ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ & ΠΛΗΡΟΦΟΡΙΚΗΣ

ΕΡΓΑΣΙΑ ΕΞΑΜΗΝΟΥ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ
<ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ ΚΑΙ ΔΙΑΣΥΝΔΕΣΗ ΔΙΚΤΥΩΝ>

<ΚΡΥΠΤΟΓΡΑΦΙΑ>

<ΧΑΡΙΤΟΥ ΛΑΜΠΡΙΝΗ>

Α.Μ <5469>

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ

ΠΑΤΡΑ 2015

ΠΕΡΙΕΧΟΜΕΝΑ

1.Εισαγωγή
1.1 Ιστορική αναδρομή
1.2 Τι πετυχένουμε με την κρυπτογραφία
1.3 Αρχές μέτρησης κρυπτογραφικής δύναμης

2. Αλγόριθμοι και κλειδιά κρυπτογράφησης
2.1 Συμμετρική Κρυπτογραφία
2.1.1 Κρυπτοαλγόριθμος DES
2.1.2 Κρυπτοαλγόριθμος τρίπλο DES
2.1.3 Κρυπτοαλγόριθμος AES
2.1.4 Κρυπτοαλγόριθμος IDEA
2.1.5 Κρυπτοαλγόριθμος DSS
2.1.6 Κρυπτοαλγόριθμοι RC2, RC4, RC5
2.1.7 Blowfish
2.2 Ασύμμετρη Κρυπτογραφία
2.2.1 Κρυπτοσύστημα RSA
2.3 Τύποι κλειδιών
2.4 Αλγόριθμοι συμμετρικού κλειδιού
2.4.1 Επιθέσεις πάνω σε αυτόν τον αλγόριθμο
2.5 Αλγόριθμοι δημόσιου κλειδιού
2.5.1 Επιθέσεις πάνω σε αυτόν τον αλγόριθμο
2.6 Diffie-Hellman(Αλγοριθμος για τη Διαχείριση και Ανταλλαγή Κλειδιών)
2.7 Ψηφιακές υπογραφές
2.8 Μειονεκτήματα και Πλεονεκτήματα την Συμμετρικής και Ασύμμετρης Κρυπτογραφίας

3. Κρυπτογραφία στο διαδίκτυο
3.1 Κρυπτογραφικές υπηρεσίες
3.2 Πρωτόκολλα για την κρυπτογράφηση μηνυμάτων του ηλεκτρονικού ταχυδρομείου (e-mail)
3.2.1 PGP
3.2.2 S/MIME
3.3 Πρωτόκολλα δικτύου
3.3.1 SSL
3.3.2 TLS
3.3.3 SSH
3.3.4 SET
3.3.5 S-HTTP
3.3.6 DNSSEC
3.3.7 IPSEC

4. Virtual Private Networks

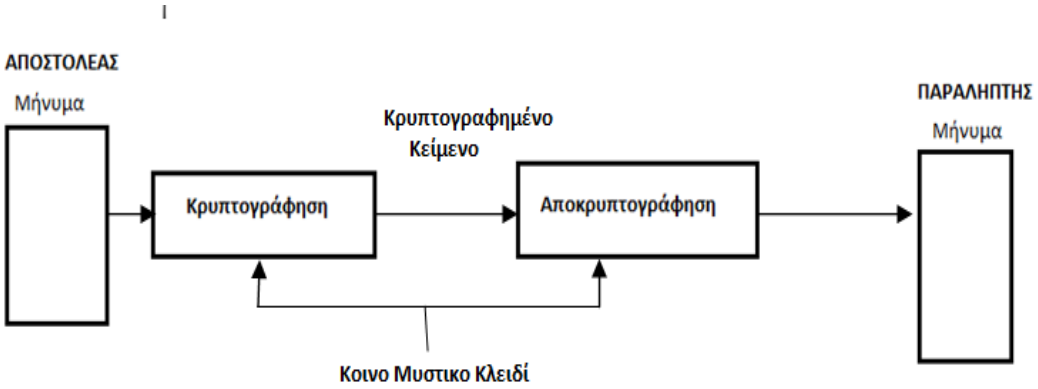
4.1 Τι είναι τα VPN
4.2 IPSec
4.3 IKE
4.4 PPTP
4.5 OpenVPN

Συμπεράσματα

Βιβλιογραφία

1. Εισαγωγή

Η κρυπτογραφία μελετά τους τρόπους με τους οποίους μπορούμε να μετασχηματίσουμε ένα μήνυμα σε φαινομενικά ακατάλληπτη μορφή. Είναι ένας επιστημονικός κλάδος που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Σήμερα χρησιμοποιείται ως ένα χρήσιμο εργαλείο στην ασφάλεια πληροφοριών, δηλαδή την προστασία των δεδομένων ως προς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα τους. Η κρυπτογραφία είναι ένας κλάδος της επιστήμης της κρυπτογραφίας, η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς για δύο ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάσει την πληροφορία εκτός από τα μέλη. Η διεργασία της κρυπτογράφησης και της αποκρυπτογράφησης φαίνεται στην παρακάτω εικόνα.
Σε αυτή την εργασία θα αναφερθούμε για τους αλγοριθμους και τα κλειδιά κρυπτογράφησης, για την κρυπτογραφία στο διαδίκτυο και τα πρωτόκολλα που χρησιμοποιεί η κρυπτογραφία, θα αναφερθούμε επίσης και στο VPNs(Virtual Private Network).



1.1. Ιστορική αναδρομή

Η πρώτη περίοδος της κρυπτογραφίας ήταν το (1900 π.Χ - 1900 μ.Χ). Κατά τη διάρκεια αυτής της περιόδου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης που βασίζονταν κυρίως σε απλές αντικαταστάσεις γραμμάτων. Στην αρχαία Ελλάδα η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες για να μπορούν να ανταλλάξουν μεταξύ τους μυστικά μηνύματα. Τα μηνύματα αυτά ήταν γραμμένα σε στενές ταινίες περγαμηνης. Αφού ξετύλιγαν την περγαμηνή, το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα, όταν δε ξετύλιγαν τη λωρίδα το κείμενο ήταν ακατάληπτο εξαιτίας της ανάμειξης των γραμμάτων. Το κλειδί ήταν η διάμετρος της σκυτάλης. Στην αρχαιότητα χρησιμοποιήθηκαν κυρίως συστήματα τα οποία βασίζονται στην στενογραφία και όχι τόσο στην κρυπτογραφία. Η δεύτερη περίοδος της κρυπτογραφίας τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950 και καλύπτει τους δύο παγκόσμιους πολέμους. Η τρίτη περίοδος χαρακτηρίζεται από την έξαρση της ανάπτυξης στους επιστημονικούς κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει ουσιαστικά με τον Claude Shannon, που αναμφισβήτητα ήταν ο πάτερας των μαθηματικών συστημάτων της κρυπτογραφίας. Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης και ενός κλειδιού κρυπτογράφησης. Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στην μυστικότητα του κλειδιού κρυπτογράφησης. (Βικιπαίδεια_1.1)

1.2 Τι πετυχένουμε με την κρυπτογραφία

Η κρυπτογραφία παίζει σημαντικό ρόλο στις καθημερινές μας υπολογιστικές και επικοινωνιακές μας ανάγκες. Καθώς μπορεί να προστατεύσει τις πληροφορίες που είναι αποθηκευμένες σε έναν υπολογιστή από την πρόσβαση τρίτων, μπορεί να προστατευσει πληροφορίες κατα την διάρκεια της μεταφοράς από ένα υπολογιστικό σύστημα σε ένα άλλο. Επίσης η κρυπτογραφία μπορεί να χρησιμοποιηθεί για να επικυρώσει την ταυτότητα του δημιουργού. Ωστόσο μπορεί να χρησιμοποιηθεί για να εμποδίσει και για να εντοπίσει τυχαίες ή σκόπιμες αλλαγές στα δεδομένα μας. Εκτός από όλα αυτά όμως η κρυπτογαφία δε μπορεί να προστατεψει τα δεδομένα από κάποιον εισβολέα που θέλει να σβήσει τα δεδομένα μας όπως είναι ή ένας εισβολέας μπορεί να έχει τροποποιήσει και να εκθέτει ένα πρόγραμμα κρυπτογράφησης από μόνος του έτσι ώστε να μπορεί να αποκρυπτογραφήσει όλα τα μηνύματα με το δικό του κλειδί. Για όλους αυτούς τους λόγους λοιπόν, η

κρυπτογράφηση θα πρέπει να θεωρείται σαν ένα μέρος της ολικής στρατηγικής ασφάλειας που έχουμε. (Βασίλειος Αν. Κάτος, 2003)

1.3 Αρχές μέτρησης κρυπτογραφικής δύναμης

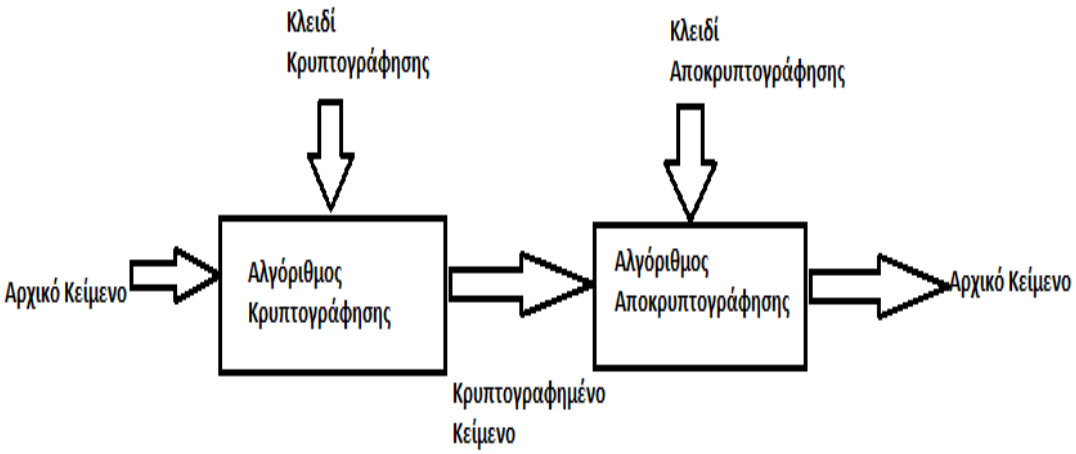
Υπάρχει ένα στάδιο για την ανάλυση της δύναμης ενός κρυπτοσυστήματος όπου είναι η υπόθεση της ικανότητας του αντιπάλου η οποία κρίνεται με βάση τους πόρους που διαθέτει, εφόσον και με την πρόσβαση που έχει στο κρυπτοκείμενο, στο απλό κείμενο και στο κρυπτοσύστημα. Οι επίθεσης ενός αντιπάλου σε ένα κρυπτοσύστημα χωρίζονται σε κάποιες κατηγορίες (σύμφωνα με το βιβλίο) και είναι οι ακόλουθες:

- ✓ Επίθεση στο κρυπτοκείμενο. Ο αντιπαλος ο οποιος έχει πρόσβαση σε μερικά κομματια του κρυπτοκειμένου και ο σκοπός του είναι να το αποκρυπτογραφήσει ή να ανακαλύψει το αντιστοιχο κλειδί. Με λίγα λόγια θεωρείται ανασφαλές ένα τετοιο κρυπτοσύστημα γιατί είναι ευαλωτο σε μια τέτοια επίθεση.
- ✓ Επίθεση με γνωστό απλό κείμενο. Εδώ ο αντίπαλος γνωρίζει κάποιες αντιστοιχίες του κρυπτοκειμένου με απλό κειμενο και ο σκοπός του είναι να ανακαλύψει το αντίστοιχο κλειδί. Τα πρωτόκολλα επικοινωνίας στα δίκτυα των υπολογιστών εμφανίζουν συστηματικά τυποποιημένα μην΄τματα. Θεωρείται ανασφαλες ενα κρυπτοσύστημα το οποίο πέφτει σε επίθεσει απλού κειμένου.
- ✓ Επίθεση με επιλεγμένο απλό κείμενο. Ο αντίπαλος εδώ έχει τη δυνατότητα πρόσβασης στο κρυπτοσύστημα ο οποίος δεν γνωρίζει το κλειδί και μάλλον θα ζητά την κρυπτογράφηση μηνυμάτων. Με αυτόν τον τρόπο μπορεί να ανακαλύψει την αντιστοιχία του απλού κειμένου με το άγνωστο κρυπτοκείμενο.
- ✓ Επίθεση προσαρμόσιμου επιλεγμένου απλού κειμένου. Ο αντίπαλος εδώ θέλει να κάνει πράξη την επίθεση με επιλεγμένο απλό κείμενο, επίσης όμως μπορεί να εφαρμόσει μεθοδολογία σύμφωνα με την οποία η επόμενη επιλογή του απλού κειμένου να εξαρτάται από τις προηγούμενες προκειμένου να ανακαλύψει πιο γρήγορα το κλειδί από μια εξαντλητική αναζήτηση.
- ✓ Επίθεση με επιλεγμένο κρυπτοκείμενο. Θεορώντας ότι εδώ ο αντίπαλος έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης, ο σκοπός του είναι να ανακαλύψει το κλειδί αποκρυπτογράφησης για να μπορεί στο μέλλον να αποκρυπτογραφεί τα νέα κρυπτοκείμενα, όταν πια δεν θα έχει πρόσβαση σε αυόν τον αλγόριθμο. Στα περισσότερα συμμετρικά κρυπτοσυστήματα η επίθεση αυτή έχει την ίδια ισχύ με την επίθεση του επιλεγμένου απλού κειμένου. Αυτή η επίθεση θεωρείται ως η πιο αυστηρή επίθεση.
- ✓ Επίθεση προσαρμόσιμου επιλεγμένου κρυπτοκειμένου. Εδώ αυτή η επίθεση είναι αντίστοιχη του προσαρμόσιμου επιλεγμένου απλού κειμένου, με τη διαφορά ότι ο αντίπαλος έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης. (Βασίλειος Αν. Κάτος, 2003)

ΚΕΦΑΛΑΙΟ2: < ΑΛΓΟΡΙΘΜΟΙ ΚΑΙ ΚΛΕΙΔΙΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ >

2.1 Συμμετρική Κρυπτογραφία

Η συμμετρική κρυπτογραφία είναι πολύ πιο αρχαιότερη από την ασύμμετρη η οποία χρονολογείται από την Αρχαία Αιγυπτο, ενώ η ασύμμετρη πρωτοεμφανίστηκε τη δεκαετία του '70. Σήμερα η κρυπτογραφία αποτελεί ένα πολύ σημαντικό κομμάτι της ασφάλειας των σύγχρονων ψηφιακών συστημάτων. Στους συμμετρικούς αλγόριθμους το κλειδί κρυπτογράφησης μπορεί να υπολογιστεί από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση αλλά και το ανάποδο. Επίσης στις περισσότερες περιπτώσεις τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης είναι τα ίδια. Αυτοί οι αλγόριθμοι χρειάζονται την συμφωνία μεταξύ του αποστολέα και του παραλήπτη για το κλειδί που θα χρησιμοποιηθεί, έτσι ώστε να μπορέσουν να επικοινωνήσουν με ασφάλεια. Η ασφάλεια των αλγόριθμων βασίζεται στην μυστικότητα αυτού του κλειδιού. Για όσο καιρό επιθυμούμε η επικοινωνία να παραμείνει μυστική, για τον ίδιο καιρό πρέπει και το κλειδί να παραμείνει μυστικό. Οι αλγόριθμοι που υποστηρίζουν τη συμμετρική κρυπτογραφία είναι ο DES, IDEA, RC5 και ο 3DES. (Βασίλειος Αν. Κάτος, 2003)



