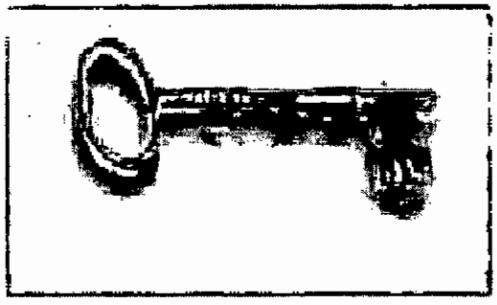
ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΩΝ

Τμήμα: **Επιχειρηματικού Σχεδιασμού & Πληροφοριακών Συστημάτων**
Σχολή: **Οικονομίας και Διοίκησης**

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ ΤΩΝ ΣΥΝΑΛΛΑΓΩΝ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ BUSINESS – TO – BUSINESS (B2B) Ή BUSINESS TO CONSUMER (B2C)



ΕΠΙΒΛΕΠΩΝ:
ΔΑΡΣΙΝΟΣ ΒΑΣΙΛΕΙΟΣ

ΣΠΟΥΔΑΣΤΡΙΑ:
ΚΟΥΤΡΑΦΟΥΡΗ ΚΛΕΑΝΘΗ

ΠΑΤΡΑ 2004

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ
ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ
ΚΡΥΠΤΟΓΡΑΦΙΑ

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ

ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Το πρώτο κεφάλαιο της εργασίας αυτής ξεκινά με μια εισαγωγή για την ανάπτυξη του ηλεκτρονικού εμπορίου κι ακολουθεί μια ιστορική αναδρομή. Επίσης, αναφέρουμε έναν ορισμό της έννοια του ηλεκτρονικού εμπορίου και το κατηγοριοποιούμε. Παρακάτω, μιλάμε για διάφορες τεχνολογίες που χρησιμοποιούνται από επιχειρήσεις προκειμένου να υποστηρίξουν διάφορες εφαρμογές του ηλεκτρονικού εμπορίου. Τέλος, δεν θα παραλείπαμε να αναφερθούμε στα πλεονεκτήματα και στα μειονεκτήματα του ηλεκτρονικού εμπορίου.

1.0 ΕΙΣΑΓΩΓΗ ΓΙΑ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Τα τελευταία χρόνια, η γρήγορη ανάπτυξη της πληροφορικής έχει ανοίξει νέους ορίζοντες σε πολλούς τομείς της ζωής μας. Ένας από αυτούς είναι και το εμπόριο, που με τη βοήθεια της πληροφορικής και των τηλεπικοινωνιών αποκτά νέα μορφή, την ηλεκτρονική.

Ένας πολύ σημαντικός συντελεστής για την ανάπτυξη του ηλεκτρονικού εμπορίου είναι οι ηλεκτρονικές πληρωμές. Με τον όρο ηλεκτρονικές πληρωμές εννοούμε όλες τις διαδικασίες που ξεκινούν από τη στιγμή που ο αγοραστής αποφασίζει ότι θέλει να αγοράσει κάποιο προϊόν ηλεκτρονικά και δίνει εντολή για την έναρξη της διαδικασίας, μέχρι την παραλαβή του προϊόντος που έχει παραγγείλει και την εξόφληση του.

Ήδη αρκετές επιχειρήσεις έχουν δημιουργήσει «ηλεκτρονικά καταστήματα» στο διαδίκτυο. Επίσης πολλές τράπεζες παρέχουν την δυνατότητα στον πελάτη να

διαχειρίζεται το λογαριασμό του μέσω του διαδικτύου. Αν λάβουμε υπόψη μας και την εξάπλωση της πληροφορικής στην κοινωνία, η ύπαρξη τέτοιων τρόπων συναλλαγής καθίσταται αναγκαία, με αποτέλεσμα στο μέλλον όλες οι επιχειρήσεις να παρέχουν τέτοιες υπηρεσίες. Άλλωστε, οι υπέρμαχοι της νέας τάσης στην αγορά όπου οι συναλλαγές γίνονται ηλεκτρονικά, χωρίς προσωπική επαφή ανάμεσα στον πωλητή και τον αγοραστή, αλλά και ούτε ανάμεσα στον καταναλωτή και το προϊόν ισχυρίζονται ότι το ηλεκτρονικό εμπόριο είναι το εμπόριο του μέλλοντος.

1.1 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Η αυγή της ανάπτυξης του ηλεκτρονικού εμπορίου έγινε κατά τη δεκαετία του εβδομήντα με την εμφάνιση των συστημάτων Ηλεκτρονικής Μεταφοράς Χρηματικών Πόρων ή Κεφαλαίων EFT (Electronic Funds Transaction). Η Ηλεκτρονική Μεταφορά Κεφαλαίων πραγματοποιούταν μεταξύ των τραπεζών, οι οποίες χρησιμοποιούσαν ασφαλή ιδιωτικά δίκτυα και με τη πάροδο του χρόνου άλλαξε την εικόνα των χρηματοοικονομικών αγορών.

Στη δεκαετία του ογδόντα εμφανίστηκαν οι τεχνολογίες ηλεκτρονικής επικοινωνίας, οι οποίες βασίζονταν στην αρχιτεκτονική της ανταλλαγής ηλεκτρονικών μηνυμάτων. Τα συστήματα που σχετίζονταν με την ανταλλαγή μηνυμάτων είναι τα γνωστά σε όλους μας EDI (Electronic Data Interchange, Ηλεκτρονική Μεταφορά Δεδομένων), καθώς επίσης και το E-mail (Electronic Mail, Ηλεκτρονικό Ταχυδρομείο). Οι παραδοσιακοί τρόποι επικοινωνίας και ανταλλαγής μηνυμάτων που χρησιμοποιούσαν ως μέσο το χαρτί μπόρεσαν να αντικατασταθούν ηλεκτρονικά για να πραγματοποιηθούν οι παραπάνω εφαρμογές επικοινωνίας.

Στη δεκαετία του ενενήντα τα δίκτυα ηλεκτρονικής επικοινωνίας και κυρίως το Internet προσέφεραν σημαντικές νέες μορφές επικοινωνίας. Έτσι, εφαρμογές όπως η ηλεκτρονική συνδιάσκεψη (conferencing), η ηλεκτρονική συνομιλία (IRC), οι ομάδες συζήτησης (newsgroups), η ηλεκτρονική μεταφορά αρχείων (FTP) καθώς και πολλές άλλες εισήγαγαν καινοτομίες στην ηλεκτρονική επικοινωνία.

Εν συνεχεία, η εμφάνιση του παγκόσμιου ιστού Web και η επικράτηση των προσωπικών ηλεκτρονικών υπολογιστών συντέλεσαν θετικά για τον γρήγορο ρυθμό ανάπτυξης του ηλεκτρονικού εμπορίου, ο οποίος σημείωσε ανοδική πορεία.

Προς το τέλος της δεκαετίας του ενενήντα η καθιέρωση μεθόδων κρυπτογράφησης του περιεχομένου και εξακρίβωσης της ταυτότητας του αποστολέα, έκαναν δυνατή την πραγματοποίηση ασφαλών ηλεκτρονικών συναλλαγών. [1]

1.2 ΤΙ ΕΝΝΟΟΥΜΕ ΜΕ ΤΟΝ ΟΡΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Με τον όρο Ηλεκτρονικό Εμπόριο εννοούμε κάθε εμπορική συναλλαγή, η οποία πραγματοποιείται σε ηλεκτρονικό επίπεδο μέσω του διαδικτύου. Το Ηλεκτρονικό εμπόριο εξαλείφει τον ανθρώπινο παράγοντα, κάνοντας τον περιττό και τα συμμετέχοντα μέλη που λαμβάνουν δράση συναλλάσσονται χωρίς να απαιτείται η φυσική παρουσία τους.

1.3 ΚΑΤΗΓΟΡΙΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Το ηλεκτρονικό εμπόριο μπορεί να διαχωριστεί σε διάφορες κατηγορίες. Ο διαχωρισμός του ηλεκτρονικού εμπορίου γίνεται με κριτήριο τις οντότητες που εμπλέκονται σε μια ηλεκτρονική συναλλαγή. Έτσι μπορούμε να διακρίνουμε τις παρακάτω κατηγορίες ηλεκτρονικού εμπορίου: [2]

1.3.1 Business – to – Government

Η κατηγορία Business – to – Government σημαίνει ότι πραγματοποιούνται ηλεκτρονικές συναλλαγές μεταξύ Κυβέρνησης κι επιχειρήσεων. Αυτός ο τρόπος εμπορίου συχνά περιγράφει τον τρόπο με τον οποίο οι κυβερνήσεις αγοράζον προϊόντα και υπηρεσίες μέσω του Διαδικτύου.

1.3.2 Government – to – Citizen

Η κατηγορία αυτή περιλαμβάνει κάθε είδους αλληλεπίδραση μεταξύ ενός πολίτη και της Κυβέρνησης. Σε αυτή την κατηγορία οι οντότητες που εμπλέκονται μεταξύ τους

μπορούν να αναπτύξουν τις εξής δραστηριότητες: πληρωμή φόρων, ψηφοφορίες, ανανέωση διπλωμάτων οδήγησης καθώς και διάφορες άλλες δραστηριότητες.

