος σε σχέση με άλλα της ίδιας ποιότητας με χαμηλότερη τιμή και δίνει πληροφορίες όχι μόνο στους πελάτες αλλά και στις επιχειρήσεις. Έτσι οι εταιρείες με το IoT μπορούν να κάνουν:

- έλεγχο των προμηθειών
- πληρωμές NFC με βάση την περιοχή ή την διάρκεια της δραστηριότητας
- εφαρμογές έξυπνης αγοράς με παροχή συμβουλών στα σημεία πώλησης σύμφωνα με τις συνήθειες και τις προτιμήσεις των πελατών
- έξυπνη διαχείριση των προϊόντων με έλεγχο τους στα ράφια και στις αποθήκες ώστε να ανανεώνονται όταν χρειάζεται

Η ιατρική παρακολούθηση από απόσταση

ο έλεγχος και η πρόληψη είναι δύο βασικοί παράγοντες για την διατήρηση της υγείας. Σήμερα οι άνθρωποι μπορούν να παρακολουθούνται και να ελέγχονται από ειδικούς ακόμα και από απόσταση. Η παροχή πληροφοριών σχετικών με την εξέλιξη της υγείας ασθενών κάνει την γενική διαδικασία πιο αποτελεσματική. Αυτά που μπορεί να προσφέρει είναι:

- η βοήθεια σε ηλικιωμένους και σε ΑΜΕΑ που ζουν μόνοι τους ανιχνεύοντας πιθανές πτώσεις των ατόμων αυτών
- ο έλεγχος σε ιατρικά ψυγεία, για τις επικρατούσες συνθήκες, όπου αποθηκεύονται εμβόλια, φάρμακα και οργανικά στοιχεία
- ο έλεγχος στην φροντίδα αθλητών σε σημεία ελέγχου στα κέντρα υψηλής απόδοσης
- η επιτήρηση ασθενών σε νοσοκομεία και γηροκομεία
- οι μετρήσεις της υπερϊώδους ακτινοβολίας, ώστε να μπορεί να ενημερωθεί και να προειδοποιηθεί ο κόσμος για την μη έκθεση στον ήλιο
- η καλύτερη ποιότητα ζωής στους ηλικιωμένους π.χ. βάζοντας μια φορητή συσκευή η οποία μπορεί να ανιχνεύει τα ζωτικά σημεία ενός ατόμου

Η έξυπνη ενέργεια

Το πεδίο αυτό έχει πολλές συσχετίσεις με το έξυπνο σπίτι και την έξυπνη πόλη. Το βασικό ζήτημα είναι να βρεθούν τρόποι με την βοήθεια των οποίων θα γίνεται εξοικονόμηση ενέργειας. Ουσιαστικά αναφερόμαστε σε αυτό που είναι γνωστό σαν έξυπνο δίκτυο. Αυτό μπορεί να επιτευχθεί με:

- έξυπνους θερμοστάτες
- ελεγκτές φόρτωσης
- Plug-in ηλεκτρικά οχήματα
- έξυπνες συσκευές
- επεκτάσεις εύρους
- ενεργειακές υπηρεσίες διασύνδεσης
- μετατροπείς

Η έξυπνη μέτρηση

Οι έξυπνες εφαρμογές μέτρησης προσφέρουν: οφέλη βελτιωμένης αξιοπιστίας και ακρίβειας, την ευκολία της βαθμονόμησης, της ασφάλειας, προηγμένα χαρακτηριστικά χρέωσης και τέλος την ευκαιρία για καλύτερη διαχείριση της χρήσης της ενέργειας. Αυτά μπορούν να επιτευχθούν με:

- την έξυπνη κατανάλωση και διαχείριση της ενέργειας.
- την παρακολούθηση της στάθμης σε δεξαμενές και βυτία νερού, πετρελαίου, φυσικού αερίου
- τις φωτοβολταϊκές εγκαταστάσεις παρακολουθώντας και βελτιστοποιώντας την απόδοση στον τομέα της ηλιακής ενέργειας

- τον έλεγχο στην ροή του νερού με μέτρηση της πίεσής του στα συστήματα μεταφοράς του
- την μέτρηση των υλικών όσο αφορά τα επίπεδα του κενού και του βάρους τους

Η έξυπνη κτηνοτροφία

Με την εμφύτευση επί παραδείγματι αισθητήρων στα αυτιά βοοειδών θα μπορούν οι κτηνοτρόφοι να παρακολουθούν την υγεία τους καθώς και τις κινήσεις τους. Αυτά μπορούν να γίνονται με:

- την φροντίδα των απογόνων με έλεγχο των συνθηκών διαβίωσης στις φάρμες ώστε να διασφαλίζεται οι υγεία των ζώων και η επιβίωσή τους
- την παρακολούθηση των ζώων με εντοπισμό και αναγνώρισή τους στα λιβάδια που βόσκουν και στους στάβλους όπου διαβιούν
- την μελέτη των επιπέδων τοξικών αερίων μετρώντας τον αερισμό και την ποιότητα του αέρα στα αγροκτήματα