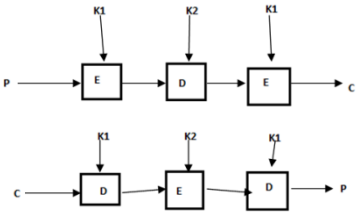
2.1.1 Κρυπτοαλγόριθμος DES

Ο DES δημοσιευθηκε το 1977 και είναι ο κρυπταλγόριθμος στον οποίο έχει γίνει η περισσότερη έρευνα με την κρυπτογραφική του δύναμη. Οι απόπειρες κρυπτανάλυσης του DES είχαν σαν αποτέλεσμα την ανακάλυψη και την καθιέρωση αρχών σχεδίασης των κρυπταλγόριθμων τμήματος. Το σύστημα αυτό δεν είναι πλέον ασφαλές στην αρχική του μορφή, αλλά εξακολουθεί να είναι χρήσιμο σε μια τροποποιημένη μορφή. Υπάρχει μια διάρθρωση αυτού του συστήματος, όπου το απλό κείμενο κρυπτογραφεί τμήματα των 64 bit τα οποία δίνουν 64 bit κρυπτοκειμένου. Αυτός ο αλγόριθμος παραμετροποιείται με ένα κλειδί των 54 bit και έχει 19 διακριτά στάδια. Το πρώτο στάδιο ειναι μια ανεξάρτητη από το κλειδί μετάθεσης του 64 bit "απλού κειμένου" ενώ το τελευταίο στάδιο είναι εντελώς το αντίστροφο αυτής της μετάθεσης. Το προτελευταίο στάδιο ανταλλάσει τα 32 bit στα αριστερά με τα 32 bit στα δεξιά. Ενώ τα υπόλοιπα 16 στάδια παραμμετροποιούνται με διαφορετικές συναρτήσεις κλειδιού. Αυτός ο αλγόριθμος έχει σχεδιαστεί για να εκτελείται η αποκρυπτογράφηση με το ίδιο κλειδί όπως και η κρυπτογράφηση όπου απαιτείται σε όλους τους αλγόριθμους του συμμετρικού κλειδιού. Αυτά τα υπόλοιπα ενδιάμεσα στάδια έχουν μια λειτουργία και το κάθε στάδιο λαμβάνει και παράγει δύο εισόδους και δύο εξόδους των 32 bit. Ωστόσο η αριστερή έξοδος είναι η διάζευξη σε επίπεδο bit μεταξύ της αριστερής εισόδου με μιας συνάρτησης της δεξιάς εισόδου και του κλειδιού του σταδίου αυτού. Αυτή η συνάρτηση αποτελείται από τέσσερα βήματα τα οποία εκτελούνται διαδοχικά. Στην αρχή κατασκευάζεται ένας αριθμός 48bit με επέκταση του 32bit σύμφωνα με έναν σταθερό κανόνα μετάθεσης και αντιγραφής. Αυτά συνδυάζονται με κάποια αποκλειστική διάζευξη και τα αποτελέσματα θα τεμαχιστούν σε οχτώ ομάδες των 6bit με την κάθε ομάδα να τροφοδοτείται σε διαφορετικό κουτί, καθε μια όμως από αυτές τις 64 πιθανές εισόδους του κάθε κουτιού θα αντιστοιχίζονται σε μια έξοδο των 4bit. Όπου αυτά τα 8x4bit παίρνουν από ένα άλλο κουτί. Και σε κάθε μια από αυτες τις 16 επαναλήψεις θα χρησιμοποιείται διαφορετικό κλειδί. Όμως πριν ακόμα ξεκινήσει ο αλγόριθμος εφαρμόζεται μια μετάθεση των 56bit στο κλειδί και πριν κάθε επανάληψη το κλειδί τεμαχίζεται σε δύο τμήματα των 25bit. Μια τεχνική που χρησιμοποιείται μερικές φορές για να κάνει αυτόν τον αλγόριθμο πιο ισχυρό ονομάζεται λευκανση. Σε αυτή τη τεχνική κάθε ομάδα ενός απλού κειμένου περνά από μια αποκλειστική διαζευξη με ένα τυχαίο κλειδί των 64bit πριν τροφοδοτηθεί ο DES και το κρυπτοκείμενο που θα προκύψει πριν την αποστολή του θα περάσει από μια αποκλειστική διάζευξη με ένα δευτερο κλειδί των 64bit. Αυτή η τεχνική προσθέτει δηλαδή περισσότερα bit στο μήκος του κλειδιού και κάνει την έρευνα των κλειδιών πιο χρονοβόρα γιατί για κάθε τμήμα χρησιμοποιεί το ίδιο κλειδί λεύκανσης. Ο κρυπταλγόριθμος DES έχει το χαρακτηριστικό ότι η κρυπτογράφηση και η αποκρυπτογράφηση μπορούν να υλοποιηθούν με την ίδια διαδικασία, με τη μόνη διαφορά ότι το πρόγραμμα κλειδιού της αποκρυπτογράφησης παράγει την αντίστροφη ακολουθία που παράγει το

πρόγραμμα κλειδιού της κρυπτογράφησης. Αυτός ο αλγόριθμος έχει μελετηθεί περισσότερο όσον αφορά το πλήθος των δημοσιευμένων μελετών και το χρονικό διάστημα. Πολλά πορίσματα που διατυπώθηκαν χαριν του DES μετατράπηκαν αργότερα σε αρχές σχεδιασμού συμμετρικών αλγόριθμων τμήματος τύπου DES. (Βασίλειος Αν. Κάτος, 2003)

2.1.2 Κρυπτοαλγόριθμος Τριπλό DES

Μετά από δύο χρόνια κατάλαβαν ότι ο DES ήταν πολύ μικρό και έτσι επινόησαν έναν άλλο τρόπο για την αυξηση του, χρησιμοποιώντας τριπλή κρυπτογράφηση. Αυτός ο αλγόριθμος χρησιμοποιεί τρία 56bit κλειδιά. Στο πρώτο σχήμα φαίνεται η τριπλή κρυπτογράφηση με την χρήση του DES και στη δευτερη η αποκρυπτογράφηση. Σε αυτή τη μέθοδο χρησιμοποιούνται δύο κλειδιά και τρία στάδια. Στο 1ο στάδιο το κείμενο κρυπτογραφείται με τον συνηθισμένο τρόπο μέσω του DES με ένα κλειδί, ενώ στο 2ο στάδιο το DES εκτελείται σε κατάσταση αποκρυπτογράφησης με ένα άλλο κλειδί και στο τέλος γίνεται άλλη μια κρυπτογράφηση ξανά μέσω του DES με το πρώτο κλειδί. Ωστόσο ο λόγος που χρησιμοποιείται η σειρά κρυπτογράφηση, αποκρυπτογράφηση και ξανα κρυπτογράφηση είναι μια συμβατότητα προς τα πίσω με τα υπάρχοντα συστήματα DES ενός κλειδιού. Οι συναρτήσεις της κρυπτογράφησης και της αποκρυπτογράφησης είναι και οι δύο αντιστοιχίσεις ανάμεσα σε σύνολα των 64bit. (Tanenbaum, 2011)



2.1.3 Κρυπτοαλγόριθμος AES

Ο κρυπταλγόριθμος AES εντοπιστηκε από μια προσπάθεια αντικατάστασης του DES. Το κλειδί αυτού του κρυπταλγόριθμου είναι ίσο με 128, 192 ή 256 bits. Ωστόσο η προσπάθεια δημοσιοποιήθηκε τον Σεπτέμβριο του 1997 με την προκήρυξη του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας για μια παγκόσμια συμμετοχή στη δημιουργία του AES. Αυτή η διαδικασία δημιουργίας του AES πληρούσε το κριτήριο του Kerchoff σχετικά με την εξάρτηση της ασφάλειας και δημοσιοποίησης. Τόσο η προκήρυξη όσο και η πρόσκληση εξέτασης της ασφάλειας του AES για τους προτεινόμενους κρυπταλγόριθμους ήταν ανοιχτές.
Υπήρχαν κάποια κριτήρια αξιολόγησης του AES σύμφωνα με το βιβλίο, τα οποία ήταν τα εξής:

- Η ασφάλεια. Αυτό το κριτήριο ήταν με το μεγαλύτερο βάρος. Δηλαδή εαν υπήρχαν κάποιες ενδείξεις ότι ο προτεινόμενος κρυπταλγόριθμος δεν ήταν ασφαλής, τότε θα απορρίπτονταν.

- Το κόστος. Αυτό το κριτήριο αναφέρεται στην υπολογιστική πολυπλοκότητα που θα απαιτούσε ο κρυπταλγόριθμος για να εκτελέσει κρυπτογράφηση και αποκρυπτογράφηση, όσο και στις απαιτήσεις μνήμης.
- Τα χαρακτηριστικά υλοποίησης του κρυπταλγόριθμου τα οποία είχαν την απλότητα των αλγορίθμων και φυσικά τον καθορισμό των μεγεθών του απλού κειμένου, του κλειδιούκαι του κρυπτοκειμένου.

Ο AES είναι επαναληπτικός κρυπταλγόριθμος και βασίζεται σε κρυπτογράφηση γινομένου και μπορεί να αντισταθεί αποτελεσματικά σε όλες τις γνωστές κρυπταναλυτικές μεθόδους. Ο βασικός αποθηκευτικός χώρος του AES συμβολίζεται με state και αρχικά περιέχει το απλό κείμενο ενώ στο τέλος της διαδικασίας περιέχει το κρυπτοκείμενο, περιγράφεται δηλαδή με τη μορφή στρωμάτων, όπου το κάθε στρώμα αντιστοιχεί σε ένα συγκεκριμένο μετασχηματισμό του state. (Tanenbaum, 2011) (Βασίλειος Αν. Κάτος, 2003)

2.1.4 Κρυπτοαλγόριθμος IDEA

Αυτός ο αλγόριθμος αποτελεί συμμετρικό κωδικοποίησης τμημάτων που αναπτύχθηκε το 1991. Ο IDEA είναι ένας 64bit επαναληπτικός αλγόριθμος που χρησιμοποιεί κλειδί μήκους 128bit και 8 γύρους. Στηρίζεται σε τρεις διαφορετικές μαθηματικές λειτουργίες,στη διαδική πράξη XOR, στη διαδική πρόσθεση ακεραίων των 16bit και στο δυαδικό πολλαπλασιασμό ακεραίων των 16bit. Οι συναρτήσεις συνδιάζονται με τέτοιο τρόπο ώστε να αναπτυχθεί ένας πολύπλοκος μετασχηματισμός που αναλύεται δύσκολα ώστε να καθίσταται πολύ δύσκολη η διαδικασία κρυπτανάλυσης. Ο αλγόριθος παραγωγής δευτερευοντων κλειδιών βασίζεται στη χρήση κυκλικών μετατοπίσεων οι οποίες χρησιμοποιούνται με πολύπλοκο τρόπο για να παραχθούν συνολικά έξι δευτερευοντα κλειδια για καθέναν από τους 8 γύρους του IDEA. Αυτός ο αλγόριθμος ήταν ένας από τους προτεινόμενους 128bit αντικαταστάτες του DES εχει υποβληθεί σε αξιοσημείωτη διερευνηση και εμφανιζεται ανθεκτικός σε κρυπταναλυτικές επιθέσεις. (Βικιπαίδεια_2.1.4)

2.1.5 Κρυπτοαλγόριθμος DSS

Το DSS(Digital Signature Algorithm) θεωρείται σαν ένας επίσημος αλγόριθμος για την παραγωγή ψηφιακών υπογραφών της κυβέρνησης των Ηνωμένων Πολιτειών της Αμερικής. Χρησιμοποείται μόνο για την παραγωγή ψηφιακών υπογραφών και βασίζεται στο πρόβλημα του διακριτού λογαρίθμου. Το DSS είναι πιο γρήγορο από τον RSA στην παραγωγή ψηφιακών υπογραφών. Παρ' όλο που μπορεί να υποστηριχθεί ότι η γρήγορη παραγωγή υπογραφών αποτελεί πλεονέκτημα, επειδή ένα μήνυμα υπογράφεται μία φορά αλλά η υπογραφή του μπορεί να επαληθευτεί πολλές φορές, κάτι τέτοιο δεν ανταποκρίνεται στην πραγματικότητα. Το DSS έχει ολοκληρωθεί σε πολλά συστήματα ασφαλείας, αν και έχει λάβει πολλές άσχημες κριτικές. Τα κυριότερα θέματα κριτικής είναι η έλλειψη ευελιξίας, η αργή επαλήθευση των υπογραφών, η αδυναμία συνεργασίας με άλλο πρωτόκολλο

πιστοποίησης ταυτότητας και τέλος ότι ο αλγόριθμος δεν είχε αποκαλυφθεί. Επίσης τα κλειδία αυτού του αλγόριθμου είναι αυτόνομα. (Βικιπαίδεια(DSS)) (Ιντερνετ)

2.1.6 Κρυπτοαλγόριθμοι RC2, RC4, RC5

Ο RC2 είναι ένας block cipher με κλειδί μεταβλητού μήκους που σχεδιάστηκε από τον Ron Rivest για την RSA Inc. Είναι γρηγορότερος από τον DES και ο στόχος της σχεδίασης του ήταν να λειτουργήσει για αντικατάσταση του DES. Ωστόσο μπορεί να γίνει περισσότερο ή λιγότερο ασφαλής από τον DES, ανάλογα με το μήκος του κλειδιού. Έχει μέγεθος block ίσο με 64bits και είναι έως και τρεις φορές ταχύτερος από τον DES. (Βικιπαίδεια(RC2))