1.3.3 Business – to – Consumer

Στην κατηγορία Business – to – Consumer τα εμπλεκόμενα μέλη που συναλλάσσονται μεταξύ τους είναι ένας καταναλωτής και μια επιχείρηση. Οι επιχειρήσεις προσφέρουν την δυνατότητα στους καταναλωτές να αγοράσουν τα προϊόντα που προωθούν μέσα από το Internet. Ένα ενδεικτικό παράδειγμα που μπορούμε να αναφέρουμε είναι η πώληση αεροπορικών εισιτηρίων από τον δικτυακό τόπο μιας αεροπορικής εταιρίας, http://www.britishairways.com)

1.3.4 Consumer – to – Consumer

Η κατηγορία αυτή περιλαμβάνει τις περιπτώσεις όπου κάποιο άτομο προβάλει τα προϊόντα του στο Διαδίκτυο. Με αυτόν τον τρόπο κάθε πολίτης, έχει τη δυνατότητα να πουλά τα προϊόντα του εύκολα και γρήγορα χωρίς να έρχεται σε επαφή με τον αγοραστή. Παράδειγμα τέτοιο είναι οι ηλεκτρονικές δημοπρασίες, όπως αυτές που γίνονται στο: (http://www.fleamarket.gr)

1.3.5 Business – to – Business

Αυτή η κατηγορία ηλεκτρονικού εμπορίου αφορά την πώληση αγαθών ή υπηρεσιών από μια επιχείρηση σε μια άλλη. Για παράδειγμα, μια εταιρία μπορεί να αγοράσει πρώτες ύλες από μια άλλη όταν παρουσιαστεί κάποιο έλλειμμα στην αποθήκη της κι έτσι θα σταλεί αυτόματα παραγγελία στο σύστημα παραγγελιών της άλλης για να την προμηθεύσει.

1.4 ΤΕΧΝΟΛΟΓΙΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Είναι οι τεχνολογίες εκείνες οι οποίες θεμελίωσαν την ανάπτυξη του ηλεκτρονικού εμπορίου και χρησιμοποιούνται εδώ και αρκετά χρόνια για να υποστηρίξουν τις δραστηριότητες των επιχειρήσεων σε διάφορες εφαρμογές του ηλεκτρονικού εμπορίου. Παρακάτω παρουσιάζονται συνοπτικά οι τεχνολογίες ηλεκτρονικού εμπορίου.

1.4.1 Ηλεκτρονική Ανταλλαγή Δεδομένων (Electronic Data Interchange – EDI)

Η τεχνολογία EDI αποτελεί μια από τις σημαντικότερες τεχνολογίες ηλεκτρονικού εμπορίου και με τον όρο EDI εννοούμε την ηλεκτρονική ανταλλαγή μηνυμάτων. Με την τεχνολογία EDI μπορούν να πραγματοποιηθούν διάφορες συναλλαγές μεταξύ των επιχειρήσεων. Τα δεδομένα της κάθε συναλλαγής περνούν από τον υπολογιστή της μίας επιχείρησης στον υπολογιστή της άλλης χωρίς να εμπλέκονται χειρόγραφες διαδικασίες, χωρίς δηλαδή να χρειάζεται ανθρώπινη παρέμβαση οπότε αποφεύγονται τα ανθρώπινα σφάλματα και γίνεται πολύ πιο γρήγορα η όλη διαδικασία.

1.4.2 Ηλεκτρονική Διαχείριση Εγγράφων (Electronic Document Management, EDM)

Η τεχνολογία EDM ορίζεται ως η ηλεκτρονική διαχείριση εγγράφων και αποτελεί την εξελικτική συνέχεια του EDI. Η διαχείριση αυτή γίνεται μέσω ειδικού λογισμικού το οποίο είναι σε θέση να αναγνωρίσει όλα τα εισερχόμενα και εξερχόμενα μηνύματα σε μια επιχείρηση και να τα διαχειριστεί κατάλληλα. Η χρήση της τεχνολογίας EDM οδηγεί στην πλήρη εξάλειψη του χαρτιού όταν πραγματοποιούνται επιχειρηματικές συναλλαγές.

1.4.3 Ηλεκτρονική Μεταφορά Κεφαλαίων (Electronic Funds Transfer, EFT)

Η ηλεκτρονική μεταφορά Κεφαλαίων αναφέρεται στην επικοινωνία που πραγματοποιείται μεταξύ των τραπεζών για την διεκπεραίωση των μεταξύ τους δοσοληψιών και η επικοινωνία αυτή γίνεται με χρήση της τεχνολογίας EDI.

1.4.4 Ηλεκτρονικό Ταχυδρομείο (Electronic Mail, E-mail)

Το ηλεκτρονικό ταχυδρομείο αναμφισβήτητα είναι πλέον γνωστό ότι αποτελεί ένα γρήγορο, οικονομικό και αποδοτικό τρόπο επικοινωνίας μέσω του Internet μεταξύ μεμονωμένων χρηστών σε ολόκληρο τον κόσμο αφού συνδυάζει άμεση διαπροσωπική επικοινωνία, αλλά και ευελιξία στη μεταφορά μηνυμάτων και αρχείων. Το ηλεκτρονικό ταχυδρομείο είναι το αντίστοιχο του παραδοσιακού ταχυδρομείου σε ηλεκτρονική μορφή και αποτελεί την πλέον ευρέως χρησιμοποιούμενη εφαρμογή ηλεκτρονικής επικοινωνίας, όχι μόνο μεταξύ μεμονωμένων χρηστών αλλά και μεταξύ επιχειρήσεων, επιτρέποντας την ανταλλαγή οποιουδήποτε είδους πληροφορίας.

1.4.5 Ηλεκτρονικοί Κατάλογοι (Electronic Catalogues, E-Cat)

Στην ουσία πρόκειται για ηλεκτρονικές σελίδες στο Internet που περιλαμβάνουν πληροφορίες για τα προϊόντα και για τις υπηρεσίες που μπορεί να προσφέρει μια εμπορική επιχείρηση. Ένας τυπικός ηλεκτρονικός κατάλογος περιλαμβάνει λεπτομερή πληροφόρηση για τη συσκευασία, τη μορφή και την τιμή των προϊόντων, ενώ υπάρχει και η δυνατότητα ηλεκτρονικής παραγγελίας, αγοράς και πληρωμής.

1.5 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Το ηλεκτρονικό εμπόριο λειτουργεί θετικά τόσο για τις επιχειρήσεις όσο και για τους καταναλωτές στους οποίους προσφέρει μεγάλες ευκολίες. Τα βασικά πλεονεκτήματα του ηλεκτρονικού εμπορίου είναι τα παρακάτω: [3]

Η αγορά είναι διευρυμένη: Τα όρια του ηλεκτρονικού εμπορίου δεν περιορίζονται από τα αντίστοιχα γεωγραφικά ή εθνικά όρια, όπου στη πραγματικότητα περιορίζουν την εμβέλεια των επιχειρήσεων. Έτσι επιτρέπεται ακόμη και στις μικρότερες επιχειρήσεις να πετύχουν μια σφαιρική παρουσίαση των προϊόντων τους, να συναγωνιστούν με ίσους όρους άλλες επιχειρήσεις άσχετα με το μέγεθος τους και να εδραιωθούν σε παγκόσμιο επίπεδο, αποκτώντας ένα αγοραστικό κοινό οποιασδήποτε εθνικότητας. Είναι προφανές λοιπόν ότι, η ηλεκτρονική προβολή των καταστημάτων αποτελεί των καλύτερο ίσως τρόπο διαφήμισης τους. Το αντίστοιχο όφελος του καταναλωτή είναι ότι μπορεί να επιλέξει αυτό που τον ενδιαφέρει από διάφορους προμηθευτές, χωρίς να τον απασχολεί η γεωγραφική θέση στην οποία βρίσκεται η επιχείρηση.

Ο αυξημένος ανταγωνισμός: Λόγω της διευρυμένης αγοράς ο ανταγωνισμός αυξάνεται και η κάθε επιχείρηση προσπαθεί να κερδίσει τους πελάτες, βελτιώνοντας όχι μόνο την ποιότητα των προϊόντων, αλλά κι ένα σύνολο άλλων πραγμάτων που προσελκύουν τον καταναλωτή. Συμπερασματικά, αν μια εταιρία επιθυμεί να διατηρήσει και να αυξήσει το αγοραστικό της κοινό πρέπει να προσέξει ούτως ώστε η προβολή των προϊόντων της να γίνεται μέσα από ένα εύχρηστο, ευχάριστο, έμπιστο και λειτουργικό περιβάλλον.

1.6 ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Τα βασικά μειονεκτήματα που παρουσιάζει το ηλεκτρονικό εμπόριο είναι τα παρακάτω: [4]

Προβλήματα ασφαλείας: Το δίκτυο είναι ένα μέσο που δεν παρέχει το επιθυμητό επίπεδο ασφάλειας στις συναλλαγές, με αποτέλεσμα και οι συναλλαγές να μην είναι ασφαλείς. Βέβαια σε αυτόν τον τομέα γίνονται εκτεταμένες έρευνες κι εφαρμόζονται πολλές τεχνικές έτσι ώστε οι συναλλαγές να πραγματοποιούνται με όσο το δυνατόν μεγαλύτερη ασφάλεια. Ωστόσο, τα ηλεκτρονικά συστήματα πληρωμών που εφαρμόζονται, παρέχουν λύσεις στα μεγαλύτερα και σημαντικότερα προβλήματα ασφάλειας και μπορεί κανείς να πει ότι είναι εξίσου, αν όχι περισσότερο, ασφαλή και ευέλικτα από τις παραδοσιακές μεθόδους πληρωμών.

Η έλλειψη επαφής μεταξύ του πωλητή και του πελάτη: Το φαινόμενο αυτό δημιουργεί δυσπιστία στον καταναλωτή αφού δεν μπορεί να είναι βέβαιος αν το προϊόν που βλέπει να εμφανίζεται στην οθόνη του υπολογιστή του είναι όντως αυτό που θα παραλάβει ή ακόμη, αν αυτά που ισχυρίζεται η εταιρία για το προϊόν είναι όντως αληθινά.

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ

ΚΡΥΠΤΟΓΡΑΦΙΑ

Στην αρχή του δεύτερου κεφαλαίου εξετάζουμε την συμπεριφορά ενός καταναλωτή ως προς τις ηλεκτρονικές πληρωμές. Όπως αναφέρουμε είναι αναμενόμενο από την πλευρά του – ένας καταναλωτής – να αντιμετωπίζει το ηλεκτρονικό εμπόριο με δυσπιστία και φόβο γι' αυτό το λόγο αναλύουμε κάποια μέτρα για να παρέχεται ασφάλεια στις ηλεκτρονικές συναλλαγές. Πέραν αυτού, υπάρχει και η κρυπτογραφία η οποία μπορεί να συμβάλλει στην αξιοπιστία των ηλεκτρονικών συναλλαγών. Αναμφισβήτητα, η κρυπτογραφία αποτελεί μια σπουδαία μαθηματική εφαρμογή στηριζόμενη σε αλγόριθμους όπου ορισμένοι από αυτούς έχουν παραβιαστεί στο παρελθόν ενώ άλλοι είναι αδύνατο να παραβιαστούν. Όμως, δεν παραλείπουμε να αναφέρουμε το ότι πρέπει να υπάρχει σωστή θωράκιση των αλγορίθμων κρυπτογράφησης.