Η έξυπνη γεωργία

Διάφορες πρακτικές και εφαρμογές μπορούν να αυξήσουν την παραγωγή τροφίμων, και να προσαρμόσουν τα συστήματα παραγωγής τους. Υπάρχουν δηλαδή οι δυνατότητες για την βελτίωση της γεωργία με:

- την υδροπονία δηλαδή τον έλεγχο των συνθηκών των φυτών που αναπτύσσονται στο νερό, ώστε να υπάρξει η μέγιστη απόδοση των καλλιεργειών
- την βελτίωση της ποιότητας κρασιού παρακολουθώντας την υγρασία του εδάφους, την διάμετρο του κορμού των φυτών
- τα θερμοκήπια όπου γίνονται έλεγχοι στις συνθήκες μικροκλίματος για την μεγιστοποίηση της παραγωγής και της ποιότητας φρούτων και λαχανικών
- την επιλεκτική άρδευση στις ξηρές ζώνες για την μείωση των υδάτινων πόρων που απαιτούνται για τις περιοχές πρασίνου
- τους μετεωρολογικούς σταθμούς όπου γίνεται μελέτη των καιρικών συνθηκών ώστε να μπορούν να προβλεφθούν περιπτώσεις βροχής, χιονιού, ξηρασίας, ανέμου και πάγου
- τον έλεγχο στο κοπρόχωμα, στο σανό και στο άχυρο για την υγρασία, την θερμοκρασία ώστε να προλαμβάνονται μύκητες και άλλοι μικροβιακοί ρύποι

10.4.5 Ιδιότητες των αυτόνομων IoT συστημάτων

Μία πρώτη ιδιότητα είναι η **Αυτο-προσαρμογή** που επιτρέπει την επικοινωνία των κόμβων, καθώς και τις υπηρεσίες που τις χρησιμοποιεί προκειμένου να αντιδράσει εγκαίρως στο πλαίσιο που συνεχώς μεταβάλλεται. Επίσης η **Αυτό-οργάνωση** όπου στα συστήματα IoT υπάρχουν κόμβοι που συνδέονται και αποσυνδέονται από το δίκτυο αυθόρμητα. Η αυτό - οργάνωση παρέχει ενεργειακά αποδοτικά πρωτόκολλα δρομολόγησης, ώστε να παρέχεται απρόσκοπτη ανταλλαγή δεδομένων σε όλα τα ετερογενή δίκτυα. Η **Αυτο-βελτιστοποίηση** με την οποία γίνεται βέλτιστη χρήση των περιορισμένων πόρων των συσκευών IoT και είναι απαραίτητη για την βιώσιμη και μεγάλης διάρκειας ζωής τους, καθώς και για την ανάπτυξη του IoT. Μία ακόμη ιδιότητα είναι

η **Αυτο-ρύθμιση** όπου τα συστήματα IoT δημιουργούνται δυνητικά από χιλιάδες κόμβους και συσκευές όπως αισθητήρες και ενεργοποιητές. Η **Αυτο-προστασία** που λόγω της ασύρματης πανταχού παρούσας φύσης του, το IoT θα είναι ευάλωτο σε πολλές κακόβουλες επιθέσεις. Η **Αυτο-ίαση** είναι ένα χαρακτηριστικό των IoT συστημάτων με στόχο την ανίχνευση και διάγνωση των προβλημάτων που προκύπτουν καθώς και την προσπάθεια για γρήγορη διόρθωσή τους με αυτόνομο τρόπο. Σημαντική ιδιότητα αποτελεί η **Αυτο-περιγραφή** με την οποία τα πράγματα και οι πόροι, όπως αισθητήρες και ενεργοποιητές, πρέπει να μπορούν να περιγράψουν τα χαρακτηριστικά και τις ικανότητές τους. Μεταξύ των άλλων χαρακτηριστικών η **Αυτο-ανακάλυψη** διαδραματίζει ουσιαστικό ρόλο για την επιτυχή ανάπτυξη του IoT. Συσκευές IoT και υπηρεσίες θα πρέπει να βρίσκονται δυναμικά και να χρησιμοποιούνται από τους άλλους με ενιαίο και διαφανή τρόπο. Τέλος η **Αυτο-προμήθεια ενέργειας** η οποία είναι ένα εξαιρετικά σημαντικό χαρακτηριστικό για να συνειδητοποιηθούν και να αναπτυχθούν βιώσιμες λύσεις IoT π.χ. τεχνικές συγκομιδής ενέργειας σε αντίθεση με τις μπαταρίες επί παραδείγματι οι οποίες επιδρούν αρνητικά στο περιβάλλον.