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

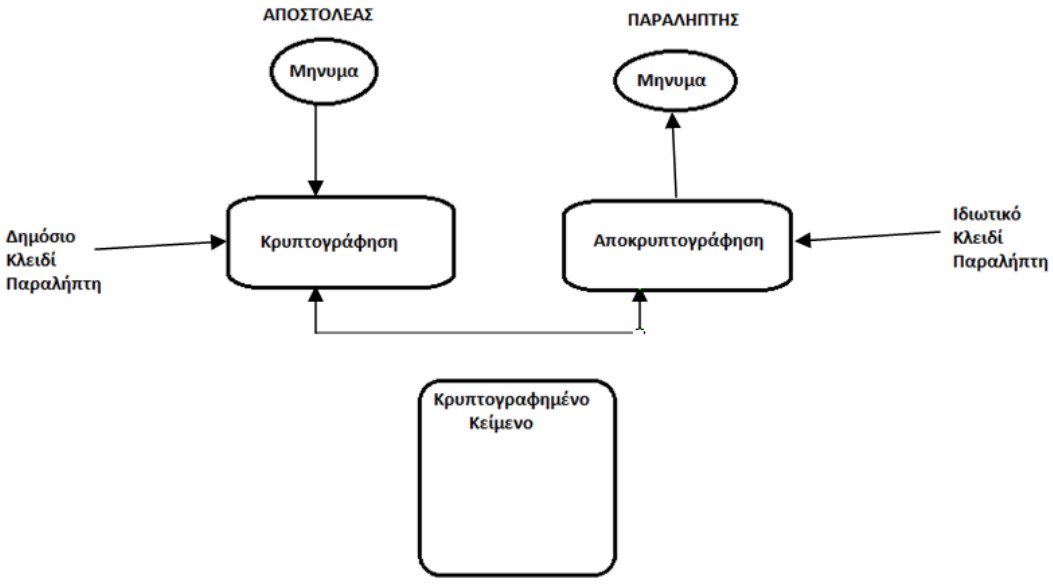
Ο RC5 είναι ένας γρήγορος block cipher από τον Ron Rivest για λογαριασμό της RSA Inc. Έχει πολλούς παραμέτρους: μεταβλητό μήκος κλειδιού, μεταβλητό μέγεθος block και μεταβλητό αριθμό επαναλήψεων. Οι τυπικές επιλογές για το μέγεθος του block είναι 32bits για τις πειραματικές εφαρμογές, 64 bits για τις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

2.1.7 Blowfish

Ο Blowfish είναι ένας block cipher που κατασκευάστηκε από τον Schneier. Είναι ένας Feistel cipher με μέγεθος block 64 bits και μεταβλητό μήκος κλειδιού, με μέγιστο μήκος 448 bits. Όλες οι διεργασίες βασίζονται σε X-OR πράξεις και προσθέσεις λέξεων των 32 bits. Από το κλειδί παράγεται πίνακας με τα subkeys που χρησιμοποιούνται σε κάθε γύρο επανάληψης της κρυπτογράφησης. Έχει σχεδιασθεί για 32-bit μηχανές και είναι σημαντικά ταχύτερος από τον DES. Παρ' όλες τις αδυναμίες που έχουν ανακαλυφθεί καθ' όλη την διάρκεια της ύπαρξης του, θεωρείται ακόμα ασφαλής αλγόριθμος. (Βικιπαίδεια(Blowfish))

2.2 Ασύμμετρη Κρυπτογραφία

Η ασύμμετρη κρυπτογραφία βασίζεται σε μαθηματικές υποθέσεις για το λόγο ότι υπάρχει μαθηματική εξάρτηση μεταξύ του δημοσίου και του ιδιωτικού κλειδιού. Οι ασύμμετροι αλγόριθμοι είναι σχεδιασμένοι έτσι ώστε το κλειδί που χρησιμοποιείται για την κρυπτογράφηση να είναι διαφορετικό από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση. Η ασφάλεια εξαρτάται από την πληροφορία που διαρρέει από το δημόσιο κλειδί όσον αφορά το ιδιωτικό. Οι αλγόριθμοι που υποστηρίζουν την ασύμμετρη κρυπτογραφία είναι ο RSA, ElGamal και ο DSA. (Βασίλειος Αν. Κάτος, 2003)



2.2.1 Κρυπτοσύστημα RSA

Το κρυπτοσύστημα RSA είναι ένα από τα πιο παλιά κρυπτοσυστήματα δημόσιου κλειδιού. Αυτή η ιδέα για το δημόσιο κλειδί διατυπώθηκε το 1976 από τους Diffie και Hellman, όμως το πρώτο κρυπτοσύστημα ανακαλύφθηκε το 1977 από τους Rivest, Shamir και Adleman. Η ασφάλεια του κρυπτοσυστήματος βασίζεται στο πρόβλημα της παραγοντοποίησης ενός σύνθετου ακεραίου σε γινόμενο πρώτων παραγόντων. Ωστόσο ο RSA μπορεί να θεωρείται ασφαλής κρυπταλγόριθμος για μεγάλες παραμέτρους, υπάρχουν όμως μερικές απειλές που οφείλονται κυρίως στην μη προσεκτική υλοποίηση και εκτέλεση του κρυπτοσυστήματος. Επίσης αυτό το κρυπτοσύστημα μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός συστήματος ψηφιακών υπογραφών. Αυτό το σύστημα απαιτεί ότι όλες οι οντότητες θα έχουν στην κατοχή τους αντίστοιχα ζεύγη δημόσιου και ιδιωτικού κλειδιού. Επίσης στο κρυπτοσύστημα RSA ένας αντίπαλος μπορεί να εκτελέσει ενεργητική επίθεση και να αναδιατάξει το μήνυμα και την υπογραφή του κατά τη μεταφορά τους από τον αποστολέα στον παραλήπτη. Ο αντίπαλος επίσης έχει τη δυνατότητα να επαναλάβει αρισμένα τμήματα του μηνύματος κατοπτρίζοντας τις επαναλήψεις και στα αντίστοιχα τμήματα ψηφιακής υπογραφής. Επίσης αυτό το κρυπτοσύστημα έχει ένα μειονέκτημα το οποίο είναι ότι απαιτεί κλειδιά με μήκος τουλαχιστον 1024bit για ασφάλεια δεν είναι όπως οι αλγόριθμοι συμμετρικού κλειδιού που χρησιμοποιούν 128bit, γεγονός που την κάνει πολύ αργή. Για να κρυπτογραφήσουμε ένα μήνυμα P για παράδειγμα υπολογίζουμε το $C=P^e(modn)$, για να αποκρυπτογραφήσουμε όμως το C υπολογίζουμε το $C=P^d(modn)$. Η ασφάλεια της μεθόδου βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων αριθμών. (Tanenbaum, 2011) (Βασίλειος Αν. Κάτος, 2003)

2.3 Τύποι κλειδιών

Οι τύποι των κλειδιών ταξινομούνται ανάλογα με τον τύπο και με τη χρήση του κρυπταλγόριθμου. Χωρίζονται σε τρεις κατηγορίες:

- ✓ Το μυστικό κλειδί το οποίο προσδιορίζεται σε συμμετρικό κρυπτοσύστημα και θα πρέπει να βρίσκεται στην κατοχή όλων των μελών που επικοινωνούν χρησιμοποιώντας συμμετρική κρυπτογραφία.
- ✓ Το δημόσιο κλειδί ορίζεται σε ασύμμετρο κρυπτοσύστημα και αυτό το κλειδί αναφέρεται σε κάποιο μέλος με το οποίο είναι επιθυμητή η επικοινωνία. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.
- ✓ Το ιδιωτικό κλειδί ορίζεται σε ασύμμετρο κρυπτοσύστημα και συνδέεται κρυπτογραφικά με το δημόσιο κλειδί και είναι γνωστό σε ένα μόνο μέλος. (Βασίλειος Αν. Κάτος, 2003)

2.4 Αλγόριθμοι συμμετρικού κλειδιού

Οι αλγόριθμοι αυτοί χρησιμοποιούνται για μεγάλο όγκο δεδομένων ή επίσης για δεδομένα σε συνεχή ροή και είναι σχεδιασμένοι για να εκτελούνται με ταχύτητα και έχουν μεγάλο αριθμό πιθανόν κλειδιών. Οι καλύτεροι αλγόριθμοι συμμετρικού κλειδιού φτάνουν το τέλειο αν ένα δεδομένο κρυπτογραφηθεί με ένα δοσμένο κλειδί, δεν υπάρχει τρόπος να το αποκρυπτογραφήσεις χωρίς να έχεις το ίδιο κλειδί. Υπάρχουν πολλοί αλγόριθμοι συμμετρικού κλειδιού σε χρήση σήμερα. Μερικούς από αυτούς τους συναντάμε συνήθως για την ασφάλεια του web. Ένας από αυτούς τους αλγόριθμους είναι ο DES. Ο αλγόριθμος συμμετρικού κλειδιού ή αλλιώς προσωπικού χρησιμοποιείται συχνότερα για να προστατεύσει πληροφορίες που είναι αποθηκευμένες στον σκληρό δίσκο ενός υπολογιστή, ή για να κρυπτογραφήσει πληροφορίες που μεταφέρονται μέσω επικοινωνιακού συνδέσμου ανάμεσα σε δύο διαφορετικές μηχανές. Επίσης είναι πολύ γρηγορότερη από την κρυπτογραφία δημόσιου κλειδιού και ευκολότερη στην εφαρμογή. (Βασίλειος Αν. Κάτος, 2003)

2.4.1 Επιθέσεις πάνω σε αυτόν τον αλγόριθμο

Οι επιθέσεις κατα κρυπτογραφημένων πληροφοριών χωρίζονται σε τρεις κύριες κατηγορίες. Οι οποιες είναι:

- ✓ Επιθέσεις αναζήτησης κλειδιού

Είναι ο ευκολότερος τρόπος να σπάσεις έναν κώδικα και να δοκιμάσεις όλα τα πιθανά κλειδιά το ένα μετά το άλλο. Οι περισσότερες προσπάθειες θα αποτύχουν αλλά κάποια στιγμή θα βρει το σωστό κλειδί και έτσι είτε θα του επιτρέψει να μπει στο σύστημα ή θα του επιτρέψει να αποκρυπτογραφήσει το κρυπτογράφημα. Και δεν μπορούμε να αμυνθούμε εναντίον αυτού του τρόπου επίθεσεις γιατί δεν μπορούμε να εμποδίσουμε τον επιτιθέμενο να προσπαθήσει να αποκρυπτογραφήσει το μήνυμα μας με κάποιο πιθανό κλειδί. Αυτές οι αναζητήσεις δεν είναι πάντα πολύ αποτελεσματικές καθώς μερικές φορές δεν υπάρχει καμία πιθανότητα να προλάβουν να δοκιμάσουν όλα τα κλειδιά, αλλά συνήθως αύτες οι επιθέσεις καταλήγουν στο να αποκρυπτογραφούν κάποιο μήνυμα επειδή οι χρήστες διαλέγουν κλειδιά με μικρούς κωδικούς.

- ✓ Επιθέσεις κρυπτανάλυσης

Αυτή η επίθεση μπορεί να έχει δύο στόχους. Ο κρυπταναλυτής ίσως έχει το κρυπτογράφημα και θέλει να ανακαλυψει το καθαρό κείμενο, ή ίσως να έχει το κρυπτογράφημα και να θέλει να βρει το κλειδί με το οποίο κρυπτογραφήθηκε.

- ✓ Επιθέσεις βασισμένες στο σύστημα κρυπτογράφησης

Ένας άλλος τρόπος να σπάσουμε ένα κρυπτογραφικό σύστημα είναι να επιτεθούμε στο κρυπτογραφικό σύστημα που χρησιμοποιεί έναν αλγόριθμο χωρίς ουσιαστικά να επιτεθούμε στο κρυπτογραφικό αλγόριθμο. Πολλές από τις

πρόσφατες επιθέσεις εναντίον των εφαρμογών SSL της Netcape ήταν επιθέσεις του Netscape Navigator παρά του ίδιου του SSL πρωτόκολλου. Σε μια άλλη επίθεση ερευνητές ανακάλυψαν ότι μπορούν εύκολα να τροποποιήσουν το ίδιο το πρόγραμμα έτσι ώστε η γεννήτρια τυχαίων αριθμών να μην μπορεί να εκτελεστεί, έτσι δεν χρειάζεται να μαντέψουμε το κλειδί. (Βασίλειος Αν. Κάτος, 2003)

2.5 Αλγόριθμοι δημόσιου κλειδιού

Το δημόσιο κλειδί είναι αυτό το οποίο ορίζεται σε ασύμμετρο κρυπτοσύστημα. Αυτό το κλειδί είναι εκείνο το οποίο αναφέρεται σε κάποιο μέλος με το οποίο είναι επιθυμητή η επικοινωνία. Το δημόσιο κλειδί είναι γνωστό σε όλους. Η ύπαρξη κρυπτογραφίας δημοσίου κλειδιού πρωτοπαρουσιάστηκε το 1975. Μέχρι τότε μια ποικιλία από κρυπτογραφικά συστήματα δημοσίου κλειδιού είχαν αναπτυχθεί. Δυστυχώς υπήρχαν σημαντικά λογότερα κρυπτογραφικά συστήματα δημοσίου κλειδιού από ότι συμμετρικού κλειδιού. Η αιτία έχει να κάνει με τον τρόπο που έχουν σχεδιαστεί οι αλγόριθμοι. Οι αλγόριθμοι δημοσίου κλειδιού στηρίζονται στα μαθηματικά. Αναπτύσσοντας έναν τέτοιο αλγόριθμο απαιτείται να λυθεί ένα μαθηματικό πρόβλημα με ειδικές ιδιότητες. (Βασίλειος Αν. Κάτος, 2003) (Βικιπαίδεια(2.5))

2.5.1 Επιθέσεις πάνω σε αυτόν τον αλγόριθμο

Οι αλγόριθμοι δημόσιου κλειδιού είναι πιο ευάλωτοι στις επιθέσεις από αυτούς του συμμετρικού κλειδιού γιατί ο επιτιθέμενος έχει ένα αντίγραφο του δημόσιου κλειδιού που χρησιμοποιήθηκε για την κρυπτογράφηση του μηνύματος. Αυτές οι επιθέσεις χωρίζονατι σε δυο κατηγορίες:

- ✓ Επιθέσεις παραγοντοποίησης

Αυτές οι επιθέσεις είναι πολύ δημοφιλείς στα συστήματα δημόσιου κλειδιού γιατί είναι πολύ εύκολες να κατανοηθούν. Αυτή η επίθεση αποσκοπεί να αντλήσει το προσωπικό κλειδί από το αντίστοιχο δημόσιο κλειδί. Στην επίθεση αυτή χρειάζεται να επιλύσουμε διάφορα είδη μαθηματικών προβλημάτων.