-"Τι σημαίνει μίλα, φίλε, καὶ είσελθε?", ρώτησε ο Μέρυ.

-"Είναι αρκετά απλό" είπε ο Γκίμλι. "Αν είσαι φίλος πες την λέξη, οι πόρτες θα ανοίξουν και θα μπορέσεις να μπεις".

Άρχοντας των Δαχτυλιδιών

J.R.R. TOLKIEN

2.0 ΕΙΣΑΓΩΓΗ

Όλοι μας αντιλαμβανόμαστε ότι οι καταναλωτές είναι συνηθισμένοι στις παραδοσιακές μεθόδους πληρωμών, οι οποίες πραγματοποιούνται με την φυσική παρουσία των συναλλασσόμενων. Όμως, λόγω της μεγάλης διάδοσης και της ραγδαίας ανάπτυξης του Διαδικτύου δημιουργήθηκαν οι ηλεκτρονικές πληρωμές.

Όπως ήταν φυσικά αναμενόμενο, οι ηλεκτρονικές πληρωμές αντιμετωπίζονται με δυσπιστία τόσο από την πλευρά των επιχειρήσεων όσο και από την πλευρά των καταναλωτών κυρίως γιατί υπάρχει ανησυχία και δισταγμός για την ασφάλεια του δικτύου και των συναλλαγών που πραγματοποιούνται μέσα σε αυτό. Επιπλέον, οι ειδήσεις που κάνουν τον γύρο του κόσμου και αφορούν σε επιτυχείς παραβιάσεις πληροφοριών, παραποίησης εγγράφων και υποκλοπής οικονομικών πληροφοριών (όπως για παράδειγμα, αριθμοί πιστωτικών καρτών), δεν βοηθούν στην καλλιέργεια κλίματος ασφαλείας.

Παρόλα αυτά, μπορεί να επιτευχθεί αξιοπιστία στο ηλεκτρονικό εμπόριο και ειδικότερα στις ηλεκτρονικές πληρωμές εφόσον παρθούν μέτρα για την διασφάλιση των ηλεκτρονικών συναλλαγών. Τέτοια μέτρα μπορεί να είναι εφαρμογή συστημάτων κρυπτογράφησης, χρήση ψηφιακών υπογραφών, όπως θα δούμε παρακάτω. Γι' αυτά τα μέτρα θα μιλήσουμε εκτενέστερα στη συνέχεια.

Με λίγα λόγια, απ' όσα κανείς συμπεραίνει ένα σύστημα ηλεκτρονικού εμπορίου για να είναι πετυχημένο θα πρέπει να είναι ασφαλές. Αυτός άλλωστε είναι ο κύριος παράγοντας που το κρίνει. Για να μπορέσει όμως το σύστημα να είναι ασφαλές, θα πρέπει να είναι καταγεγραμμένα με πλήρη σαφήνεια τα σημεία στα οποία είναι ευάλωτο και με συγκεκριμένες τεχνικές να τα αντιμετωπίσει με επιτυχία καθώς επίσης με ποιον τρόπο θα πεισθεί ο υποψήφιος καταναλωτής για την ασφάλεια και την αξιοπιστία του συστήματος ηλεκτρονικού εμπορίου, για να δεχτεί να ολοκληρώσει τη συνδιαλλαγή και να δώσει τα προσωπικά του στοιχεία και δεδομένα.

2.1 ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Είναι σαφές ότι η ασφάλεια στο ηλεκτρονικό εμπόριο είναι το πιο σημαντικό δεδομένο που πρέπει να αντιμετωπισθεί σοβαρά υπόψη για την υλοποίηση ενός ασφαλούς συστήματος. Προκειμένου λοιπόν να αποφευχθούν οι δυσάρεστες καταστάσεις που αναφέραμε παραπάνω όπως παραβιάσεις, υποκλοπές κι επιθέσεις σε πληροφορίες και προσωπικά στοιχεία θα πρέπει να υλοποιούνται κάποια μέτρα για να παρέχουν ασφάλεια στις ηλεκτρονικές συναλλαγές. Αυτά είναι τα παρακάτω: [5] – [6]

2.1.1 Εμπιστευτικότητα (Confidentiality)

Η εμπιστευτικότητα αποτελεί σημαντικό συστατικό της ιδιωτικότητας του χρήστη (user privacy) καθώς και της προστασίας μυστικών πληροφοριών. Η εμπιστευτικότητα είναι συνυφασμένη με την αποφυγή μη εξουσιοδοτημένης τροποποίησης μιάς πληροφορίας και παρέχεται μέσω κρυπτογράφησης.

2.1.2 Ακεραιότητα (Integrity)

Η ακεραιότητα έχει να κάνει με την αποφυγή τυχόν τροποποιήσεων που μπορούν να συμβούν κατά την ανταλλαγή διαφόρων πληροφοριών στο δίκτυο και παρέχεται μέσω ψηφιακής υπογραφής. Τα συστήματα ηλεκτρονικού εμπορίου πρέπει να χρησιμοποιούν τέτοιες μεθόδους ώστε να μπορούν να διασφαλίσουν ότι τα δεδομένα φτάνουν στον προορισμό τους αναλλοίωτα κι ότι δεν είναι διαθέσιμα σε οποιονδήποτε και για οποιονδήποτε σκοπό, χωρίς την προσωπική έγκριση του.

2.1.3 Διαθεσιμότητα (Availability)

Το μέτρο ασφάλειας της διαθεσιμότητας αποσκοπεί στο να διασφαλίζει την προσπελασιμότητα της πληροφορίας μόνο σε εξουσιοδοτημένους χρήστες και φυσικά όποτε αυτό απαιτείται να συμβεί.

2.1.4 Έλεγχος αυθεντικότητας (Authentication)

Η διαδικασία του ελέγχου της αυθεντικότητας σκοπό έχει να εξακριβώσει την ταυτότητα του χρήστη, την οποία ισχυρίζεται ότι έχει ο χρήστης και να βεβαιώσει ότι το περιεχόμενο του μηνύματος παρέμεινε αναλλοίωτο κατά την μεταφορά. Επίσης, θα πρέπει να αναφέρουμε ότι ο έλεγχος της αυθεντικότητας του χρήστη διενεργείται πριν ξεκινήσει κάποια ηλεκτρονική συναλλαγή και υλοποιείται με τη χρήση

διαφόρων μεθόδων. Πιο συγκεκριμένα, τα συστήματα ασφαλείας ελέγχου της αυθεντικότητας επαληθεύουν τα στοιχεία που ο χρήστης παρέχει με αυτά που το σύστημα ήδη γνωρίζει για το χρήστη. Οι μέθοδοι αυθεντικοποίησης βασίζονται είτε σε κωδικούς πρόσβασης (passwords), είτε σε προσωπικούς αριθμούς αναγνώρισης (Personal Identification Numbers, PIN's).

Κάποια ακόμη θέματα που αφορούν την ασφάλεια είναι:

2.1.5 Εξουσιοδότηση (Authorization)

Η εξουσιοδότηση αφορά την παραχώρηση δικαιωμάτων από τον ιδιοκτήτη στον χρήστη κι έτσι ο χρήστης μπορεί να έχει πρόσβαση σε διάφορα προϊόντα και υπηρεσίες.

2.1.6 Μη αποποίηση της ευθύνης (Non – Repudiation)

Η μη αποποίηση της ευθύνης αποτελεί ένα πολύ σημαντικό τομέα στην ασφάλεια του ηλεκτρονικού εμπορίου. Λέγοντας λοιπόν μη αποποίηση της ευθύνης εννοούμε ότι όταν κάποιος συμμετέχει σε μια ηλεκτρονική συναλλαγή και η συναλλαγή αυτή ολοκληρώνεται, μετά δεν μπορεί να ισχυριστεί ότι δεν συμμετείχε σε αυτήν γιατί το σύστημα εφαρμόζει μεθόδους γνησιότητας της ταυτότητας του ατόμου το οποίο συναλλάσσεται και με αποδεικτικά μέσα εξασφαλίζεται η γνησιότητα της συναλλαγής.

Ο πίνακας που ακολουθεί είναι μια συνοπτική αναφορά των όσων αναφέρθηκαν παραπάνω.

Μέτρα ασφαλείας	**Χαρακτηριστικά**
Εμπιστευτικότητα (Confidentiality)	Προστασία της ιδιωτικότητας του χρήστη και των μυστικών πληροφοριών από τρίτους.
Ακεραιότητα (Integrity)	Τα δεδομένα φτάνουν στον προορισμό τους αναλλοίωτα και δεν είναι διαθέσιμα στον οποιονδήποτε χωρίς έγκριση.

Διαθεσιμότητα (Availability)	Μόνο εξουσιοδοτημένα άτομα έχουν προσπέλαση σε πληροφορίες.
Έλεγχος αυθεντικότητας (Authentication)	Επιβεβαιώνεται η ταυτότητα του χρήστη και το περιεχόμενο των μηνυμάτων.
Εξουσιοδότηση (Authorization)	Παραχωρείται το δικαίωμα στον χρήστη να έχει πρόσβαση σε πληροφορίες και υπηρεσίες.
Μη αποποίησης ευθύνης (Non – Repudiation)	Εφόσον κάποιος συμμετείχε σε κάποια συναλλαγή μετά δεν μπορεί να υποστηρίξει ότι δεν συμμετείχε.