10.4.6 Πηγές κινδύνου

Οι πηγές κινδύνου, δηλαδή οι απειλές, μπορεί να είναι η πλαστογράφηση ταυτότητας, που σημαίνει ότι κάποιος χρησιμοποιεί παράνομα την ταυτότητα κάποιου άλλου. Επίσης η παραποίηση δεδομένων όπου κάποιος εισβολέας μπορεί να αλλάξει το περιεχόμενο των δεδομένων που ανταλλάσσονται μεταξύ δύο ή περισσότερων συμμετεχόντων. Η αποκρήρυξη η οποία εμπλέκεται σε επιθέσεις κατά τις οποίες ο εισβολέας πραγματοποιεί παράνομες ενέργειες και στην συνέχεια αμφισβητεί ότι τις διέπραξε. Η δημοσιοποίηση πληροφοριών αποτελεί επίσης κίνδυνο αφού πληροφορίες αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα. Μία άλλη απειλή είναι και η άρνηση παροχής υπηρεσιών δηλαδή απενεργοποίηση των υπηρεσιών που προσφέρονται σε νόμιμους χρήστες. Τέλος υπάρχει και ο κίνδυνος της απόδοσης δικαιωμάτων, αυτό μπορεί να συμβεί σε συστήματα τα οποία διαθέτουν διαφορετικές κατηγορίες χρηστών, όταν μάλιστα η κάθε κατηγορία έχει ένα συγκεκριμένο σύνολο των δικαιωμάτων.

Βιβλιογραφία

- [1] Andrew S. Tanenbaum, “Δίκτυα Υπολογιστών”, Παπασωτηρίου 2000
- [2] Whitfield Diffie and Martin E. Hellman, “New Directions in Cryptography”, Invited Paper, 1976.
- [3] D.E. Denning. Cryptography and Data Security. Addison-Wesley, 1982.
- [4] Menezes A., P.C. van Oorschot, S.Vanstone, Handbook of Applied Cryptography, CRC Press, 1997
- [5] C.E. Shannon. Communication theory of secrecy systems. Bell System Technical Journal, 28:656715, 1949.
- [6] Handbook of Applied Cryptography, by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996. Ch. 9 Hash Functions and Data Integrity
- [7] L.R. Knudsen. Block Ciphers Analysis, Design and Applications. PhD thesis, Aarhus University, Denmark, 1994.
- [8] J.L. Massey. Cryptography: Fundamentals and applications. Copies of transparencies, Advanced Technology Seminars, 1993.
- [9] Andrew S. Tanenbaum , Computer Networks, Prentice Hall, 1996
- [10] William Stallings, Cryptography and Network Security, Prentice Hall, 1999
- [11] Σ. Κάτσικας, Ασφάλεια Δικτύων, Ελληνικό Ανοικτό Πανεπιστήμιο, 2000
- [12] Σ. Κάτσικας, Προστασία Δεδομένων, Ελληνικό Ανοικτό Πανεπιστήμιο, 2000
- [13] Β. Ζορκάδης, Κρυπτογραφία, Ελληνικό Ανοικτό Πανεπιστήμιο, 2002
- [14] Σ. Γκρίζαλης, Σ. Κάτσικας, Δ. Γκρίζαλης, Ασφάλεια Δικτύων Υπολογιστών, Εκδόσεις Παπασωτηρίου, Αθήνα 2003
- [15] Γ. Πάγκαλος, Ι. Μαυρίδης, Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων, Εκδόσεις Ανίκουλα
- [16] Κρυπτογραφία Χ.Κουκουβίνος-Α.Παπαϊωάννου, Εκδόσεις Εθνικού Μετσοβίου Πολυτεχνείου, Αθήνα 2007
- [17] Introduction to Cryptography with Coding Theory Wade Trappe-Lawrence C. Washington, Εκδόσεις Pearson, 2002
- [18] Modern Cryptography: Theory and Practice, Wenbo Mao, Εκδόσεις Prentice Hall, 2003

- [19] Cryptography: Theory and Practice (Discrete Mathematics and Its Applications), Douglas R. Stinson, Εκδόσεις CRC Press, 1995
- [20] Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης, Β.Α Κάτος-Γ.Χ Στεφανίδης, Εκδόσεις Ζυγός, Θεσσαλονίκη 2003
- [21] Santos N., Gummadi K., Rodriques R., (2009), "Towards Trusted Cloud Computing", In Proceedings of the 2009 conference on Hot topics in cloud computing. USENIX Association
- [22] Kamara S., Lauter K., (2010), "Cryptographic Cloud Storage", Microsoft research
- [23] Ηλίας Λυπιτάκης, (2000), Εισαγωγή στην επιστήμη των υπολογιστών, Εκδόσεις: Ελληνικό Ανοικτό Πανεπιστήμιο, Πάτρα
- [24] Mell Peter, Grance Timothy, (2009), "The NIST definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology", NIST Special Publication 800-145, pp 2
- [25] Alessandro Bassi et al. «Enabling Things to Talk: Designing IoT solutions with the IoT Architectural Reference Model» Springer Open. 2013
- [26] Samiuel Greengard "The Internet of Things"
- [27] John Rhoton "Security Assessment Handbook"
- [28] Raghuram Yeluri "Building the Infrastructure for Cloud Security"