- ✓ Αλγοριθμική επίθεση

Ένας άλλος τρόπος επίθεσης είναι να βρούμε ένα βασικό ελάττωμα ή αδυναμία του μαθηματικού προβλήματος στο οποίο είναι βασισμένο το σύστημα κρυπτογράφησης. (Βασίλειος Αν. Κάτος, 2003)

2.6 Diffie-Hellman(Αλγοριθμος για τη Διαχείριση και Ανταλλαγή Κλειδιών)

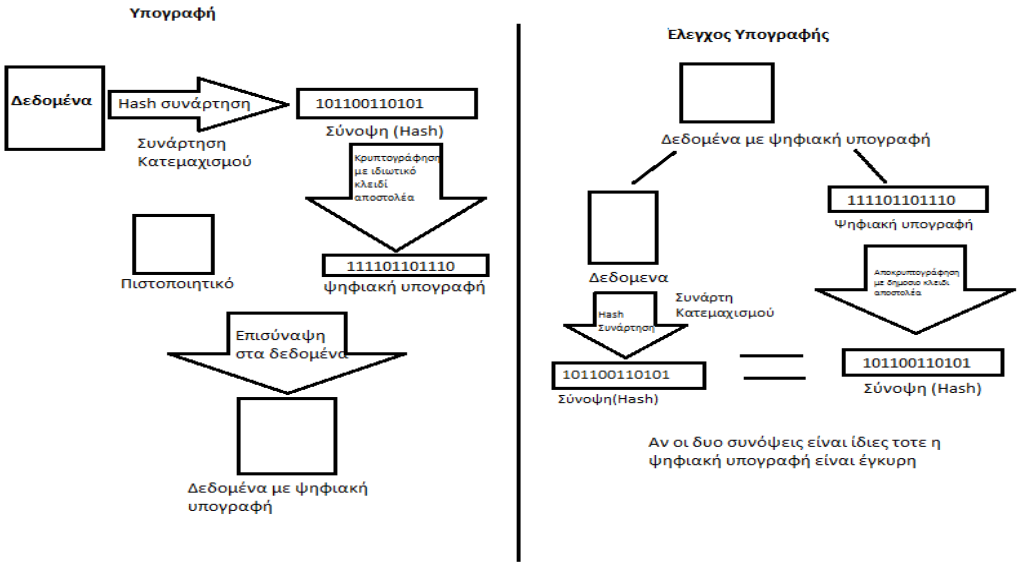
Αυτό το πρωτόκολλο δημιουργήθηκε το 1976 και είναι ένας μηχανισμός ανταλλαγής κλειδιών και αναπτύχθηκε από τους Diffie και Hellman το 1976. Το Diffie Hellman επιτρέπει σε δύο χρήστες να ανταλλάσσουν ένα μυστικό κλειδί μέσα από ένα μη ασφαλές δίκτυο. Οι δύο χρήστες δημιουργούν ο καθένας από ένα ιδιωτικό ακέραιο αριθμό, στη συνέχεια δημιουργούν ένα δημόσιο κλειδί και τέλος ανταλλάσσουν τα δημόσια κλειδία τους. Χρησιμοποιώντας όμως ο καθένας το δημόσιο κλειδί του άλλου δημιουργούν το μυστικό κλειδί. Το πρωτόκολλο έχει δύο παραμέτρους οι οποίοι είναι δημοσιοποιημένοι και μπορούν να χρησιμοποιηθούν από όλους τους χρήστες του συστήματος. Η πρώτη παράμετρος είναι ένας πρώτος αριθμός και η δευτερη παραμετρος είναι ένας ακέραιος. Οι πρώτες εκδόσεις του μηχανισμού γι αυτό το πρωτοκολλο ήταν εύαλωτες σε επιθέσεις ενδιάμεσου. Αυτό το πρωτόκολλο βασίζεται στο πρόβλημα του διακριτού λογάριθμου, που σημαίνει ότι αν ανακαλυφθεί ο αλγόριθμος ο οποίος μπορεί να βρίσκει αποτελεσματικά το διακριτό αλγόριθμο ενός αριθμού ως προς κάποια βάση τοτε το πρωτόκολλο δεν είναι ασφαλές. Το πρωτόκολλο ανταλλαγής κλειδιών θεωρείται ασφαλές στην περίπτωση παθητικής επίθεσης δηλαδή στην περίπτωση που ο αντίπαλος λειτουργεί ως υποκλοπέας και καταγράφει τα μηνυματα που ανταλλάσσονται μεταξύ τους. Ωστόσο όμως στην περίπτωση ενεργητικής επίθεσης το πρωτόκολλο δεν είναι ασφαλές. (Βικιπαίδεια(Diffie-Hellman))

2.7 Ψηφιακές υπογραφές

Η ψηφιακή υπογραφή θεωρείται ως το ηλεκτρονικό ισοδύναμο της συμβατικής υπογραφής και είναι μια συμβολοσειρά που προκύπτει από το συνδυασμό των δυαδικών ψηφίων ενός μηνύματος και αυτών ενός μυστικού κλειδιού. Η χρησιμοποίηση της ψηφιακής υπογραφής σε ένα σύστημα ασφαλείας ενός δικτύου είναι απαραίτητη καθώς παρέχει αυθεντικοποίηση του αποστολέα, εμπιστευτικότητα και ακεραιότητα του μηνύματος.
Οι ασύμμετροι αλγόριθμοι είναι υπολογιστικά αργοί για την κρυπτογράφηση ενός ολόκληρου μηνύματος. Έστω λοιπόν ότι ο Α επιθυμεί να στείλει υπογεγραμμένο έγγραφο ή μήνυμα στον Β. Το πρώτο βήμα είναι γενικά να εφαρμόσει μια hash συνάρτηση στο μήνυμα και να δημιουργήσει ένα message digest. Το message digest είναι συνήθως αισθητά μικρότερο από το πρωτότυπο μήνυμα. Ουσιαστικά η δουλειά της hash συνάρτησης είναι να πάρει ένα μήνυμα οποιουδήποτε μεγέθους και να το συρρικνώσει σε προκαθορισμένο μέγεθος. Για να δημιουργήσει κανείς μια ψηφιακή υπογραφή κρυπτογραφεί συνήθως το message digest και όχι το ίδιο το μήνυμα (μ' άλλα λόγια το κρυπτογραφημένο message digest είναι η ψηφιακή υπογραφή του αποστολέα). Ο Α στέλνει στον Β το κρυπτογραφημένο message digest και το μήνυμα

κρυπτογραφημένο ή όχι. Προκειμένου ο Β να αυθεντικοποιήσει την υπογραφή κάνει τα εξής:

- Εφαρμόζει, πρώτα απ' όλα, την ίδια hash συνάρτηση με τον Α στο μήνυμα που παρέλαβε (το οποίο επαναλαμβάνουμε είναι κρυπτογραφημένο ή απλό κείμενο). Δημιουργεί έτσι τη δική του εκδοχή για το ορθό message digest.
- Στη συνέχεια αποκρυπτογραφεί τη ψηφιακή υπογραφή την οποία παρέλαβε συνημμένη με το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του Α. Η διαδικασία αυτή οδηγεί στην αναπαραγωγή του message digest το οποίο δημιούργησε ο Α.
- Ο Β έχει τώρα στη διάθεση του δύο message digests. Τα συγκρίνει και αν ταιριάζουν, αυθεντικοποίησε επιτυχώς τη ψηφιακή υπογραφή του Α. Αν όχι, υπάρχουν λίγες πιθανές εξηγήσεις. Είτε κάποιος προσποιείται τον Α, ή το μήνυμα μεταβλήθηκε από τη στιγμή που το υπέγραψε ο Α, ή υπήρξε λάθος στη μετάδοση. (Βασίλειος Αν. Κάτος, 2003)



2.8 Μειονεκτήματα και Πλεονεκτήματα την Συμμετρικής και Ασύμμετρης Κρυπτογραφίας

Το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας, είναι η συνεννόηση και ανταλλαγή του κλειδιού, χωρίς κάποιος τρίτος να μάθει για αυτό. Η μετάδοση μέσα από το Διαδίκτυο δεν είναι ασφαλής γιατί οποιοσδήποτε γνωρίζει για την συναλλαγή και έχει τα κατάλληλα μέσα μπορεί να καταγράψει όλη την επικοινωνία μεταξύ αποστολέα και παραλήπτη και να αποκτήσει το κλειδί. Έπειτα, μπορεί να διαβάσει, να τροποποιήσει και να πλαστογραφήσει όλα τα μηνύματα που ανταλλάσσουν οι δύο ανυποψίαστοι χρήστες. Βέβαια, μπορούν να βασισθούν σε άλλο μέσο επικοινωνίας για την μετάδοση του κλειδιού (π.χ. τηλεφωνία) αλλά ακόμα και έτσι δεν μπορεί να εξασφαλιστεί ότι κανείς δεν παρεμβάλλεται μεταξύ της γραμμής επικοινωνίας των χρηστών. Η ασύμμετρη κρυπτογραφία δίνει λύση σε αυτό το

πρόβλημα αφού σε καμία περίπτωση δεν ταξιδεύουν στο δίκτυο οι εν λόγω ευαίσθητες πληροφορίες.

Άλλο ένα ακόμα πλεονέκτημα των ασύμμετρων κρυπτοσυστημάτων είναι ότι μπορούν να παρέχουν ψηφιακές υπογραφές που δεν μπορούν να αποκηρυχθούν από την πηγή τους. Η πιστοποίηση ταυτότητας μέσω συμμετρικής κρυπτογράφησης απαιτεί την κοινή χρήση του ίδιου κλειδιού και πολλές φορές τα κλειδιά αποθηκεύονται σε υπολογιστές που κινδυνεύουν από εξωτερικές επιθέσεις. Σαν αποτέλεσμα, ο αποστολέας μπορεί να αποκηρύξει ένα πρωτύτερα υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι το μυστικό κλειδί είχε κατά κάποιον τρόπο αποκαλυφθεί. Στην ασύμμετρη κρυπτογραφία δεν επιτρέπεται κάτι τέτοιο αφού κάθε χρήστης έχει αποκλειστική γνώση του ιδιωτικού του κλειδιού και είναι δικιά του ευθύνη η φύλαξη του.

Μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα. Κατά κανόνα, η διαδικασίες κρυπτογράφησης και πιστοποίησης ταυτότητας με συμμετρικό κλειδί είναι σημαντικά ταχύτερη από την κρυπτογράφηση και ψηφιακή υπογραφή με ζεύγος ασύμμετρων κλειδιών. Η ιδιότητα αυτή καλείται διασφάλιση της μη αποκήρυξης της πηγής non-repudiation. Επίσης, τεράστιο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλείδων από οργανισμούς, ώστε να διασφαλίζεται η κατοχή τους νόμιμους χρήστες. Όταν κάποιος απατεώνας κατορθώσει και ξεγελάσει τον οργανισμό, μπορεί να συνδέσει το όνομα του με το δημόσιο κλειδί ενός νόμιμου χρήστη και να προσποιείται την ταυτότητα αυτού του νόμιμου χρήστη.

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

Τα δύο κρυπτοσυστήματα μπορούν να εφαρμοστούν μαζί συνδυάζοντας τα καλά τους χαρακτηριστικά και εξαλείφοντας τα μειονεκτήματα τους. Ένα παράδειγμα τέτοιου συνδυασμού είναι οι ψηφιακοί φάκελοι . (Βασίλειος Αν. Κάτος, 2003)

ΚΕΦΑΛΑΙΟ3: <ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ >

3.1 Κρυπτογραφικές υπηρεσίες(Λειτουργίες)

Οι κρυπτογραφικές υπηρεσίς είναι υπηρεσίες που χρησιμοποιώντας κρυπτογραφία, στοχεύουν στην αντιμετώπιση συγκεκριμένων απειλών. Οι κρυπτογραφικές υπηρεσίες σύμφωνα με το βιβλίο είναι (η εμπιστευτικότητα, η ακεραιότητα, η αυθεντικότητα και η μη-απάρνηση):

- ✓ Η Εμπιστευτικότητα είναι μια προστασία από μη εξουσιοδοτημένη αποκάλυψη της πληροφορίας και θα πρέπει να προσφέρεται με έναν τρόπο που θα είναι αδύνατη η αποκάλυψη ή και η ύπαρξη της πληροφορίας σε μη εξουσιοδοτημένα άτομα. Μερικοί ονομάζουν αυτή την ιδιότητα μυστικότητα αλλά οι περισσότεροι χρησιμοποιούν αυτή τη λέξη για να αναφέρονται στην προστασία της ατομικής πληροφορίας.
- ✓ Η Ακεραιότητα είναι μια προστασία από μη εξουσιοδοτημένη τροποποίηση των δεδομένων και θα πρέπει να παρέχει στον παραλήπτη τη δυνατότητα να μπορεί να ανιχνεύσει πιθανές αλλαγές στο μήνυμα από μη εξουσιοδοτημένα άτομα. Επίσης η ακεραιότητα είναι γνωστή και ως ανίχνευση σφαλμάτων στον χώρο τον τηλεπικοινωνιών και της πληροφορίας, όπου ένα μήνυμα λόγω του θορύβου του καναλιού επικοινωνίας, μπορεί να υποστεί τροποποίηση.
- ✓ Η Αυθεντικότητα είναι μια εξασφάλιση, δηλαδή ότι γνωρίζουμε το χρήστη ή με λίγα λόγια αυτόν που επικοινωνούμε. Η αυθεντικότητα των δεδομένων είναι η εξασφάλιση, δηλαδή ότι ένα μήνυμα προέρχεται πράγματι από τον αποστολέα που πιστεύουμε ότι το έστειλε. Οι ψηφιακές υπογραφές χρησιμοποιούνται για να εξακριβώνουν την ταυτότητα του αποστολέα ενός μηνύματος. Οι παραλλήπτες ενός μηνύματος μπορούν να ελέγξουν την ταυτότητα του αποστολέα, ο οποίος υπέγραψε ψηφιακά το μήνυμα.
- ✓ Η Μη-απάρνηση είναι η υπηρεσία κατά την οποία ο παραλήπτης δεν μπορεί να απαρνηθεί ότι έλαβε το μήνυμα ή η υπηρεσία κατά την οποία ο αποστελέας δεν μπορεί να απαρνηθεί ότι έστειλε το μήνυμα.

Υπάρχει αλληλεξάρτηση της ακεραιότητας και της αυθεντικότητας ενός μηνύματος. Όμως δεν είναι δυνατό να προσφέρεται με επιτυχία μόνον η ακεραιότητα χωρίς να προσφέρεται η αυθεντικότητα και αντίστροφα. Σε περίπτωση που θα προσφέρεται η αυθεντικοποίηση χωρίς την ακεραιότητα ο αντίπαλος θα μπορεί να τροποποιήσει την πληροφορία αυθεντικοποίησης, προσδίδοντας όμως διαφορετικό κάτοχο στο μήνυμα. Ωστόσο σε περίπτωση που προσφέρεται η ακεραιότητα χωρίς την αυθεντικότητα, ο αντίπαλος θα μπορεί να τροποποιήσει το μήνυμα και να επανυπολογίσει το κρυπτογραφικό άθροισμα που προσδιορίζει την ακεραιότητα του μηνύματος. (Βασίλειος Αν. Κάτος, 2003)

3.2 Πρωτόκολλα για την κρυπτογράφηση μηνυμάτων του ηλεκτρονικού ταχυδρομείου (e-mail)

Τα τελευταία χρόνια έχουν αναπτυχθεί και χρησιμοποιηθεί αρκετά κρυπτογραφικά συστήματα στο ιντερνετ. Τα πιο δημοφιλή είναι τα παρακάτω:

- ✓ PGP(Εφαρμογή κρυπτογράφησης για προγράμματα ηλεκτρονικού ταχυδρομείου)
- ✓ S/MIME(Format για κρυπτογράφηση ηλεκτρονικού ταχυδρομείου)