2.2 ΑΣΦΑΛΕΙΑ ΣΤΙΣ ΣΥΝΑΛΛΑΓΕΣ ΜΕΣΩ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Ένας αναμφισβήτητα βέβαιος τρόπος για να διασφαλίσουμε το απόρρητο των πληροφοριών είναι η κρυπτογράφηση. Χάρη στην κρυπτογράφηση και των μέτρων ασφαλείας που αναφέραμε παραπάνω μπορούμε να επιτύχουμε τα βέλτιστα δυνατά αποτελέσματα για την ασφάλεια των ηλεκτρονικών συναλλαγών και να διαφυλάξουμε όλες τις οντότητες που θα λάβουν μέρος για την πραγματοποίηση μιας ηλεκτρονικής συναλλαγής.

2.3 ΤΙ ΕΙΝΑΙ ΚΡΥΠΤΟΓΡΑΦΙΑ

Η κρυπτογραφία είναι μια επιστήμη η οποία στηρίζεται σε μαθηματικούς τύπους και αλγόριθμους υπολογιστών. Μέσω της κρυπτογραφίας έχει κανείς την δυνατότητα να γράφει με μυστικότητα, δηλαδή να κρατά τις πληροφορίες μυστικές και αποτελεί ένα σημαντικό μέρος της ασφάλειας των ηλεκτρονικών συναλλαγών. [7] – [8]

Ο παρακάτω πίνακας που ακολουθεί περιέχει κάποιους όρους, οι οποίοι δεν θα μας απασχολήσουν στην συνέχεια αλλά θεωρούμε σκόπιμο να τους αναφέρουμε.

Έννοιες	Ορισμοί
Κρυπτογραφία (Cryptography)	Η τέχνη της επιστήμης σχετικά με τις αρχές, τα μέσα, και τις μεθόδους για τη μετατροπή των μηνυμάτων σε ακατανόητη μορφή ώστε να μπορούν να τα επαναφέρουν στην αρχική μορφή τους και να τα διαβάσουν μόνο τα κατάλληλα άτομα.
Κρυπτανάλυση (Cryptanalysis)	Η ανάλυση ενός κρυπτογραφικού συστήματος ή /και των εισόδων και των εξόδων του για να εξαχθούν οι εμπιστευτικές μεταβλητές του κρυπτογραφήματος. Ο τελικός στόχος είναι να αποκαλυφθούν οι διαδικασίες που εκτελούνται ώστε να γίνει εφικτή η μετατροπή των κρυπτογραφημένων μηνυμάτων στο αρχικό κείμενο χωρίς γνώση του αλγορίθμου κρυπτογράφησης ή /και των κλειδιών που χρησιμοποιούνται στην κρυπτογράφηση.
Κρυπτολογία (Cryptology)	Είναι ο συνδυασμός της κρυπτογραφίας και της κρυπτανάλυσης σε ένα ενιαίο επιστημονικό κλάδο.
Κρυπτογράφηση	Είναι η εφαρμογή της Κρυπτογραφίας.

2.4 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Η γνώση για την κρυπτογραφία μπορεί να εξακριβωθεί από τους αρχαίους χρόνους. Στην αρχαία Ελλάδα, οι Σπαρτιάτες στρατηγοί χρησιμοποιούσαν μια μορφή κρυπτογραφίας έτσι ώστε να μπορούν να ανταλλάξουν μεταξύ τους μυστικά μηνύματα. Τα μηνύματα γράφονταν σε μακρόστενες ταινίες περγαμηνής, οι οποίες

τοποθετούνταν σε κυλινδρικές σκυτάλες. Όταν ξεδίπλωναν την περγαμηνή, το γραπτό μπορούσε να διαβαστεί μόνο από κάποιο άτομο που κατείχε μια παρόμοια κυλινδρική σκυτάλη με το ίδιο ακριβώς μέγεθος. Αυτό το πρωτόγονο σύστημα έκανε μια αρκετά καλή δουλειά στο να προστατεύει τα μηνύματα από παρεμβολή και από τα μάτια των περίεργων αγγελιοφόρων.

Ο Samuel F. Morse δημόσια παρουσίασε τον τηλέγραφο το 1845, οι χρήστες του τηλεγράφου άρχισαν να ανησυχούν για το πόσο εμπιστευτικά ήταν τα μηνύματα που μετέφεραν. Κάποιος θα μπορούσε να ηχογραφεί τη γραμμή του τηλεγράφου ή να κρατά ένα αντίγραφο του μηνύματος όπου σα συνέπεια θα μπορούσε να το αναμεταδώσει και σε άλλους. Έτσι λοιπόν κωδικοποιούσαν τα μηνύματα με ένα μυστικό κώδικα ώστε να τα αποκωδικοποιεί μόνο ο παραλήπτης. [9]

Από την άλλη μεριά όμως, ο Edgar Allan Poe ο οποίος θεωρούσε την κρυπτογραφία συναρπαστική επιστήμη, ισχυριζόταν ότι, δεδομένης της ανθρώπινης ευφυΐας είναι αδύνατο να εφευρεθεί ένα απαραβίαστο σύστημα κρυπτογράφησης.

Όμως η κρυπτογραφία έγινε ακόμα πιο σημαντική κι έκανε ένα μεγάλο βήμα προς τα εμπρός εκμεταλλευόμενη την ραδιοτηλεφωνία και τη χρήση της στον πόλεμο. Χωρίς κρυπτογραφία, τα μηνύματα που μεταδίδονταν μεταξύ συμμάχων θα μπορούσαν να υποκλαπούν από τον εχθρό.

Σήμερα ο κύριος ρόλος της κρυπτογραφίας είναι να προστατεύσει τις ηλεκτρονικές συναλλαγές.

2.5 ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

Καθαρό κείμενο (clear text ή plain text): Το καθαρό κείμενο είναι το αρχικό μήνυμα σε τέτοια μορφή που να μπορεί να διαβαστεί.

Κρυπτογραφημένο κείμενο (Cipher text): Το κρυπτογραφημένο κείμενο είναι στην ουσία το καθαρό κείμενο αλλά σε συνθηματική μορφή που να μην μπορεί να αναγνωστεί.

Κρυπτοσύστημα (Cryptosystem): Το κρυπτοσύστημα είναι το σύστημα που εκτελεί τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης κειμένων.

Αλγόριθμος κρυπτογράφησης: Λέγοντας αλγόριθμο κρυπτογράφησης εννοούμε μια μαθηματική διαδικασία που χρησιμοποιείται για να μετατρέψει ένα καθαρό κείμενο σε κρυπτογραφημένο κείμενο κι αντιστρόφως.

Κλειδί κρυπτογράφησης: Ένα κλειδί είναι ένας μυστικός κώδικας που χρησιμοποιεί ο αλγόριθμος κρυπτογράφησης για να μετατρέπει τα δεδομένα σε κρυπτογραφημένα και αντίστροφα. Ένα απλό παράδειγμα που θα μπορούσαμε να αναφέρουμε είναι αν υποθέσουμε ότι δυο άνθρωποι επισκέπτονται ένα κατάστημα και αγοράζουν τις ίδιες κλειδαριές από το ράφι. Οι συνδυασμοί των κλειδαριών όμως είναι διαφορετικοί. Στην κρυπτογράφηση η μέθοδος μπορεί να είναι η ίδια (όπως η κλειδαριά), αλλά τα κλειδιά είναι διαφορετικά (όπως οι συνδυασμοί).

Μερικές φορές το κλειδί είναι το ίδιο για την κρυπτογράφηση και την αποκρυπτογράφηση. Άλλες φορές όμως μπορεί να έχουμε ένα ζεύγος κλειδιών, δηλαδή άλλο κλειδί να χρησιμοποιούμε στην κρυπτογράφηση και κάποιο άλλο στην αποκρυπτογράφηση. Ακόμη και αν για κάποιο λόγο ο αλγόριθμος γίνει γνωστός, εξακολουθεί να είναι ασφαλής αν δεν γίνει γνωστό το κλειδί.

Βέβαια, θα πρέπει να επισημανθεί ότι το μέγεθος του κλειδιού είναι ο κύριος παράγοντας διασφάλισης ενός μηνύματος. Για παράδειγμα, αν ένα κλειδί έχει μέγεθος 4 bits (0101), τότε θα υπάρξουν δεκαέξι ενδεχόμενα κλειδιά ($2^4 = 16$). Αν όμως ένα κλειδί έχει περισσότερα bits τότε θα υπάρχουν περισσότερα ενδεχόμενα κλειδιά που θα πρέπει να δοκιμάσει κάποιος επιτιθέμενος για να βρει το σωστό. Άρα από αυτό συμπεραίνουμε ότι τα μακρύτερα κλειδιά είναι περισσότερο δύσκολο να τα βρει κάποιος από τα μικρότερα γιατί υπάρχουν περισσότερες δυνατές περιπτώσεις, όπως αναφέραμε παραπάνω.

Από τα παραπάνω γίνεται φανερό ότι σε ένα κρυπτοσύστημα σημαντικό ρόλο παίζουν ο αλγόριθμος κρυπτογράφησης και το κλειδί κρυπτογράφησης. Με βάση το χρησιμοποιούμενο κλειδί, τα κρυπτοσυστήματα ταξινομούνται σε κατηγορίες, και παρακάτω θα ακολουθήσει μια αναφορά αυτών των κατηγοριών.