3.2.1 PGP

Για την κρυπτογράφηση, αρχικά χρησιμοποιείται ένας συμμετρικός αλγόριθμος για τη μετάδοση του δημοσίου κλειδιού και στη συνέχεια αποστέλλεται το μήνυμα κρυπτογραφημένο με το κλειδί αυτό. Το PGP παρουσιάστηκε το 1991 (από τον Phill Zimmerman) και χρησιμοποιείται για την ασφαλή αποθήκευση και αποστολή αρχείων μεσω e-mail δηλαδή είναι ένα πλήρες πακέτο ασφάλειας ηλεκτρονικού ταχυδρομλιου το οποίο παρέχει προστασία απορρήτου, πιστοποίηση ταυτότητας, ψηφιακές υπογραφές και συμπίεση όλα σε μια εύκολη μορφή. Αυτό το πρωτόκολλο κρυπτογραφεί τα δεδομένα χρησιμοποιώντας ένα κρυπταλγόριθμο τμήματος, αυτός ο κρυπταλγόριθμος λέγεται IDEA(International Data Encryption Algorithm) ο οποίος χρησιμοποιεί κλειδιά των 128bit. Αυτός ο αλγόριθμος είναι παρόμοιος με τους αλγοριθμους DES και AES. Ο IDEA αναμιγνύει τα bit σε μια σειρά γύρων.
Το PGP συνδυάζει την ευκολία του RSA κρυπτοσυστήματος δημοσίων κλειδιών με την ταχύτητα της συμβατικής κρυπτογράφησης, περιλήψεις μηνυμάτων για ψηφιακές υπογραφές, συμπίεση δεδομένων πριν την κρυπτογράφηση, καλός εργονομικός σχεδιασμός και υψηλού επιπέδου διαχείριση κλειδιών. Επιπλέον το PGP εκτελεί τις λειτουργίες των δημοσίων κλειδιών πιο γρηγορα από τα περισσότερα αντίστοιχα προγράμματα. Το PGP είναι κρυπτογράφηση δημοσίων κλειδιών για τις μάζες. Το PGP χρησιμοποιεί υπάρχοντες κρυπτογραφικούς αλγόριθμους αντί να επινοεί νέους. Επίσης είναι ένας προεπεξεργατής που λαμβάνει ως είσοδο ένα απλό κείμενο και παράγει ως έξοδο υπογεγραμμένο κρυπτοκείμενο σε κωδικοποίηση βάση 64. Για να καταλαβουμε καλυτερα την συμβατική κρυπτογραφία ενός κλειδιού ας υποθέσουμε ότι κάποιος θέλει να στείλει ένα μήνυμα, δεν θέλει όμως να το διαβάσει κανένας αλλος εκτός από τον παραλήπτη, οπότε το κρυπτογραφει με τη χρήση ενός κλειδιού το οποίο θα πρέπει να χρησιμοποιηθεί στην αποκρυπτογράφηση του μηνύματος από τον παραλήπτη του. Επίσης παρέχεται υπηρεσία πιστοποίησης του μηνύματος, όπου το μυστικό κλειδί του αποστολέα μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση του μηνύματος άρα και για την υπογραφή του. Έτσι δημιουργείται μια ψηφιακή υπογραφή του μηνύματος την οποία ο παραλήπτης ή οποιοσδήποτε άλλος μπορεί να ελέγξει χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα για να την αποκρυπτογραφήσει. (Tanenbaum, 2011) (Σημειώσεις(PGP)) (Βικιπαίδεια(PGP))

3.2.2 S/MIME

Το MIME είναι ένα standard για αποστολή αρχείων με binary attachments μέσω του ιντερνετ. Το Secure/MIME είναι μια επέκταση του MIME standard για την αναγνώριση των κρυπτογραφημένων e-mail. Αντίθετα από το PGP, το S/MIME δεν εφαρμόσθηκε σαν ένα αυτόματο πρόγραμμα αλλά σαν ένα εργαλείο που σχεδιάστηκε για να προστίθεται σε διάφορα πακέτα ηλεκτρονικού ταχυδρομίου. Το S/MIME προσφέρει εμπιστευτικότητα εξαιτίας του ότι ο κρυπτογραφικός αλγόριθμος καθορίζεται από τον χρήστη. Για να στείλουμε κρυπτογραφημένα μηνύματα σε κάποιον με το S/MIME πρέπει να έχουμε ένα αντίγραφο του δημόσιου κλειδιού του. Παρέχει επίσης πιστοποίηση ταυτότητας, ακεραιότητα δεδομένων, μυστικότητα και μη απάρνηση. Ωστόσο είναι κ πολύ ευέλικτο, υποστηρίζοντας μεγάλη ποικιλία κρυπτογραφικών αλγορίθμων. (Tanenbaum, 2011)

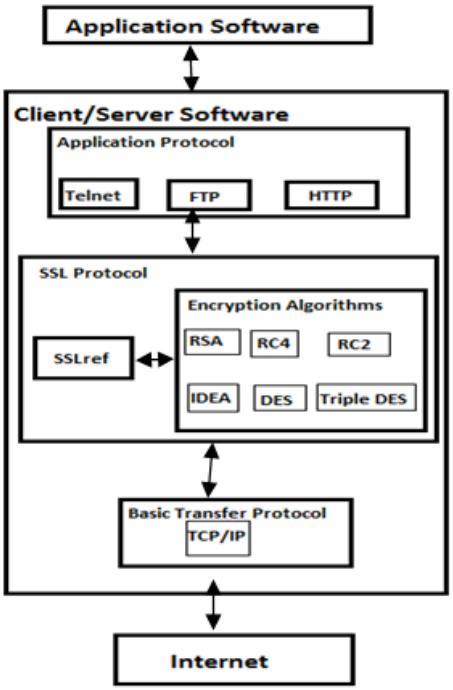
3.3 Πρωτόκολλα δικτύου

Τα πρωτόκολλα δικτύου χρησιμοποιούνται για να παρέχουν εμπιστευτικότητα, ακεραιότητα και αναγνώριση ταυτότητας σε περιβάλλον δικτύου. Τέτοια συστήματα χρειάζονται αλληλεπίδραση πραγματικού χρόνου ανάμεσα στο client κι ενός server για να δουλέψουν σωστά. Τα πιο δημοφιλή είναι τα παρακάτω:

- ✓ SSL(Πρωτόκολλο για να κρυπτογραφεί τις TCP/IP μεταδόσεις)
- ✓ TLS(Transport Layer Security)
- ✓ PTC(Πρωτόκολλο για να κρυπτογραφεί τις TCP/IP μεταδόσεις)
- ✓ SSH(Κρυπτογράφηση απομακρυσμένου τερματικού)
- ✓ SET(Πρωτόκολλο για αποστολή ασφαλών εντολών πληρωμής μέσω ιντερνετ)
- ✓ S-HTTP(Πρωτόκολλο για να κρυπτογραφεί τις HTTP αιτήσεις και απαντήσεις)
- ✓ DNSSEC(Secure Domain Name System)
- ✓ IPSEC

3.3.1 SSL

Το πρωτόκολλο SSL αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Το SSL είναι ένα κρυπτογραφικό πρωτόκολλο για ασφαλή κανάλια επικοινωνίας διπλής κατεύθυνσης. Χρησιμοποιείται συχνά με το TCP/IP πρωτόκολλο του ίντερνετ. Το SSL είναι το κρυπτογραφικό σύστημα που χρησιμοποιείται από τους web browser αλλά μπορεί να χρησιμοποιηθεί σε οποιαδήποτε υπηρεσία TCP/IP. Αυτό το πρωτόκολλο χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου, όπως είναι για παράδειγμα το HTTP (προβολή ιστοσελίδων), το FTP (μεταφορά αρχείων) και το IMAP(email). Άρα λοιπόν αυτό που ουσιαστικά κάνει το SSL είναι να παίρνει τις πληροφορίες από τις εφαρμογές υψηλότερων επιπέδων, να τις κρυπτογραφεί και στην συνέχεια να τις μεταδίδει στο Internet προς τον Η/Υ που βρίσκεται στην απέναντι πλευρά και τις ζήτησε. Πάντα, όταν επισκεπτόμαστε μια ιστοσελίδα που χρησιμοποιεί SSL certificate, υπάρχουν συγκεκριμένα στοιχεία, που αποδεικνύουν ότι βρισκόμαστε υπό ασφαλή σύνδεση. Κάποια από αυτά είναι ένα μικρό εικονίδιο με λουκέτο, το πρόθεμα https που εμφανίζεται μπροστά από την διεύθυνση της ιστοσελίδας, καθώς και το σύμβολο της εταιρίας η οποία παρέχει το πιστοποιητικό και εγγυάται την ασφαλή ανταλλαγή δεδομένων αλλά και την ταυτότητα της ιστοσελίδας. Τα SSL δεν διασφαλίζουν μόνο στον χρήστη την ορθή ταυτότητα της ιστοσελίδας, αλλά ταυτόχρονα και στην ίδια την ιστοσελίδα ότι ο επισκέπτης εισάγει σωστά και έγκυρα στοιχεία. Έτσι, μέσα από μία συναλλαγή, τόσο η εταιρία όσο και ο χρήστης μπορούν να είναι σίγουροι για την ασφάλεια των δεδομένων τους. Επίσης, χάρη στην ευρεία χρήση SSL, οι χρήστες του διαδικτύου έχουν εξοικειωθεί με τις https ιστοσελίδες αλλά και με τα διάφορα πρωτόκολλα ασφαλείας, με αποτέλεσμα να δίνουν έμφαση στις ενδείξεις ύπαρξης κάποιου πιστοποιητικού κατά τις online συναλλαγές τους. Αρκετοί χρήστες δεν εμπιστεύονται sites τα οποία ζητάνε στοιχεία και προσωπικά δεδομένα απουσία κάποιου πιστοποιητικού, με αποτέλεσμα να αποφεύγουν την ολοκλήρωση της συναλλαγής. Στην εικόνα βλέπουμε μια αναπαράσταση του πρωτόκολλου. Το SSL υποστηρίζει δυο υποπρωτόκολλα το πρώτο είναι εγγραφής SSL το οποίο χρησιμοποιείται για την μετάδοση μεγάλων όγκων δεδομένων και το δευτερο είναι χειραψίας SSL το οποίο χρησιμοποιείται για να εγκαταστήσει τους κωδικούς και τους αλγορίθμους

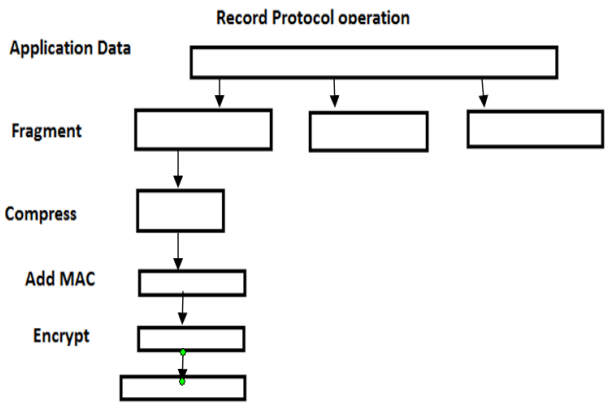


που θα χρησιμοποιηθούν για τη μεταφορά δεδομένων. Στο SSL οι αλγόριθμοι που υποστηρίζονται είναι ο DES(Digital Signature Algorithm), KEA(είναι ένας αλγόριθμος που χρησιμοποιείται για την ανταλλαγή κλειδιών), RSA(αλγόριθμος δημοσίου κλειδιού) και τον τριπλο DES. Σκοπός αυτού του πρωτόκολλου είναι η ενθυλάκωση πρωτοκόλλου υψηλότερου επιπέδου. (Tanenbaum, 2011) (Βικιπαίδεια(SSL)) (ίντερνετ)

3.3.2 TLS

Το TLS είναι ένα πρωτόκολλο που εγγυάται ότι κατά την επικοινωνία εξυπηρετητή-πελάτη μέσω του διαδικτύου δεν πρόκειται να μεσολαβήσει κάποιος τρίτος που θα υποκλεψει το περιεχόμενο της επικοινωνίας. Πιο συγκεκριμένα οι στόχοι του είναι σε σειρά προτεραιότητας και είναι οι εξής:
1. Κρυπτογραφική ασφάλεια
2. Διαλειτουργικότητα
3. Επεκτασιμότητα
4. Σχετική αποδοτικότητα

Το TLS χρησιμοποιείται ως ενδιάμεσο πρωτόκολλο μεταξύ επιπέδου εφαρμογών και του επιπέδου μεταφοράς. Ωστόσο το TLS ανταλλάσει “έγγραφα” που ενθυλακώνουν τα δεδομένα που ανταλλάσσονται και κάθε έγγραφο έχει ένα πεδίου “τύπου περιεχομένου” που ορίζει τον τύπο του εγγράφου, ένα πεδίο μήκους και ένα πεδίο έκδοσης του TLS. Χρησιμοποιεί ασύμμετρη κρυπτογραφία για ανταλλαγή κλειδιών, συμμετρική κρυπτογραφία για ιδιωτικότητα και κωδικες επαλήθευσης αυθεντικοποίησης μηνυμάτων για επαλήθευση της ακεραιότητας ρων δεδομένων. Επίσης ανταλλάσει έγγραφα που ενθυλακώνουν τα δεδομένα που ανταλλάσονται. Τα πακέτα μπορεί να είναι συμπιεσμένα, παραγεμισμένα, κρυπτογραφημένα ή και να περιέχουν κώδικες αυθεντικοποίησης μηνυμάτων(MAC),ανάλλογα βέβαια με την κατάσταση της σύνδεσης. Το TLS πρωτόκολλο επιτρέπει στις εφαρμογές πελάτη-εξυπηρετητή να επικοινωνούν δια μέσου του δικτύου με συγκεκριμένο τρόπο. Εφόσον τα πρωτόκολλα μπορουν να να λειτουργούν με ή χωρίς TLS ή SSL, είναι απαραίτητο δηλαδή ο πελάτης να δείχνει στον εξυπηρετητή την εγκαθίδρυση της σύνδεσης TLS. Υπάρχουν δυο βασικοί τρόποι να επιτευχθεί κάτι τέτοιο. Η πρώτη επιλογή είναι η χρήση διαφορετικού αριθμού θύρας για το TLS όταν αυτό συνδέεται, για παράδειγμα είναι δυνατή η χρήση της θύρας 443 για το HTTPS. Και η δευτερη λύση είναι ο πελάτης να ζητήσει από τον εξυπηρετητή να αλλάξει τη σύνδεση με το TLS χρησιμοποιώντας ένα ειδικό μηχανισμό πρωτοκόλλου, για παραδειγμα STARTTLS για ηλεκτρονικό ταχυδρομείο και πρωτόκολλα ειδήσεων. Ο RC4(λογισμικό κρυπτογράφησης stream δεδομένων) χρησιμοποιεί το TLS για την προστασία της κίνησης στο διαδίκτυο και την ασφάλεια των ασύρματων δικτύων.