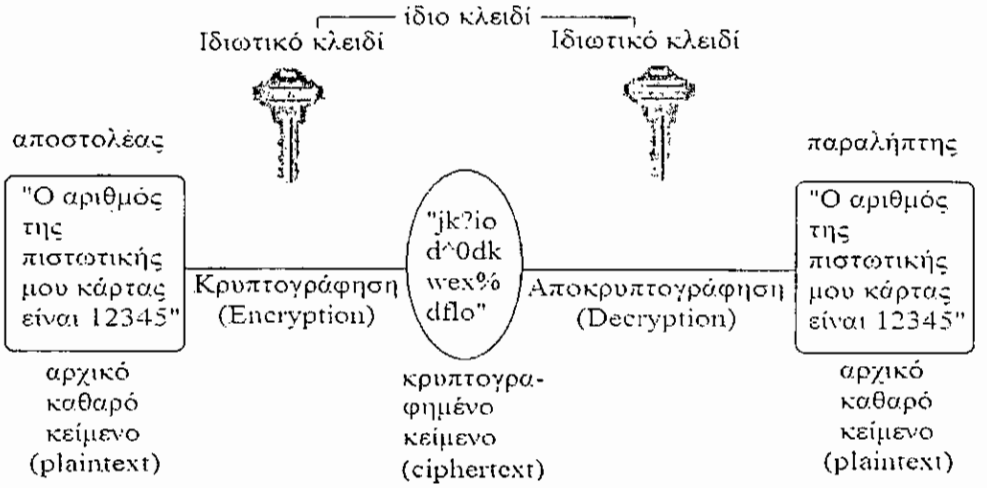
2.6 ΚΑΤΗΓΟΡΙΕΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Συναντάμε δυο κατηγορίες κρυπτογραφίας. Η μια είναι η κρυπτογραφία ιδιωτικού κλειδιού (ή αλλιώς συμμετρική κρυπτογραφία) και η άλλη είναι η κρυπτογραφία δημόσιου κλειδιού (ή αλλιώς ασύμμετρη κρυπτογραφία).

2.6.1 Συμμετρική Κρυπτογραφία (Symmetric Cryptography)

Στη συμμετρική κρυπτογραφία, υπάρχει μόνο ένα κοινό κλειδί το οποίο ονομάζεται ιδιωτικό (private) ή αλλιώς και μυστικό (secret) και χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση. Για να εξασφαλιστεί η μυστικότητα σε ένα συμμετρικό κρυπτοσύστημα θα πρέπει ο αποστολέας και ο παραλήπτης να έχουν συμφωνήσει εξ' αρχής για το κλειδί που θα χρησιμοποιήσουν, χωρίς φυσικά να είναι γνωστό σε άλλους. Ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να αποκρυπτογραφήσει το μήνυμα. Αυτή η μέθοδος καλείται συμμετρική κρυπτογραφία ή κρυπτογραφία μυστικού κλειδιού. Η συμμετρική κρυπτογραφία χρησιμοποιείται όχι μόνο για κρυπτογράφηση, αλλά και για πιστοποίηση ταυτότητας. Η πιστοποίηση ταυτότητας γίνεται με το να υπάρχει διαφορετικό ιδιωτικό κλειδί για κάθε ζεύγος επικοινωνούντων μερών. Με τον τρόπο αυτό όταν κάποιος λάβει ένα μήνυμα από κάποιον άλλον θα είναι βέβαιος πως η ταυτότητα που υποστηρίζει ο άλλος ότι έχει είναι αληθής μόνο εφόσον χρησιμοποιεί το κατάλληλο κλειδί που έχει προσυμφωνηθεί για την μεταξύ τους επικοινωνία. [10] – [15]

Το παρακάτω σχήμα που ακολουθεί είναι μια απεικόνιση συμμετρικής κρυπτογραφίας.



Πλεονεκτήματα της συμμετρικής κρυπτογράφησης

Η συμμετρική κρυπτογραφία είναι γρήγορη, γιατί οι αλγόριθμοι που χρησιμοποιούνται είναι εξαιρετικά ταχείς μιας και βασίζονται σε απλές μαθηματικές σχέσεις που βοηθούν την γρήγορη αποκρυπτογράφηση μεγάλου αριθμού κρυπτογραφημένων μηνυμάτων. Για τους αλγόριθμους ιδιωτικού κλειδιού θα αναφερθούμε παρακάτω.

Μειονεκτήματα της συμμετρικής κρυπτογράφησης

Το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας είναι η συνεννόηση του αποστολέα και του παραλήπτη στο κοινό μυστικό κλειδί που θα χρησιμοποιήσουν για να κρυπτογραφήσουν και να αποκρυπτογραφήσουν την πληροφορία που θα ανταλλάξουν, χωρίς να μαθευτεί από κάποιο άλλο τρίτο πρόσωπο. Επιπλέον, κάθε χρήστης πρέπει να έχει τόσα μυστικά (ή ιδιωτικά) κλειδιά όσα και τα μέλη με τα οποία συναλλάσσεται και η απαίτηση για αυθεντικότητα δεν ικανοποιείται, γιατί δεν μπορεί να αποδειχθεί η ταυτότητα των συναλλασσόμενων μερών. Από την στιγμή που δυο άτομα κατέχουν το ίδιο κλειδί, τότε και οι δυο μπορούν να κρυπτογραφήσουν κάποιο μήνυμα και να ισχυριστούν ότι το έστειλε άλλο άτομο. Κατά συνέπεια, η μη αποποίηση της ευθύνης για την αποστολή ενός μηνύματος καθίσταται και αυτή αδύνατη. Όμως το πρόβλημα αυτό επιλύεται με την ασύμμετρη κρυπτογράφηση ή αλλιώς με την κρυπτογράφηση δημόσιου κλειδιού.

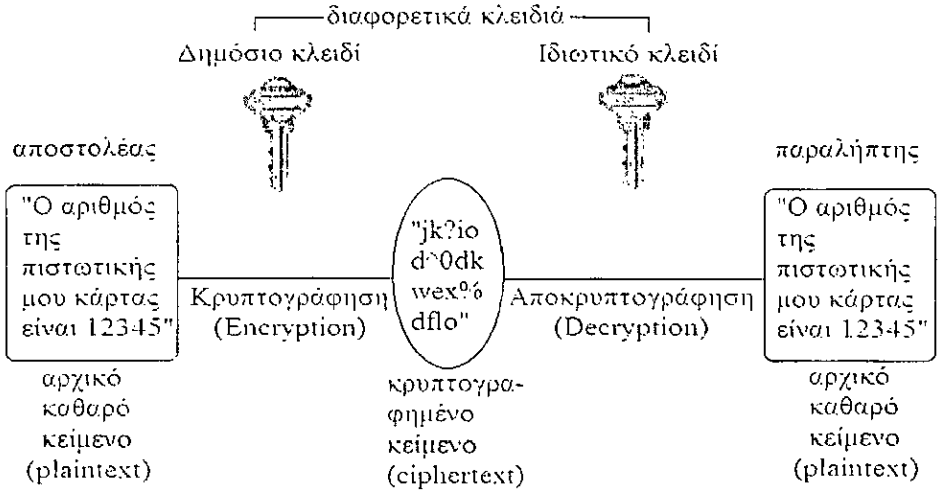
2.6.2 Ασύμμετρη κρυπτογραφία (Asymmetric Cryptography)

Η ασύμμετρη κρυπτογράφηση ή αλλιώς κρυπτογράφηση δημόσιου κλειδιού (public key cryptography), προτάθηκε το 1976 από τους Whitfield Diffie και Martin Hellman. Οι δυο ερευνητές τότε στο Stanford University, έγραψαν ένα έγγραφο στο οποίο υποστήριξαν την ύπαρξη μιας κρυπτογραφικής τεχνικής, με την οποία μια πληροφορία που κρυπτογραφούταν με ένα κλειδί μπορούσε να αποκρυπτογραφηθεί από ένα δεύτερο, χωρίς να έχουν σχέση τα δυο κλειδιά μεταξύ τους.

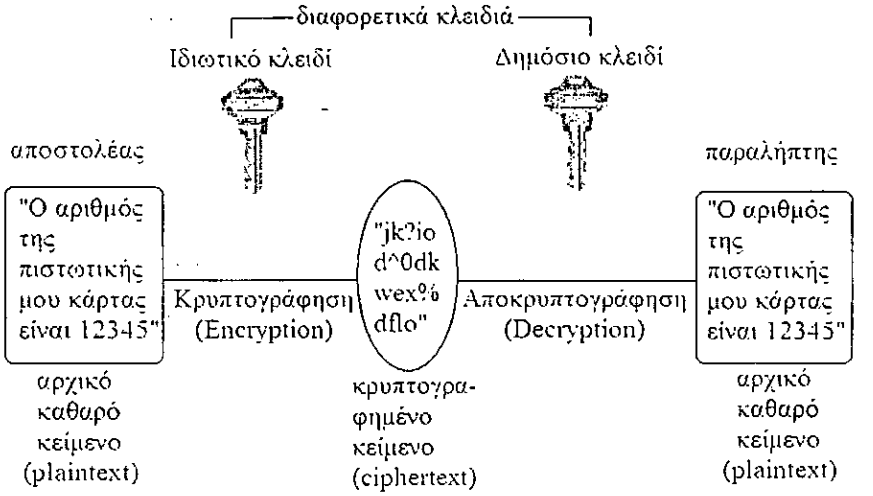
Με την μέθοδο της ασύμμετρης κρυπτογράφησης, χρησιμοποιούνται δυο κλειδιά για κρυπτογράφηση και αποκρυπτογράφηση τα οποία διαφέρουν μεταξύ τους. Το ένα από τα δυο είναι γνωστό μόνο στον κάτοχο του και ονομάζεται μυστικό ή ιδιωτικό και το άλλο κλειδί είναι διαθέσιμο σε οποιοδήποτε ενδιαφερόμενο και ονομάζεται δημόσιο (public). Στο διαδίκτυο υπάρχουν τόποι με λίστες δημόσιων κλειδιών – κάτι σαν τηλεφωνικοί κατάλογοι. Από εκεί βρίσκουμε δημόσια κλειδιά άλλων χρηστών ή προσθέτουμε τα δικά μας (http://www.keyserver.net). Σε κάθε σύστημα κρυπτογραφίας δημόσιου κλειδιού, για κάθε ιδιωτικό κλειδί υπάρχει ακριβώς ένα δημόσιο και οι πληροφορίες που κρυπτογραφούνται με χρήση του ενός κλειδιού αποκρυπτογραφούνται από το αντίστοιχο «ταίρι» και μόνο από αυτό. Επίσης, αυτό το κρυπτοσύστημα έχει το χαρακτηριστικό ότι δοθέντος του δημοσίου κλειδιού να μην είναι δυνατό να υπολογιστεί το ιδιωτικό κλειδί.