Στο σχήμα φαίνεται η λειτουργία του TLS Record πρωτοκόλλου(είναι ένα πρωτόκολλο που δομείται σε στρώματα και σε κάθε στρώμα τα μηνύματα συμπεριλαμβάνουν

πεδία για το μήκος την περιγραφή και το περιεχόμενο) παρατηρείται λοιπόν ότι λαμβάνει τα μηνύματα και τα μεταδίδει από τις εφαρμογές, διαιρεί τα δεδομένα σε εύκολα διαχειρίσιμα μπλοκ πληροφορίας, συμπιέζει τα δεδομένα, κρυπτογραφεί, εφαρμόζει MAC και μεταδίδει το αποτέλεσμα. Ενώ στο τέλος στην υποδοχή υποστηρίζει την ανάστροφη λειτουργία δηλαδήτην αποκρυπτογράφηση, αποσυμπίεση και αποστολή στις εφαρμογές. (Βικιπαίδεια(TLS)) (Λινκ)

3.3.3 SSH

Το SSH (Secure Shell) είναι ένα ασφαλές δικτυακό πρωτόκολλο το οποίο επιτρέπει τη μεταφορά δεδομένων μεταξύ δύο υπολογιστών. Το SSH όχι μόνο κρυπτογραφεί τα δεδομένα που ανταλλάσσονται κατά τη συνεδρία αλλά προσφέρει επίσης και ένα ασφαλές σύστημα αναγνώρισης καθώς και άλλα χαρακτηριστικά όπως ασφαλή μεταφορά αρχείων. Ωστόσο παρέχει κρυπτογραφικά προστατευμένα εικονικά τερματικά και λειτουργίες μεταφοράς αρχείων. Το πρωτόκολλο SSH επιτρέπει τους χρήστες να συνδέονται, σε συστήματα που το υποστηρίζουν από απόσταση. Συγκρινόμενο με το telnet, το SSH αποκρύπτει τα δεδομένα που ανταλλάσσει ο συνδεόμενος χρήστης με το σύστημα, κάνοντας την επικοινωνία ασφαλέστερη και για τον χρήστη αλλά και για το σύστημα.
Στο SSH πρωτόκολλο, ο συνδεόμενος υπολογιστής (client machine) ξεκινάει μια σύνδεση με τον διακομιστή (server machine).
Το SSH υποστηρίζει και μερικά μέτρα προφύλακης, το πρώτο είναι ότι μετά την αρχική σύνδεση ένας συνδεόμενος υπολογιστής ελέγχει ότι η σύνδεση γίνεται με τον συγκεκριμένο διακομιστή και κατα την διάρκεια όλων των επόμενων υπο συνδέσεων συνεχίζεται ακόμα με αυτον τον υπολογιστή. Το δευτερο είναι ότι ο συνδεόμενος υπολογιστής στέλνει τις πληροφορίες της πιστοποίησης στον διακομιστή, αυτές περιλαμβάνουν το όνομα του χρήστη και έναν κρυφό κωδικό σε κωδικοποιημένη μορφή. Και το τελευταίο είναι ότι όλα τα δεδομένα που διακινολυνται κατα την επικοινωνία των δύο υπολογιστών είναι κωδικοποιημένα με 128bit στον αλγόριθμο κρυπτογράφησης.
Λόγω του ότι το SSH κρυπτογραφεί όλα τα δεδομένα που στέλνονται και λαμβάνονται μπορεί να χρησιμοποιηθεί για να προστατεύσει αλλά πρωτόκολλα επικοινωνίας. Έτσι υπάρχει ένας μεγάλος αριθμός προγραμμάτων που κάνουν τη χρήση του SSH όπως επίσης και πολλές διαφορετικές εκδόσεις client SSH για όλα τα λειτουργικά συστήματα. Σε αυτό το πρωτόκολλο οι αλγόριθμοι που υποστηρίζονται είναι ο RSA, ο MD5, ο 3DES και ο DSA. (Πτυχιακή)

3.3.4 SET

Το SET είναι ένα κρυπτογραφικό πρωτόκολλο σχεδιασμού για την αποστολή κρυπτογραφημένων αριθμών πιστωτκών καρτών μέσω του ίντερνετ. Υπάρχουν τρία μέρη που αποτελούν το SET το πρώτο είναι ένα ηλεκτρονικό πορτοφόλι που υπάρχει στον υπολογιστή του χρήστη, ένας server που τρέχει στα εμπορικά web sites, και ο SET πληρωμής που τρέχει στις διάφορες τράπεζες των εμπόρων. Το πρωτόκολλο αυτό είναι ακόμα υπό ανάπτυξη. Το SET προσφέρει εμπιστευτικότητα για τους αριθμούς των πιστωτικών καρτών, καθώς όταν εμείς θελήσουμε να αγοράσουμε κάτι ο αριθμός της πιστωτικής μας κάρτας κρυπτογραφείται και στέλνεται στον έμπορο και το πρόγραμμα του έμπορου υπογράφει ψηφιακά το μήνυμα πληρωμής και το προωθεί στην τράπεζα όποθ επεξεργάζεται. Το SET παρέχει ακεραιότητα, αναγνώριση ταυτότητας και απαγόρευση απάρνησης χρησιμοποιώντας συναρτήσεις αποσύνθεσης μηνύματος και ψηφιακές υπογραφές. Επίσης το SET είναι το μόνο πρωτόκολλο ηλεκτρονικού εμπορίου που σχεδιάστηκε για συνεργασία με πολλαπλά προγράμματα που προέρχονται από διαφορετικούς κατασκευαστές. (Πτυχιακή(SET)) (Υπολογιστών"Λινκ")

3.3.5 S-HTTP

Το πρωτόκολλο S-HTTP αναπτύχθηκε το 1994. Στη σημερινή του μορφή το πρωτόκολλο ορίζει μια επέκταση του HTTP που μπορεί να χρησιμοποιηθεί για να υποστηρίξει υπηρεσίες ασφάλειας απ' άκρη σ' άκρη σε συναλλαγές www. Επίσης παρέχει ασφαλής μηχανισμούς επικοινωνίας μεταξύ HTTP server-client με σκοπό να επιτρέψει αυθόρμητες εμπορικές συναλλαγές. Στόχος της σχεδίασης ήταν ενα ευέλικτο πρωτόκολλο που διαθέτει πολλαπολους μηχανισμους και αλγορίθμους για την δυνατότητα διαπραγματευσης αυτων. Το πρωτόκολλο παρέχει συμμετρικές δυνατότητες στον client και server που σημαίνει ότι τα μηνύματα και οι προτιμήσεις και των δύο πλευρών μεταχειρίζονται με τον ίδιο τρόπο, ενώ παράλληλα διατηρούνται το μοντέλο συναλλαγής και τα χαρακτηριστικά επικοινωνίας του HTTP.
Το S-HTTP ορίζει δύο μηχανισμούς διακίνησης κλειδιών. Ο πρώτος απαιτεί πιστοποιητικά δημόσιων κλειδιών. Ενώ ο δεύτερος μηχανισμός δεν απαιτεί τέτοια πιστοποιητικά και στην περίπτωση αυτή η συναλλαγή εξασφαλίζεται με ένα κλειδί που έχει εξωτερικά συμφωνηθεί και οι σχετικές πληροφορίες βρίσκονται σε μια από τις συγκεκριμένες γραμμές της επικεφαλίδας S-HTTP. Η προστασία ενός μηνύματος εφαρμόζεται με τρεις διαφορετικούς τρόπους: με υπογραφή, με κρυπτογράφηση και με παραγωγή MACs. Κάθε μήνυμα μπορεί να υπογραφεί, να κρυπτογραφηθεί ή οποιοσδήποτε συνδυασμός αυτών, συμπεριλαμβανομένων της παραγωγής και της παροχής καμίας προστασίας.
Το S-HTTP δημιουργεί μηνύματα τα οποία μπορούν να θεωρηθούν σαν μια συνάρτηση με τρεις εισόδους. Η πρώτη είσοδος είναι ότι το μήνυμα που πρόκειται να προστατευτεί μπορεί να είναι ένα HTTP μήνυμα ή κάποιο άλλο αντικείμενο το οποίο επίσης μπορεί να είναι οποιασδήποτε έκδοδης του πρωτοκόλλου. Η δευτερη εισοδος είναι οι κρυπτογραφικές προτιμήσεις ενός παραλήπτη και αυτές είτε

καθορίζονται σε προήγομενη επικοινωνία είτε βασίζονται σε προρυθμισεις. Κ η τριτη είναι οι κρυπτογραφικές προτιμήσεις του αποστολέα.
Ο αποστολέας συνδυάζει τις προτιμήσεις και των δύο πλευρών και αποφαίνεται για τους αλγόριθμους και μηχανισμούς που θα χρησιμοποιηθούν καθώς και για την μορφή των κλειδιών. Ίσως χρειαστεί η επέμβαση του χρήστη σε περίπτωση πολλών επιλογών. Στο προστατευμένο HTTP μήνυμα, έπειτα, προστίθονται κατάλληλες S-HTTP επικεφαλίδες και παράγεται το τελικό S-HTTP μήνυμα. Οι αλγόριθμοι που υποστηρίζουν αυτό το πρωτόκολλο είναι ανάλογα με το ειδος της παρεχόμενης προστασίας με την οποία χρησιμοποιούνται. Είναι ο αλγόριθμος διαχείρισης κλειδιών όπου ο μηχανισμος που καθορίζεται για την διαχείριση και την ανταλλαγή κλειδιών είναι ο RSA. Σε μια αλλη κατηγορία ειναι οι αλγόριθμοι συμμετρικής κρυπτογραφίας και σε αυτούς τους αλγοριθμους είναι ο DES και ο IDEA. (Tanenbaum, 2011) (Πτυχιακή(S-HTTP)) (Blogspot)

3.3.6 DNSSEC

Το DNSSEC είναι ένα σύστημα που σχεδιάστηκε για να φέρει ασφάλεια στο DNS. Επίσης το DNSSEC χρησιμοποιεί την τεχνολογία των ψηφιακών υπογραφών για να υπογράψει ένα σύνολο εγγραφών πόρων. Η ψυφιακή υπογραφή περιέχει τον κρυπτογραφημένο κατακερματισμό του συνόλου των εγγραφών πόρων. Όπου ο κατακερματισμός είναι ένας κρυπτογραφημένος έλεγχος αθροίσματος των δεδομένων που περιέχονται στο σύνολο των εγγραφών πόρων. Το DNSSEC δημιουργεί και ένα παράλληλο δημόσιο κλειδί υποδομής χτισμένο πάνω στο DNS σύστημα. Κάθε DNS domain καθορίζεται από ένα δημόσιο κλειδί. Ένα τέτοιο δημόσιο κλειδί μπορούμε να το αποκτήσουμε με έναν έμπιστο τρόπο από το εν λόγο domain ή αυτό μπορεί να φορτωθεί από πριν μέσα σε ένα DNS server χρησιμοποιώντας το αρχείο boot του server. Επίσης το DNSSEC αναγνωρίζεται για τις ασφαλης ανανεώσεις πληροφοριών στους DNS servers, κάνοντας το ιδανικό για απομακρυσμένη διαχείριση. Επίσης το DNS παρέχει τη δυνατότητα προσωρινής αποθήκευσης των αρνητικών απαντήσεων. Μια αρνητική απάντηση σημαίνει ότι ένα αντίστοιχο σύνολο εγγραφών πόρων δεν υπάρχει για το ερώτημα. Οι αλγόριθμοι που υποστηρίζουν αυτό το πρωτόκολλο είναι ο DSA, ο MD5. (Σελίδα)

3.3.7 IPSEC

Το IPSec παρέχει κρυπτογράφηση στο επίπεδο του IP και για αυτό το λόγο αποτελεί ένα αξιοσημείωτο κομμάτι της συνολικής ασφάλειας. Οι προδιαγραφές του IPSec ορίζουν δύο νέους τύπους δεδομένων στα πακέτα: την επικεφαλίδα πιστοποίησης (AH-Authentication Header), για την παροχή υπηρεσίας ακεραιότητας δεδομένων και το φορτίο ενθυλάκωσης ασφάλειας (ESP-Encapsulating Security Payload) το οποίο παρέχει πιστοποίηση ταυτότητας και ακεραιότητα

δεδομένων. Ορίζονται επίσης οι παράμετροι επικοινωνίας μεταξύ δύο συσκευών που είναι η διαχείριση των κλειδιών και η συσχετισμοί ασφάλειας. Το IPSEC είναι ένα κρυπτογραφικό πρωτόκολλο σχεδιασμένο από το ίντερνετ. Αυτό το πρωτόκολλο φαίνεται να είναι ένα πρωτόκολλο για την δημιουργία εικονικών προσωπικών δικτύων μέσω του ίντερνετ. Το IPSec διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα των επικοινωνιών δεδομένων σε ένα IP δίκτυο. Επίσης παρέχει τον απαραίτητο μηχανισμό για την ανάπτυξη ευκίνητων λύσεων ασφάλειας σε ένα δίκτυο. Το IPSec παρέχει πολλές επιλογές για την υλοποίηση κρυπτογράφησης και πιστοποίησης ταυτότητας στο δίκτυο. Κάθε IPSec σύνδεση μπορεί να παρέχει είτε κρυπτογράφηση είτε ακεραιότητα και πιστοποίηση ταυτότητας δεδομένων ή και τα δυο. Όταν η υπηρεσία ασφάλειας καθοριστεί οι δυο επικοινωνούντες κόμβοι πρέπει να καθορίσουν ακριβώς ποίους αλγόριθμους θα χρησιμοποιήσουν και αφού αποφασίσουν για τους αλγόριθμους οι δυο συσκευές πρέπει να μοιράσουν κλειδιά σύνδεσης. Οι αλγόριθμοι που υποστηρίζουν αυτό το πρωτόκολλο είναι ο 3DES και ο AES. Το IPSec έχει επίσης δύο καταστάσεις λειτουργίας, η πρωτη είναι η λειτουργία μεταφοράς κ η δευτερη ειναι η λειτουργία της σήραγγας. Στη πρώτη λειτουργια της μεταφοράς μια IPSec επικεφαλιδα AH ή ESP παρεμβάλεται μεταξύ της κεφαλίδας IP και του ανώτερου στρώματος πρωτοκολλου κεφαλιδας. Ενώ η λειτουργία σήραγγας παρεχει προστασια σε ολόκληρο το πακετο IP, για να επιτευχθει αυτό μετα την προσθήκη των πεδίων AH και ESP στο πακετο IP, και ολόκληρο το πακετο μαζι με τα πεδία ασφαλειας αντιμετωπίζονται ως φορτιο ενος εξωτερικού πακετου IP με μια νεα εξωτερικη επικεφαλιδα IP. Ωστόσο ολόκληρο το αρχικό πακετο μεταφερεται μεσω μιας σηραγγας απο το ένα άκρο του δικτυου IP στο αλλο και κατα τη μεταφορα του κανενας δρομολογητης δε μπορει να εξετασει την επικεφαλιδα IP του εσωτερικου πακετου. Επισης με τη λειτουργια αυτη πολλοι υπολογιστες υπηρεσιας σε δικτυα που βρίσκονται πισω απο αντιπυρινικες ζωνες μπορουν να εγκαθιδρυουν ασφαλεις επικοινωνιες χωρις να υλοποιουν οι ιδιοι το πρωτοκολλο IPSec. Ωστόσο η προεπιλεγμένη μέθοδος IPSec για ασφαλή κλειδί είναι το IKE(Internet key exchange) πρωτόκολλο το οποίο έχει σχεδιαστει για να παρεχει αμοιβαια πιστοποίηση στα συστήματα. (Tanenbaum, 2011) (Πτυχιακή(IPSEC))

ΚΕΦΑΛΑΙΟ4:<VIRTUAL PRIVATE NETWORKS >

4.1 Τι είναι τα VPN

Το VPN είναι ένα ιδιωτικό δίκτυο και άρχισε να εμφανίζεται το 1997. Αυτό το δίκτυο είναι ένα περιβάλλον επικοινωνίας στο οποίο η πρόσβαση ελέγχεται με τέτοιο τρόπο ώστε να επιτρέπει συνδέσεις μεταξύ μελων μιας ορισμένης περιοχής ενδιαφεροντος. Το περιβάλλον αυτό κατασκευαζεται μεσα απο τη διασπαση ενός κοινού μεσου επικοινωνιας το οποιο προσφερει υπηρεσιες στο δίκτυο σε μη αποκλειστικη βάση. Τα VPN αποτελούνται από υλικό και λογισμισκό το οποίο καλείται να ικανοποιήσει ένα σύνολο απαιτήσεων που θα κανουν το VPN εύκολο στη χρήση και στη συνάρτηση επίσης ασφαλές και διαθέσιμο στους χρηστες. Η υλοποιηση ενός VPN πρέπει να υποστηρίζει κάποια χαρακτηριστικα τα οποία είναι η διαθεσιμότητα, ο έλεγχος, η διαλειτουργικότητα, η αξιοπιστία, η πιστοποίηση δεδομένων και χρηστών και η επιβάρυνση φορτιου. Επίσης ένα από τα κυριότερα θέματα για τα VPN είναι η ασφαλής μεταδοση των δεδομένων χωρις να παρέχεται η δυνατότητα σε τρίτους να κλέψουν ρα δεδομένα μιας απικοινωνίας. Η ασφάλεια των VPN βασίζεται στην κρυπτογραφική δυνατότητα των αλγόριθμων κρυπτογράφησης. (Διπλωματική) (Λινκ!)