Θα πρέπει να αναφέρουμε ότι τα δυο αυτά κλειδιά μπορούν να χρησιμοποιηθούν με δυο διαφορετικούς τρόπους. Ο πρώτος τρόπος αποσκοπεί στο να εξασφαλιστεί η εμπιστευτικότητα του μηνύματος και ο δεύτερος τρόπος αποσκοπεί στο να αποδειχθεί η αυθεντικότητα του χρήστη. [16] – [22]

Πιο αναλυτικά, στην πρώτη περίπτωση για την παραγωγή ενός εμπιστευτικού μηνύματος, ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα, έτσι ώστε να παραμείνει απόρρητο έως ότου αποκρυπτογραφηθεί από το ιδιωτικό κλειδί του παραλήπτη. Αυτό αναπαρίσταται στο παρακάτω σχήμα.



Στην δεύτερη περίπτωση, ο αποστολέας κρυπτογραφεί ένα μήνυμα με το ιδιωτικό του κλειδί, το οποίο είναι απόρρητο. Το ιδιωτικό κλειδί αποδεικνύει την ταυτότητα του χρήστη (αυθεντικοποίηση). Και όπως θα δούμε σε επόμενο κεφάλαιο, η χρήση ιδιωτικού κλειδιού για την κρυπτογράφηση ενός μηνύματος αποτελεί τη βάση για το σχεδιασμό συστημάτων ψηφιακών υπογραφών. Έτσι λοιπόν οποιοσδήποτε χρησιμοποιήσει το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφήσει το μήνυμα θα είναι βέβαιος για την ταυτότητα του αποστολέα. Αυτό αναπαρίσταται στο παρακάτω σχήμα.



Πλεονεκτήματα της ασύμμετρης κρυπτογραφίας

Το μεγάλο πλεονέκτημα της μεθόδου της ασύμμετρης κρυπτογράφησης είναι ότι χρειάζεται να διανεμηθούν συνολικά λιγότερα κλειδιά ασφαλείας ανάμεσα στο σύνολο των χρηστών που πρέπει να μπορούν να επικοινωνήσουν. Αυτό οφείλεται στο ότι απαιτούνται μόνο δυο κλειδιά ανά χρήστη ενώ με τα ιδιωτικά κλειδιά ασφαλείας πρέπει να υπάρχει ένα μοναδικό ιδιωτικό κλειδί ανά ζεύγος χρηστών. Έτσι, για να υπάρχει δυνατότητα ασφαλούς επικοινωνίας ανάμεσα σε N χρήστες απαιτούνται $2 \times N$ κλειδιά στην περίπτωση της ασύμμετρης κρυπτογραφίας ενώ απαιτούνται N(N-1)/2 κλειδιά στην περίπτωση της συμμετρικής κρυπτογραφίας, κάτι που κάνει πολύ πιο αποτελεσματική την ασύμμετρη κρυπτογραφία από τον μικρό αριθμό των 5 μόλις χρηστών. Αυτό γίνεται πιο προφανές με το παρακάτω παράδειγμα. Ας θεωρήσουμε πως έχουμε 100 χρήστες. Τότε θα απαιτούνται 2*100=200 κλειδιά στην περίπτωση της ασύμμετρης κρυπτογραφίας ενώ στην συμμετρική θα απαιτούταν να διανεμηθούν $100*(100-1)/2 \cong 100*100/2 = 5.000$ διαφορετικά κλειδιά! [23]

Επιπροσθέτως, οι ψηφιακές υπογραφές που παρέχει η ασύμμετρη κρυπτογραφία δεν επιτρέπουν στην πηγή τους να αρνηθεί ότι έστειλε το μήνυμα που αυτές συνοδεύουν. Το χαρακτηριστικό αυτό όπως έχουμε προαναφέρει λέγεται μη αποποίηση της ευθύνης (Non – Repudiation). Η πιστοποίηση ταυτότητας όμως μέσω συμμετρικής κρυπτογραφίας 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 υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι το ιδιωτικό κλειδί είχε κατά κάποιον τρόπο αποκαλυφθεί.

Μειονεκτήματα της ασύμμετρης κρυπτογραφίας

Ένα μεγάλο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα. Κατά κανόνα, οι διαδικασίες συμμετρικής κρυπτογράφησης είναι σημαντικά ταχύτερες από την ασύμμετρη κρυπτογράφηση. Επίσης, ένα άλλο σημαντικό μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλειδιών από οργανισμούς πιστοποίησης (Certificate Authority) ώστε να διασφαλίζεται η κατοχή τους από νόμιμους χρήστες. Με αυτό εννοούμε ότι όταν κάποιος απατεώνας κατορθώσει να ξεγελάσει τον οργανισμό, μπορεί να προσποιείται την ταυτότητα ενός νόμιμου χρήστη.

Ο παρακάτω πίνακας που ακολουθεί περιέχει μια συνοπτική αναφορά των πλεονεκτημάτων και των μειονεκτημάτων της συμμετρικής και ασύμμετρης κρυπτογραφίας.

	Πλεονεκτήματα	**Μειονεκτήματα**
Συμμετρική κρυπτογραφία	- Ταχύτερη (λόγω του ότι αποκρυπτογραφείται πολύ γρήγορα μεγάλος αριθμός κρυπτογραφημένων κειμένων)	- Το ιδιωτικό κλειδί μπορεί να διαρρεύσει - Διανέμονται πάρα πολλά κλειδιά - Δεν παρέχεται αυθεντικότητα και μη αποποίηση της ευθύνης
Ασύμμετρη κρυπτογραφία	- Το ιδιωτικό κλειδί δεν 'ταξιδεύει' εκτεθειμένο μέσα στο Διαδίκτυο και μόνο ο χρήστης έχει την αποκλειστική γνώση του ιδιωτικού (του) κλειδιού - Διανέμονται λιγότερα κλειδιά - Εξασφαλίζεται εμπιστευτικότητα του μηνύματος και η αυθεντικότητα του αποστολέα - Υποστηρίζει τις Ψηφιακές Υπογραφές	- Δεν είναι γρήγορη και κάποιος απατεώνας μπορεί να προσποιηθεί έναν νόμιμο χρήστη στον οργανισμό πιστοποίησης

2.7 ΤΥΠΟΙ ΑΛΓΟΡΙΘΜΩΝ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Ένα κρυπτοσύστημα λειτουργεί είτε ως **block cipher** είτε ως **stream cipher**. Το block cipher, μετατρέπει ένα block μη κρυπτογραφημένου καθορισμένου μήκους κειμένου (plaintext), σε block κρυπτογραφημένου του ίδιου μήκους κειμένου (cipher text). Η αποκρυπτογράφηση γίνεται με την εφαρμογή του αντίστροφου μετασχηματισμού στο κρυπτογραφημένο κείμενο. Το καθορισμένο μήκος καλείται block size και συνήθως είναι μεγαλύτερο ή ίσο των 64 bits. Ένα block cipher αποτελεί ένα αξιόλογο και σημαντικό στοιχείο σε κρυπτογραφικά συστήματα. Ιδιαιτέρως, ένα block cipher σε κρυπτογραφικό σύστημα συμμετρικού κλειδιού παρέχει εμπιστευτικότητα και επιπλέον μπορεί να χρησιμεύσει σε τεχνικές αυθεντικοποίησης μηνυμάτων και πρωτοκόλλων, ακεραιότητα δεδομένων και σε ψηφιακές υπογραφές. Ένας block cipher με μικρού μήκους block size μπορεί να είναι τρωτός σε επιθέσεις που βασίζονται σε στατιστικές αναλύσεις και μιας τέτοιας μορφής επίθεση μπορεί να εμπεριέχει απλή ανάλυση συχνότητας κρυπτογραφημένων blocks.

Από την άλλη μεριά, το Stream cipher λειτουργεί με μια ακολουθία από bits μεταβλητού μήκους, παράγοντας cipher text του ιδίου μήκους. Στην πραγματικότητα, το stream cipher επεξεργάζεται τα δεδομένα σαν ακολουθίες χαρακτήρων, όπου κάθε χαρακτήρας μπορεί να θεωρηθεί ένα bit ή ένας μικρός αριθμός bits. Σε αντίθεση με τους block ciphers, οι stream ciphers είναι εξαιρετικά ταχύς αλγόριθμοι. [24] – [26]

2.8 ΒΑΣΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ ΙΔΙΩΤΙΚΟΥ ΚΛΕΙΔΙΟΥ

Οι αλγόριθμοι ιδιωτικού κλειδιού (private key) ή αλλιώς συμμετρικοί αλγόριθμοι ξεκίνησαν να χρησιμοποιούνται σε εμπορικές εφαρμογές από την δεκαετία του εβδομήντα. [27] – [37]

2.8.1 Ο αλγόριθμος DES (Data Encryption Standard)

Το πρώτο συμμετρικό κρυπτοσύστημα που χρησιμοποιήθηκε ευρέως ήταν το **Data Encryption Standard (DES)**, το οποίο καθιερώθηκε ως πρότυπο από τις Ηνωμένες Πολιτείες Αμερικής το 1977. Αρχικά, αναπτύχθηκε από την IBM με το κωδικό όνομα Lucifer και στόχευε να αποτελέσει τον αλγόριθμο που δεν θα μπορούσε να