4.2 IPSec

Το IPSec αποτελείται από ένα σύνολο πρωτοκόλλων ανεπτυγμένων από το Internet Engineering Task Force(IETF) με στόχο την ασφαλή μετάδοση και ανταλλαγή δεδομένων μέσω της IP επειδή το TCP/IP δεν ήταν και τόσο ασφαλής. Ωστόσο η εξέλιξη του IPV4 σε IPV6 από την μια παρέχει περισσότερες διευθύνσιες και από την άλλη περιέχει υποχρεωτικά ένα τμήμα προδιαγραφών του IPSec που βελτιώνει σημαντικά το ζήτημα της ασφάλειας. Σήμερα το IPSec αποτελεί έναν από τους πιο διαδεδομένους τρόπους υλοποίησης των VPNs δικτύων. Για το IPSec ο στόχος ήταν να αντιμετωπιστούν οι απειλές οι οποίες ήταν (η απώλεια της ιδωτικότητας των δεδομένων, η απώλεια ακεραιότητας των δεδομένων, η προσποίηση ταυτότητας και η άρνηση των ηπηρεσιών) χωρίς να απαιτείται προσθετως εξοπλισμός ή υπάρχει ανάγκη για ένα σύνολο τροποποιήσεων και αλλαγών σε διαφορες εφαρμογές. Αυτό το πρωτόκολλο προσφέρει κάποιες υπηρεσίς οι οποίες είναι: η ακεραιότητα των δεδομένων, την εξακρίβωση γνησιότηταν της προέλευσης των δεδομένων, την

εμπιστευτικότητα, τον έλεγχο πρόσβασης και την απόρριψη των πακέτων επανεκπομπής. Το IPSec επίσης παρέχει ένα σύνολο αλγόριθμων ασφάλειας καθώς και ένα γενικό πλαίσιο το οποίο επιτρέπει την επικοινωνία δύο οντοτήτων με τη χρήση οποιουδήποτε αλγοριθμου που παρέχει την κατάλληλη ασφάλεια για την επικοινωνία. Η κάθε IPSec σύνδεση μπορεί να προσφέρει είτε κρυπτογράφηση με ESP(Encapsulating Security Payload) είτε ακεραιότητα και πιστοποίηση ταυτότητας δεδομένων με AH(Authentication Header). Επίσης ορίζει και λενα νέο σετ κεφαλίδων το οποίο προστίθεται στα IP πακέτα. Αυτές οι νέες κεφαλίδες που διασφαλίζουν την ασφάλεια των IP ειναι η κεφαλίδα πιστοποίησης ταυτότητας (AH) και ασφαλής ενθυλάκωση της πληροφορίας(ESP). Η κεφαλίδα AH διασφαλίζει την ακεραιότητα, την πιστοποίηση ταυτότητας των δεδομένων καθώς και την αποφυγή διπλότυπων πακετων και δεν παρεχει ασφάλεια εμπιστευτικότητας. Η επικεφαλίδα ESP παρέχει υπηρεσίες για την πιστοποίηση και την ακεραιότητα των πακετων IP που διαβιβάζονται μεταξύ δυο IPSec συστημάτων. Διασφαλίζει την ακεραιότητα και την πιστοποίηση. Επίσης το ESP υποστηρίζει ένα μεγάλο αριθμό αλγοριθμων πιστοποιησης ταυτοτητας και ακεραιότητας όπως HMAC-MD5 και HMAC-SHA1. Ωστόσο παρέχει εμπιστευτικότητα μέσω των μεθόδων κρυπτογράφησης ενός IP πακετου. Επίσης υποστηρίζει και ενα μεγαλο αριθμο συμμετρικών αλγοριθμων κρυπτογράφησης οι οποίοι είναι ο 3DES, ο DES, ο RC5, ο IDEA, ο CAST, ο Blowfish όμως ο πιο συνηθισμένος είναι ο AES(128bit).

Το IPSec έχει και δύο λειτουργίες η πρώτη ειναι η κατάσταση λειτουργίας μεταφοράς. Αυτή η κατάσταση επιτρέπει την επεξεργασία των πακετων βασισμένη στην πληροφορία που βρίσκεται στην IP επικεφαλίδα. Χρησιμοποείται κυρίως για τη διασύνδεση μεταξύ δύο LAN ή για εφαρμογές πελάτη - εξυπηρετητή, δηλαδή με πιο απά λόγια είναι ο τρόπος με τον οποίο μπορούν να επικοινωνήσουν δύο συσκευές του δικτύου. Αυτή η κατάσταση έχει το πλεονέκτημα της προσθήκης μόνο μερικών bytes σε κάθε πακέτο, επίσης οι συσκευες σε ενα δημόσιο δικτυο μπορούν να δουν τον τελικο αποδεκτη του πακετου αφού οι IP μεταδίδουνται μη κρυπτογραφημένες. Η δέυτερη λειτουργία είναι η κατάσταση λειτουργίας διόδου. Σε αυτή τη κατάσταση το αρχικό IP πακετο κρυπτογραφείται και γίνεται το φορτίο ενός καινουριου IP πακετου. Αυτό το πακετο που προκύπτει έχει μια νεα IP διευθυνση. Επιτρέφει επίσης σε μια δικτυακή συσκευη όπως ένας δρομολογητής να ενεργήσει σαν ένας IPSec proxy. Ο δρομολογητής ειναι ο αποστολέας και κρυπτογραφεί τα πακετα και τα προωθεί στην IPSec δίοδο. Το βασικό πλεονέκτημα που έχει αυτή η λειτουργία είναι ότι τα ακραία συστήματα δεν χρειάζονται να έχουν οπωσδήποτε ρυθμίσεις για να απολάβουν τα οφέλη από τη χρήση του IPSec. Επίσης προστατευει το σύστημα από την διαδικασία της ανάλυσης κίνησης. Αποτελεί επίσης τον πιο κοινό τρόπο λειτουργίας όσον αφορά τη σύνδεση μεταξύ δύο gateway συσκευών ή μια συνδεση μεταξυ μιας gateway συσκευής και ενός τερματικού σταθμού. Ωστόσο το IPSec χρησιμοποιεί τη συσχέτιση ασφάλειας για να παρακολουθήσει όλες τις λεπτομέρειες που αφορούν μια δεδομένη IPSec επικοινωνία. Αυτή η συσχέτιση είναι μια

μονοσήμαντη σχέση μεταξύ δύο ή περισσότερων οντοτητων που περιγράφει πως οι οντότητες θα χρσιμοποιήσουν τις υπηρεσίες ασφάλειας έτσι ώστε να επικοινωνήσουν με ασφάλεια. Αυτές οι συσχετίσεις είναι μη κατευθυντικές, δηλαδή για καθε ζευγος υπάρχουν τουλάχιστον δυο συνδεσεις ασφάλειας για παράδειγμα μια από το Α στο Β και μια από το Β στο Α. Όταν μια συσκευή θα στείλει ενα πακετο το οποίο απαιτεί IPSec προστασία θα κοιτάξει τη συσχέτιση ασφάλειας στη βάση των δεδομένων της και όταν η αντίστοιχη συσκευή IPSec λάβει το πακέτο θα κοιτάξει με τη σειρά της τη συσχέτιση ασφαλειας στη βαση των δεδομένων της και θα το επεξεργαστεί όπως ορίζεται. Επίσης εκτός από τις κεφαλίδες AH και ESP ο IPSec περιλαμβάνει και πρωτόκολλα ανταλλαγής κλειδιών. Για τη διαχείριση των κλειδιών επιλέχτηκε ο IKE(Internet Key Exchange) σαν τρόπος ρύθμισης των συσχετίσεων ασφάλειας το οποίο δημιουργεί ένα πιστοποιημένο και ασφαλές κανάλι μεταξύ δύο αντοτήτων και διαπραγματευεται τις συσχετίσεις ασφαλειας για τον IPSec. Η τεχνολογία IPSec στα VNP δίκτυα έχει γίνει αποδεκτή και αποδεικνύεται ιδαίτερα επιτυχημένη αφου αποτελεί μια από τις κυριότερες ασπίδες προστασίας των δεδομένων. (Διπλωματική) (Λινκ!)

4.3 IKE

Αυτή η διαδικασία όπως είπαμε και στο IPSec πιο πάνω δημιουργεί ένα πιστοποιημένο και ασφαλές κανάλι μεταξύ δύο αντοτήτων και διαπραγματευεται τις συσχετίσεις ασφαλειας για τον IPSec. Αυτή η διαδικασία απαιτεί από αυτές τις οντότητες δύο οντότητες να πιστοποιήσουν η μια την αλλη και να μοιρασουν τα κλειδιά. Επίσης αυτες οι οντότητες θα πρέπει να συμφωνήσουν όμως σε ένα κοινό πρωτόκολλο πιστοποίησης μέσω μια κατάλληλης διαδικασίας. Και σε αυτή τη φάση θα υλοποιηθούν κάποιο μηχαισμοί που υλοποιούνται συνήθως. Ο πρώτος μηχανισμός είναι ο Προ Μοιρασμένα Κλειδιά ο οποίος κάνει κρυπτογράφηση συμμετρικού κλειδιού. Ο δευτερος μηχανισμός είναι η Κρυπτογράφηση Δημόσιων Κλειδιών όπυ η κάθε μηχανή παράγει έναν ψευτο τυχαίο αριθμό τονοποίο και κρυπτογραφεί με το δημίσιο κλειδί της αλλης μηχανής. Επίσης υποστηρίζεται μόνο ο αλγόριθμος δημοσιων κλειδιών RSA. Και ο τρίτος μηχανισμος είναι οι Ψηφιακες Υπογραφές όπου η κάθε συσκευη υπογράφει ψηφιακά ένα σύνολο δεδομένων και τα στέλνει στην άλλη. Ως βασικός αλγόριθμος ανταλλαγής κλειδιού του IKE είναι ο Diffie-Hellmann που αναπτύχθηκε το 1976 από τους Diffie και Hellman ο οποίος είναι για τη δημιουργία ενός ή περισσότερων κοινών μυστικών κλειδιών. Μέσω του IKE υλοποιείται η διαχείριση των κλειδιών. Το IKE για να υπολοιηθεί στο IPSec περνά από καποια βήματα το πρωτο είναι η ενεργοποίηση μιας IPSec συνόδου οπου σε αυτό το βήμα καθορίζεται το σύνολο των IP πακετων που προκειται να προστατευθουν μεσω του IPSec. Στο δευτερο βημα είναι η πρώτη φάση όπου είναι η δημιουργία και η

λειτουργία της IKE συσχέτισης ασφάλειας. Στο τριτο βήμα είναι η δευτερη βαση δηλαδή η δημιουργία και η λειτουργία της AH/ESP συσχέτισης ασφάλειας. Στο τεταρτο βήμα είναι η μεταφορά δεδομένων οπου τα IP πακετα που επιλεχθηκαν από το πρωτο βήμα μεταφέρονται. Στο πεμπτο βήμα είναι ο τερματισμός της IPSec συνοδου εφόσον ολοκληρωθεί η μεταφορά των IP πακετων και δεν χρησιμοποιείται η παραπανω συνοδος η τελευταία τότε τερματίζεται. (Διπλωματική) (Λινκ!)

4.4 PPTP

Αυτό το πρωτόκολλο είναι ένας συνδιασμός του Point to Point Protocol και του TCP/IP. Συνδιάζει τα χαρακτηριστικά του PPP και κυρίως του TCP/IP. Ωστόσο μαζί με το IPSec είναι λενα από τα κύρια VPN πρωτόκολλα που χρησιμοποιούνται σήμερα. Μπορεί να πάρει πακέτα όπως IP, IPX, NetBios και να τα μετατρέψει σε ένα καινούριο IP πακέτο για μεταφορά. Χρησιμοποιεί ωστόσο το GRE(Generic Pouting Protocol) για τη μεταφορά των PPP πακέτων. Η κίνηση του PPTP αποτελείται από δύο είδη πακέτων για διαφορετικούς τύπους δεδομένων το πρώτο είναι το data packets τα οποία έχουν υποστεί την διαδικασία του encapsulation χρησιμοποιώντας το Gre v2(Internet Generic Routing Encapsulation Protocol Version 2) και το δευτερο είναι το control packets. Η PPTP σύνδεση ξεκινά σαν ένα handshake μεταξύ δύο απομακρυσμένων σημείων με σκοπό την επίτευξη συμφωνίας στο συμπιεσμένο σχήμα και στη μέθοδο για encapsulation που θα χρησιμοποιηθεί. Κατα τη διάρκει της επικοινωνίας αυτά τα πακέτα μπορούν να τμηματοποιηθούν και ένα PPP header προσθέτει ένα serialization αριθμο για την εξακρίβωση χαμένων πακέτων.
Πάνω από το επίπεδο της IP είναι κατασκευασμένες υπηρεσίες διασωλήνωσης tunneling που προσφέρονται από το PPTP ενώ το PPP πρωτόκολλο βρίσκεται κάτω από το επίπεδο της IP. Το PPTP αναφέρεται στην ασφάλεια ενός LAN με LAN ενώ το PPP δεν ήταν ασφαλές. Ωστόσο για να δημιουργήσει κρυπτογραφημένα κανάλια για την επικοινωνία το PPTP ενσωματώνει το PPP αλλά και το MPPE(Microsoft Point to Point Encryption) όπου χρησιμοποιεί 40bit RC4 και 128bit RC4 κρυπτογράφηση. Τα δεδομένα διακινούνται με τη θύρα TCP 1723 και με το πρωτόκολλο IP GRE(Generic Routing Encapsulation ID 47) το οποίο το έχει ορίσει η αρχή IANA(Internet Assigned Numbers Authority). Το PPTP έχει μια τεχνική ενθυλάκωσης που βασίζεται πάνω στο πρωτόκολλο GRE το οποίο χρησιμοποιείται για να περάσει πρωτόκολλα σύνδεσης πάνω από το διαδίκτυο. Ενα πακέτο PPTP αποτελείται από την κεφαλή GRE και το φορτιο που περιεχει το πακετο. Η IP κεφαλή έχει πληροφορίες για το IP datagram όπως το μήκος πακετου, τη διευθυνση αποστολέα και παραλήπτη.
Το PPTP αποτελείται από τρια είδη επικοινωνίας. Η πρώτη επικοινωνία είναι PPTP σύνδεση: Αυτή γίνεται όταν ο client εγκαταστήσει ένα PPP ή ISDN συνδεσμο με το ISP του.

Η δευτερη είναι PPTP σύνδεση ελέγχου: Χρησιμοποιώντας το ίντερνετ ο χρήστης δημιουργεί την PPTP σύνδεση στον VPN server και θέτει τα PPTP χαρακτηριστικά του tunnel.
Και η τρίτη είναι PPTP data tunnel: Ο client και ο server επικοινωνούν μεταξύ τους μέσω του κρυπτογραφημένου tunnel.
Η επικοινωνία μεταξύ απομακρυσμένων χρηστών και το ιδιωτικό δίκτυο της εταιρείας τους γίνεται με RSA κρυπτογράφηση και πιστοποίηση. Τα πρωτόκολλα πιστοποίησης που χρησιμοποιούνται είναι τα PAP, CHAO και MS-CHAP. Τα πρωτόκολλα κρυπτογράφησης είναι κλειδιών των 40bit όπως RSA-RC4 και DES. (Διπλωματική) (Λινκ!)

4.5 OpenVPN

Το OpenVPN είναι μια εφαρμογή λογισμικού ανοιχτού κώδικα που εφαρμόζει τεχνικές εικονικών ιδιωτικών δικτύων για τη δημιουργία ασφαλών συνδέσεων σε δρομολογημένες ή γεφυρωμένες υπηρεσίες και σε υπηρεσίες απομακρυσμένης πρόσβασης. Χρησιμοποιεί προσαρμοσμένο πρωτόκολλο ασφάλειας που χρησιμοποιεί το SSL/TLS για την ανταλλαγή κλειδιών. Επίσης έχει τη δυνατότητα να χρησιμοποιεί Firewalls και Network Address Translators(NATs). Επίσης επιτέπει στις συσκευες που συνδεονται μεταξύ τους να αυθεντικοποιήσουν η μια την άλλη χρησιμοποιώντας ένα προ διαμοιραζόμενο μυστικό κλειδί, ψηφιακά πιστοποιητικά ή όνομα χρηστη / κωδικό πρόσβασης. Το OpenVPN χρησιμοποίει τη βιβλιοθήκη OpenSSL για να παρέχει κρυπτογράφηση των δεδομένων και των καναλιών ελέγχου. Αυτό επιτρέπει στο OpenSSL να κάνει όλη την εργασία κρυπτογράφησης και αυθεντικοποίησης επιτρέποντας στο OpenVPN να χρησιμοποίει όλους τους κρυπτογραφικούς αλγόριθμους που υπάρχουν διαθέσιμοι στο πακέτο OpenSSL. Επίσης μπορεί να χρησιμοποιήσει τη λειτουργία αυθεντικοποίησης HMAC για να προσθέσει ένα πρόσθετο στώμα ασφάλειας στη σύνδεση. Ωστόσο το OpenVPN έχει διάφορους τρόπους να αυθεντικοποιήσει το κάθε σημείο σύνδεσης στο άλλο και διαθέτει λειτουργίες αυθεντικοποίησης με χρήση προδιαμοιραζόμενων κλειδιών, ψηφιακών πιστοποιητικών και όνομα χρήστη / κωδικό πρόσβασης. Το προδιαμοιραζόμενο μυστικό κλειδί είναι ο πιο ευκολος τρόπος αυθεντικοποίησης ενω το ψηφιακό πιστοποιητικό παρέχει τον πιο ασφαλή τρόπο αυθεντικοποίησης και είναι από τις σημαντικότερες λειτουργίες. Το OpenVPN επίσης μπορεί να εκτελεστεί πάνω από τα πρωτόκολλα UDP ή TCP εφαρμόζοντας πολυπλεξία στα SSL tunnels σε μια μονή πόρτα TCP/UDP. Έχει τη δυνατότητα να λειτουργεί μέσω των περισσότερων proxy servers και λειτουργεί σε πολύ καλό βαθμό μεσω NAT και μεσω firewalls. Ο server έχει τη δυνατότητα να προωθεί ορισμένες επιλογές παραμετροποίησης δικτύου στους clients. Αυτές περιλαμβάνουν τις IP διευθύνσεις, τις εντολές δρομολόγησης κα μερικές επιλογές σύνδεσης. Το OpenVPN προσφέρει διάφορες

εσωτερικές λειτουργίες ασφάλειας. Για να μπορέσει να λειτουργήσει ο OpenVPN server χρειάζεται ενα βασικό αρχείο server.conf που μέσα περιέχει τις βασικές λειτουργίες παραμετροποίησης του server όπως και τις εντολές που καλεί τα modules και ψηφιακά πιστοποιητικά που χρειάζεται κάθε φορά. Τους αλγόριθμους που υποστηρίζει το OpenVPN είναι ο AES, Blowfish, 3DES και CAST-128. (Διπλωματική) (Λινκ!)

<ΣΥΜΠΕΡΑΣΜΑ>

Σε έναν κόσμο χωρίς κρυπτογράφηση δεδομένων θα ήταν αδύνατον να έχουμε ένα προσωπικό email, έναν προσωπικό λογαριασμό στο facebook, ή να χρησιμοποιήσουμε την πιστωτική για αγορές στο Internet. Η κρυπτογράφηση δεδομένων χρησιμοποιείται παντού και είναι η κλειδαριά που κρατάει την ψηφιακή μας ζωή ασφαλή. Η κρυπτογράφηση δεδομένων ακούγεται μυστηριώδης και εξωτική. Και μόνο στην αναφορά της φανταζόμαστε ιδιοφυείς χάκερ να χειρίζονται υπερυπολογιστές σε εργαστήρια κρυμμένα στα έγκατα της γης, σε συνθήκες απόλυτης μυστικότητας, με στρατιωτική φρουρά. Στην πραγματικότητα όμως, η βασική λογική πίσω από την κρυπτογράφηση δεδομένων είναι εξαιρετικά απλή. Αφορά το πώς να "μεταμφιέσουμε" μια πληροφορία, ένα κείμενο, έναν αριθμό ή ένα αρχείο, έτσι ώστε να μην βγάζει κανένα απολύτως νόημα στα μάτια τρίτων. Μόνο όποιος έχει το κλειδί της κρυπτογράφησης θα μπορεί να διαβάσει την αρχική πληροφορία.

Β Ι Β Λ Ι Ο Γ Ρ Α Φ Ι Α

Βιβλία:
Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) Εκδοση 2003
Δίκτυα Υπολογιστών (Tanenbaum, Wetherall) Πέμπτη αμερικάνικη εκδοση 2011

Κεφάλαιο 1ο

1.1. Ιστορική αναδρομή
Βικιπαίδεια_1.1
https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1

1.2 Τι πετυχένουμε με την κρυπτογραφία
Βιβλίο(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης)
Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) Εκδοση 2003

1.3 Αρχές μέτρησης κρυπτογραφικής δύναμης
Βιβλίο(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης)
Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) Εκδοση 2003

Κεφάλαιο 2ο

2.1 Συμμετρική Κρυπτογραφία
Βιβλίο(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης)
Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) Εκδοση 2003

2.1.1 Κρυπτοαλγόριθμος DES
Βιβλίο(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης)
Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) Εκδοση 2003

2.1.2 Τριπλό DES
Βιβλίο(Tanenbaum, Wetherall)
Δίκτυα Υπολογιστών (Tanenbaum, Wetherall) Πέμπτη αμερικάνικη εκδοση 2011

2.1.3 Κρυπτοαλγόριθμος AES

Βιβλία (Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) /(Tanenbaum, Wetherall)

Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) Εκδοση 2003

Δίκτυα Υπολογιστών (Tanenbaum, Wetherall) Πέμπτη αμερικάνικη εκδοση 2011

2.1.4 IDEA

Βικιπαίδεια_2.1.4

https://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm

https://el.wikipedia.org/wiki/%CE%91%CE%BB%CE%B3%CF%8C%CF%81%CE%B9%CE%B8%CE%BC%CE%BF%CF%82

2.1.5 DSS

Σελίδες στο ίντερνετ

http://searchsecurity.techtarget.com/answer/How-RSA-keys-differ-from-DH-DSS-keys

http://searchsecurity.techtarget.com/definition/RSA

Βικιπαίδεια(DSS)

https://simple.wikipedia.org/wiki/RSA_(algorithm)

2.1.6 RC2, RC4, RC5

Βικιπαίδεια(RC2)

https://en.wikipedia.org/wiki/RC2

Βικιπαίδεια(RC4)

https://en.wikipedia.org/wiki/RC4

Βικιπαίδεια(RC5)

https://en.wikipedia.org/wiki/RC5

2.1.7 Blowfish

Βικιπαίδεια(Blowfish)

https://el.wikipedia.org/wiki/Blowfish

2.2 Ασύμμετρη Κρυπτογραφία

Βιβλίο(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης)

Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) Εκδοση 2003

2.2.1 Κρυπτοσύστημα RSA
Βιβλία(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης)/ (Tanenbaum, Wetherall)
Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) Εκδοση 2003
Δίκτυα Υπολογιστών (Tanenbaum, Wetherall) Πέμπτη αμερικάνικη εκδοση 2011

2.3 Τύποι κλειδιών
Βιβλία(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης)
Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) Εκδοση 2003

2.4 Αλγόριθμοι συμμετρικού κλειδιού
Βιβλία(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης)
Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) Εκδοση 2003

2.4.1 Επιθέσεις πάνω σε αυτόν τον αλγόριθμο
Βιβλία(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης)
Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) Εκδοση 2003

2.5 Αλγόριθμοι δημόσιου κλειδιού
Βιβλίο(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης)
Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) Εκδοση 2003
Βικιπαίδεια(2.5)
https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%94%CE%B7%CE%BC%CF%8C%CF%83%CE%B9%CE%BF%CF%85_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D

2.5.1 Επιθέσεις πάνω σε αυτόν τον αλγόριθμο
Βιβλίο(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης)
Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) Εκδοση 2003

2.6.1 Diffie-Hellman
Βικιπαίδεια(Diffie-Hellman)
https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

2.7 Ψηφιακές υπογραφές
Βιβλίο(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης)
Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) Εκδοση 2003

2.8 Μειονεκτήματα και Πλεονεκτήματα την Συμμετρικής και Ασύμμετρης Κρυπτογραφίας

Βιβλίο(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης)

Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) Εκδοση 2003

Κεφάλαιο 3

3.1 Κρυπτογραφικές υπηρεσίες(Λειτουργίες)

Βιβλίο(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης)

Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης(Βασίλειος Αν. Κάτος, Γεώργιος Χρ. Στεφανίδης) Εκδοση 2003

3.2.1 PGP

Βιβλίο(Tanenbaum, Wetherall)

Δίκτυα Υπολογιστών (Tanenbaum, Wetherall) Πέμπτη αμερικάνικη εκδοση 2011

Σημειώσεις(PGP)

http://www.ekoletsou.gr/pdfFiles/PGP.pdf

Βικιπαίδεια(PGP)

https://en.wikipedia.org/wiki/Pretty_Good_Privacy

3.2.2 S/MIME

Βιβλίο(Tanenbaum, Wetherall)

Δίκτυα Υπολογιστών (Tanenbaum, Wetherall) Πέμπτη αμερικάνικη εκδοση 2011

3.3.1 SSL

Βιβλίο(Tanenbaum, Wetherall)

Δίκτυα Υπολογιστών (Tanenbaum, Wetherall) Πέμπτη αμερικάνικη εκδοση 2011

Βικιπαίδεια(SSL)

https://el.wikipedia.org/wiki/SSL

Σελίδα στο ιντερνετ

http://pdplab.it.uom.gr/teaching/ince_2e_gr/Text/C11/SSLacasestudy_7.htm

3.3.2 TLS

Βικιπαίδεια(TLS)

https://en.wikipedia.org/wiki/Transport_Layer_Security

Λινκ

http://tech.yanatm.com/?p=338

3.3.3 SSH

Πτυχιακή

http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/ssh.htm

3.3.4 SET

Πτυχιακή(SET)

http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/set.htm

Δίκτυα υπολογιστών "Λινκ"

http://dgavalas.ct.aegean.gr/CN/slides/CN_08.pdf

3.3.5 S-HTTP

Βιβλίο(Tanenbaum, Wetherall)

Δίκτυα Υπολογιστών (Tanenbaum, Wetherall) Πέμπτη αμερικάνικη εκδοση 2011

Πτυχιακή(S-HTTP)

http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/shttp.htm

Blogspot

http://fuckip.blogspot.gr/2011/07/s-http.html

3.3.6 DNSSEC

Σελίδα στο ιντερνετ

http://digilib.lib.unipi.gr/dspace/bitstream/unipi/4907/1/Ioannou.pdf

3.3.7 IPSEC

Βιβλίο(Tanenbaum, Wetherall)

Δίκτυα Υπολογιστών (Tanenbaum, Wetherall) Πέμπτη αμερικάνικη εκδοση 2011

Πτυχιακή(IPSEC)

http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/ipsec.htm

Κεφάλαιο 4ο

4.1 Τι είναι τα VPN

Διπλωματική

http://vivliothmmy.ee.auth.gr/17/1/%CE%94%CE%B9%CE%B1%CF%83%CF%8D%CE%BD%CE%B4%CE%B5%CF%83%CE%B7_%CE%BA%CE%B1%CE%B9_%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD.pdf

Σελίδα στο ιντερνετ

https://www.bestvpn.com/blog/4147/pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

4.2 IPSec

Διπλωματική

http://vivliothmmy.ee.auth.gr/17/1/%CE%94%CE%B9%CE%B1%CF%83%CF%8D%CE%BD%CE%B4%CE%B5%CF%83%CE%B7_%CE%BA%CE%B1%CE%B9_%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD.pdf

Σελίδα στο ιντερνετ

https://www.bestvpn.com/blog/4147/pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

4.3 IKE

Διπλωματική

http://vivliothmmy.ee.auth.gr/17/1/%CE%94%CE%B9%CE%B1%CF%83%CF%8D%CE%BD%CE%B4%CE%B5%CF%83%CE%B7_%CE%BA%CE%B1%CE%B9_%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD.pdf

Σελίδα στο ιντερνετ

https://www.bestvpn.com/blog/4147/pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

4.4 PPTP

Διπλωματική

http://vivliothmmy.ee.auth.gr/17/1/%CE%94%CE%B9%CE%B1%CF%83%CF%8D%CE%BD%CE%B4%CE%B5%CF%83%CE%B7_%CE%BA%CE%B1%CE%B9_%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD.pdf

Σελίδα στο ιντερνετ

https://www.bestvpn.com/blog/4147/pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

4.5 OpenVPN

Διπλωματική

http://vivliothmmy.ee.auth.gr/17/1/%CE%94%CE%B9%CE%B1%CF%83%CF%8D%CE%BD%CE%B4%CE%B5%CF%83%CE%B7_%CE%BA%CE%B1%CE%B9_%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD.pdf

Σελίδα στο ιντερνετ

https://www.bestvpn.com/blog/4147/pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/