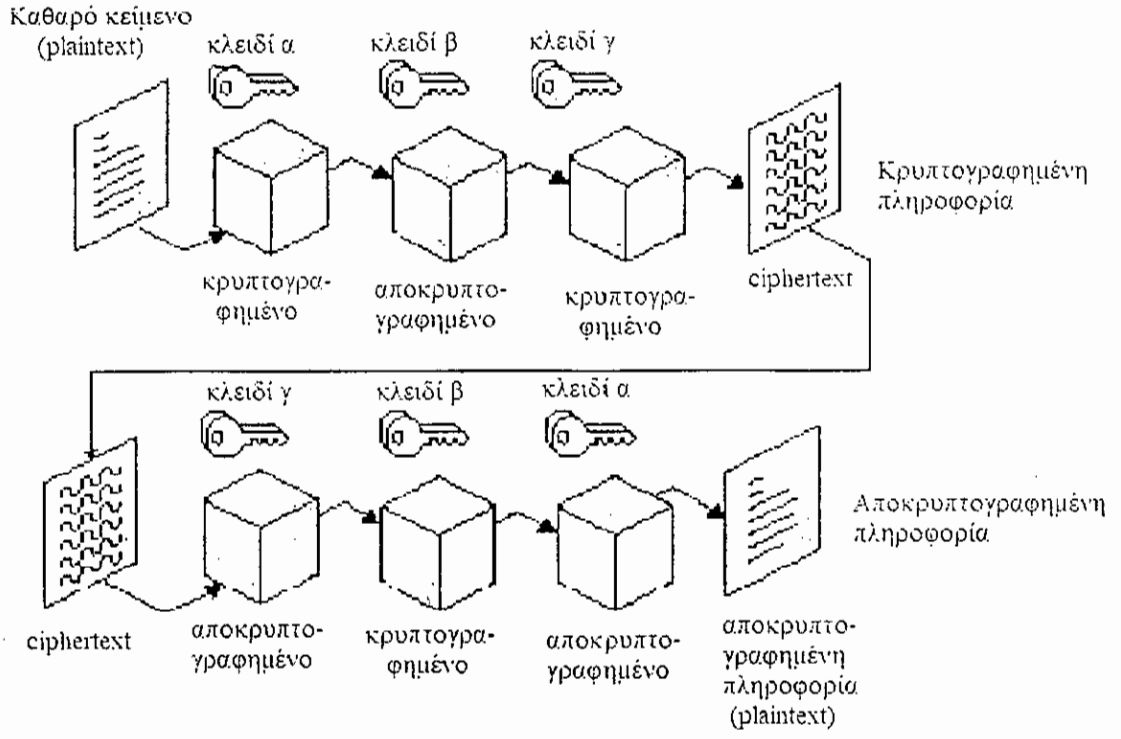
παραβιαστεί ούτε και από τις γρηγορότερες μηχανές εκείνης της εποχής. Τον αλγόριθμο αυτό υιοθέτησε και το ANSI (American National Standards Institute) ως πρότυπο για τη βιομηχανία, με την ονομασία DEA (Data Encryption Algorithm). Μετέπειτα, αντικαταστάθηκε από τον **AES (Advanced Encryption Standard)**.

Ο αλγόριθμος DES λειτουργεί ως block cipher σε blocks δεδομένων των 64 bits και χρησιμοποιεί κλειδί των 56 bits. Γενικά ο DES θεωρείται καλό κρυπτοσύστημα διότι δεν έχει βρεθεί άλλη μέθοδος παραβίασης του, πέραν της εξαντλητικής αναζήτησης του κλειδιού, η οποία μέχρι πρόσφατα δεν θεωρούνταν εφικτή λόγω των υπολογιστικών πόρων που απαιτούσε. Παρόλα αυτά η τεχνολογία έχει προχωρήσει αρκετά, σε σημείο που να είναι αμφισβητήσιμη η ασφάλεια που παρέχει ένα οποιοδήποτε block cipher με κλειδί μήκους 56 bits. Για το λόγο αυτό έχουν αναπτυχθεί εναλλακτικές λύσεις για την αντικατάσταση του DES και την προστασία του ηλεκτρονικού εμπορίου.

Το NIST (National Institute of Standards and Technology – Εθνικό Ινστιτούτο Προτύπων και Τεχνολογιών) δημιούργησε τον αλγόριθμο **AES (Advanced Encryption Standard)** και αναπτύχθηκε προκειμένου να αντικαταστήσει τον αλγόριθμο DES (Data Encryption Standard). Ο αλγόριθμος AES είναι σχεδιασμένος έτσι ώστε να παρέχει περισσότερη ασφάλεια από τον DES. Δίνοντας μια περιγραφή του AES θα μπορούσαμε να αναφέρουμε ότι κρυπτογραφεί και αποκρυπτογραφεί 128 bits πακέτα μηνυμάτων κι επίσης υποστηρίζει μεγαλύτερο μέγεθος κλειδιού. Το μέγεθος του κλειδιού αυτού του αλγορίθμου μπορεί να είναι 128, 192 ή και 256, ανάλογα των απαιτήσεων κατά την κρυπτογράφηση.

Ο αλγόριθμος Triple-DES (3-DES) χρησιμοποιείται ως μια παραλλαγή του DES, έτσι ώστε η αποτελεσματικότητα του DES να είναι σημαντικά βελτιωμένη χρησιμοποιώντας τεχνικές πολλαπλής κρυπτογράφησης, κρυπτογραφώντας τον DES τρεις φορές με διαφορετικά κλειδιά. Δηλαδή το αρχικό μήνυμα, σε blocks των 64 bits, κρυπτογραφείται χρησιμοποιώντας ένα κλειδί α, στη συνέχεια αποκρυπτογραφείται χρησιμοποιώντας ένα κλειδί β και το αποτέλεσμα κρυπτογραφείται χρησιμοποιώντας ένα κλειδί γ. Το αποτέλεσμα που προκύπτει είναι πολλές τάξεις μεγέθους ισχυρότερο του DES. Επίσης, κι ο Triple-DES έχει αντικατασταθεί από τον AES (Advanced Encryption Standard).

Στο παρακάτω σχήμα που ακολουθεί αναπαρίσταται ο αλγόριθμος Triple – DES



2.8.2 Ο αλγόριθμος IDEA (International Data Encryption Algorithm)

Ο αλγόριθμος IDEA αναπτύχθηκε στη Ζυρίχη της Ελβετίας, από τον James L. Massey και Xuejia Lai. Ο αλγόριθμος IDEA δημοσιεύτηκε το 1991, είναι ένας εμπορικός αλγόριθμος και χρησιμοποιείται σε εμπορικά προϊόντα. Ο αλγόριθμος κρυπτογράφησης συμμετρικού κλειδιού IDEA λειτουργεί σε block πακέτου των 64 bits και το μήκος του κλειδιού του είναι 128 bits συγκριτικά μεγαλύτερο από του DES.

2.8.3 Ο αλγόριθμος RC2

Όπως και με τους άλλους συμμετρικούς αλγόριθμους DES κι IDEA που αναφέραμε προηγουμένως έτσι και ο αλγόριθμος RC2, είναι block αλγόριθμος, ο οποίος σχεδιάστηκε και αναπτύχθηκε από τον Ronald Rivest και τα αρχικά RC σημαίνουν "Rod's Code" ή "Rivest's Cipher". Ο αλγόριθμος RC2 λειτουργεί σε πακέτο των 64 bits. Μια βασική διαφορά που έχει ο αλγόριθμος RC2 είναι ότι στο λογισμικό (software) είναι δύο με τρεις φορές γρηγορότερος από τον DES. Ο αλγόριθμος RC2 βρίσκεται στην ιδιοκτησία της RSA Data Security.

2.8.4 Ο αλγόριθμος RC4

Ο αλγόριθμος RC4 είναι stream αλγόριθμος, έχει κλειδί μεταβλητού μεγέθους. Δεν θεωρείται πλέον ασφαλής γιατί έχει παραβιαστεί.

2.8.5 Ο αλγόριθμος RC5

Ο αλγόριθμος RC5 είναι κι αυτός ένας block αλγόριθμος, ο οποίος λειτουργεί σε blocks των 32, 64 ή και 128 bits κι επιτρέπει στον χρήστη να ορίζει το μέγεθος του block δεδομένων, το μήκος του κλειδιού καθώς επίσης και το πόσες φορές να γίνει η κρυπτογράφηση. Το κλειδί είναι μεταβλητού μεγέθους (0 – 2048 bits) και θεωρείται αρκετά αποτελεσματικός και ασφαλής αλγόριθμος. Επίσης είναι κατάλληλος τόσο για το λογισμικό όσο και για το υλικό.

2.8.6 Ο αλγόριθμος SKIPJACK

Είναι ένα κρυπτοσύστημα που προτάθηκε από το υπουργείο Άμυνας των Η.Π.Α. και που παρέχει τη δυνατότητα των οργάνων του νόμου να αποκρυπτογραφούν το μήνυμα όταν πρέπει. Το SKIPJACK είναι ένα 64 bits block cipher το οποίο χρησιμοποιεί ένα κλειδί μήκους 80 bits. Παρόλα αυτά επειδή τα τεχνικά χαρακτηριστικά του είναι απόρρητα δεν είναι πιθανό να χρησιμοποιηθεί για εμπορικούς σκοπούς.

2.9 ΒΑΣΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Ορισμένοι σημαντικοί αλγόριθμοι δημόσιου κλειδιού που χρησιμοποιούνται για την κρυπτογράφηση προσωπικών δεδομένων είναι οι παρακάτω:

2.9.1 Ο αλγόριθμος RSA

Ο αλγόριθμος RSA χρησιμοποιείται τόσο για την κρυπτογράφηση δεδομένων, όσο και για την εξασφάλιση της αυθεντικότητας του αποστολέα. Ονομάστηκε έτσι από τα αρχικά των καθηγητών του MIT που τον επινόησαν, οι οποίοι ήταν ο Ron Rivest, ο Adi Shamir και ο Len Adleman, το 1978.

Ο RSA μπορεί να χρησιμοποιηθεί για να κρυπτογραφεί πληροφορίες αλλά και σαν βάση του συστήματος ψηφιακών υπογραφών. Οι ψηφιακές υπογραφές μπορούν να

χρησιμοποιηθούν για να αποδείξουν την πατρότητα και τη γνησιότητα της πληροφορίας. Για τις ψηφιακές υπογραφές θα αναφερθούμε πιο αναλυτικά παρακάτω. Για ικανοποιητική προστασία το μήκος του κλειδιού μπορεί να είναι 1024 bits και θεωρείται υπεραρκετό για τις περισσότερες εμπορικές εφαρμογές. Όμως όταν χρειάζεται ακόμα περισσότερη ασφάλεια χρησιμοποιείται μήκος κλειδιού 2048 bits.

2.9.2 Ο αλγόριθμος DSS (Digital Signature Standard)

Αναπτύχθηκε από την National Security Agency (NSA) και εφαρμόστηκε σαν ομοσπονδιακό πρότυπο επεξεργασίας πληροφοριών FIPS (Federal Information Processing Standard) από την NIST (National Institute for Standards and Technology). Ο DSS είναι βασισμένος στον αλγόριθμο ψηφιακών υπογράφων (DSA). Αν και ο DSA επιτρέπει κλειδιά οποιουδήποτε μήκους, μόνο κλειδιά ανάμεσα σε 512 και 1024 bits επιτρέπονται στον DSS. Όπως αναφέρθηκε, ο DSS μπορεί να χρησιμοποιηθεί μόνο για ψηφιακές υπογραφές, αν και είναι πιθανό να χρησιμοποιήσει DSA εφαρμογές για την κρυπτογράφηση επίσης.

2.10 ΕΠΙΘΕΣΕΙΣ ΣΤΟΥΣ ΑΛΓΟΡΙΘΜΟΥΣ ΙΔΙΩΤΙΚΟΥ ΚΛΕΙΔΙΟΥ

Όταν χρησιμοποιούμε την κρυπτογραφία για να προστατεύσουμε πληροφορίες, τότε θα πρέπει να δεχτούμε ότι οι άνθρωποι από τους οποίους προσπαθούμε να κρύψουμε την πληροφορία ενδέχεται να ανακαλύψουν τις παραμέτρους του κρυπτοσυστήματος. Για να είναι χρήσιμο ένα κρυπτογραφικό σύστημα θα πρέπει να αντιστέκεται σε επιθέσεις.

Οι επιθέσεις που λαμβάνουν χώρα στις κρυπτογραφημένες πληροφορίες χωρίζονται σε τρεις κατηγορίες. Αυτές είναι οι παρακάτω: [38] – [40]

2.10.1 Επιθέσεις αναζήτησης κλειδιού (Key Search Attack)

Ο ευκολότερος τρόπος να 'σπάσει' κανείς έναν κώδικα είναι να δοκιμάσει όλα τα πιθανά κλειδιά το ένα μετά το άλλο προσπαθώντας να βρει το σωστό κλειδί. Οι περισσότερες προσπάθειες θα αποτύχουν, αλλά κάποια μπορεί να επιτύχει. Οι συνέπειες μπορεί να είναι να καταφέρει ένας "cracker" να μπει στο σύστημα ή να

αποκρυπτογραφήσει κάποια εμπιστευτική επικοινωνία. Δυστυχώς δεν υπάρχει τρόπος να προβάλλουμε άμυνα εναντίον αυτού του τρόπου επίθεσης, γιατί δεν μπορούμε να εμποδίσουμε τον επιτιθέμενο να προσπαθήσει να αποκρυπτογραφήσει το κρυπτογραφημένο μήνυμα μας με κάθε πιθανό κλειδί.

Ευτυχώς, οι αναζητήσεις κλειδιών δεν είναι πολύ αποτελεσματικές. Στην πλειοψηφία των περιπτώσεων δεν υπάρχει πρακτικά καμία πιθανότητα να ανακαλυφθεί το κλειδί με απλή δοκιμή κλειδιών γιατί υπάρχουν υπερβολικά πολλά κλειδιά για να δοκιμαστούν σε ένα λογικό χρονικό διάστημα από ένα σύστημα με λογική, ή και μεγάλη, υπολογιστική ισχύ. Για παράδειγμα, αν ένα κλειδί έχει μήκος 128 bits τότε έχει μεγάλη ανθεκτικότητα σε μια τέτοια επίθεση. Αυτό ισχύει γιατί ένα τέτοιο κλειδί επιτρέπει 2^{128} ($3.4*10^{38}$) πιθανά κλειδιά. Εάν υπήρχε ένας υπολογιστής που θα μπορούσε να δοκιμάσει ένα δισεκατομμύριο κλειδιά το δευτερόλεπτο, και είχαμε ένα δισεκατομμύριο από αυτούς τους υπολογιστές, αυτοί θα χρειάζονταν για να δοκιμάσουν κάθε πιθανό 128 bits κλειδί 10^{13} χρόνια, δηλαδή δέκα χιλιάδες δισεκατομμύρια χρόνια!. Αυτός ο χρόνος είναι κατά προσέγγιση χιλιάδες φορές μεγαλύτερος από την ηλικία του σύμπαντος, που εκτιμήθηκε πρόσφατα σαν 18 δισεκατομμύρια χρόνια. Προφανώς, δεν θα είναι ποτέ λογική μια επίθεση απλή διαδοχικής δοκιμής κλειδιών σε ένα μήνυμα κρυπτογραφημένο με κλειδί μήκους 128 bit και τα δεδομένα που θα προστατεύονται από μια τέτοια κρυπτογράφηση θα μπορούν να θεωρούνται απόλυτα προστατευμένα απέναντι σε επιθέσεις αυτού του τύπου.

2.10.2 Επιθέσεις κρυπτανάλυσης (Cryptanalysis)

Εάν το μήκος του κλειδιού ήταν ο μόνος παράγοντας που καθόριζε την ασφάλεια ενός κρυπτογραφήματος τότε ο καθένας που θα ενδιαφερόταν να ανταλλάζει μυστικά μηνύματα απλά θα χρησιμοποιούσε κώδικες με 128-bit κλειδιά και κάθε επικοινωνία δεδομένων θα ήταν απόλυτα ασφαλής λόγω του αστρονομικού αριθμού πιθανών κλειδιών που θα έπρεπε να δοκιμαστούν από τις επιθέσεις αναζήτησης κλειδιού. Δυστυχώς τα πράγματα δεν έχουν ακριβώς έτσι. Αυτό που κρατά στην επικαιρότητα την κρυπτογραφία είναι το γεγονός ότι οι κρυπτογραφικοί αλγόριθμοι δεν ανταποκρίνονται πάντα στις προσδοκίες μας. Οι επιθέσεις αναζήτησης κλειδιού σπάνια χρειάζονται να γνωρίζουν τα περιεχόμενα ενός κρυπτογραφημένου μηνύματος. Σε αντίθεση, οι περισσότεροι κρυπτογραφικοί αλγόριθμοι μπορούν να

νικηθούν χρησιμοποιώντας συνδυασμούς από βελτιωμένα μαθηματικά και υπολογιστική ισχύ. Το αποτέλεσμα είναι ότι πολλά κρυπτογραφημένα μηνύματα αποκρυπτογραφούνται χωρίς να γνωρίζουμε το κλειδί. Μάλιστα, ένας επιδέξιος κρυπταναλυτής (cryptanalyst) μπορεί μερικές φορές να αποκρυπτογραφήσει κάποιο κείμενο χωρίς ούτε καν να γνωρίζει τον κρυπτογραφικό αλγόριθμο!

2.10.3 Επιθέσεις βασισμένες στο σύστημα κρυπτογράφησης (System-based Attacks)

Ένας άλλος τρόπος για να 'σπάσουμε' ένα κρυπτογραφικό σύστημα είναι να επιτεθούμε στο κρυπτογραφικό σύστημα που χρησιμοποιεί έναν αλγόριθμο, εκμεταλλευόμενοι τα κενά που ενδεχομένως να υπάρχουν στην υλοποίησή του, χωρίς ουσιαστικά να επιτεθούμε στο κρυπτογραφικό αλγόριθμο κάθε αυτό.

Ένα καλό παράδειγμα τέτοιας επίθεσης είναι ο VC-I Video, κρυπτογραφικός αλγόριθμος που χρησιμοποιούταν παλαιότερα για την δορυφορική μετάδοση προγράμματος τηλεόρασης. Για πολλά χρόνια υπήρχαν πειρατές που πουλούσαν αποκωδικοποιητές που μπορούσαν να υποκλέψουν τα κλειδιά μεταφοράς και ύστερα να τα χρησιμοποιήσουν για να αποκρυπτογραφήσουν την μετάδοση. Ο VC-I κρυπτογραφικός αλγόριθμος ήταν ασφαλής, αλλά το σύστημα σαν σύνολο ήταν αδύνατο.

2.11 ΕΠΙΘΕΣΕΙΣ ΣΤΟΥΣ ΑΛΓΟΡΙΘΜΟΥΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Οι αλγόριθμοι δημοσίου κλειδιού είναι θεωρητικά πιο ευάλωτοι στις επιθέσεις από τους αλγόριθμους συμμετρικού κλειδιού γιατί ο επιτιθέμενος μπορεί να έχει ένα αντίγραφο του δημόσιου κλειδιού που χρησιμοποιήθηκε για την κρυπτογράφηση του μηνύματος. Η δουλειά του επιτιθέμενου είναι ακόμα ευκολότερη γιατί το ίδιο το μήνυμα πιθανώς να υποδηλώνει με ποιόν αλγόριθμο έχει κρυπτογραφηθεί. Οι επιθέσεις στους αλγόριθμους δημόσιου κλειδιού χωρίζονται σε δυο κατηγορίες και είναι οι παρακάτω: [41] – [43]

2.11.1 Επιθέσεις παραγοντοποίησης (Factoring attacks)

Αυτού του είδους οι επιθέσεις είναι πολύ δημοφιλής στα συστήματα δημόσιου κλειδιού γιατί είναι πολύ εύκολες να κατανοηθούν. Αυτή η επίθεση αποσκοπεί να αντλήσει το προσωπικό κλειδί από το αντίστοιχο δημόσιο κλειδί.

2.11.2 Επίθεση αλγοριθμική

Ένας άλλος τρόπος επίθεσης είναι να βρούμε ένα βασικό ελάττωμα ή αδυναμία του μαθηματικού προβλήματος στο οποίο είναι βασισμένο το σύστημα κρυπτογράφησης. Αυτό έχει γίνει περισσότερες από μια φορές στο παρελθόν. Το πρώτο κρυπτογραφικό σύστημα που εφαρμόστηκε ήταν βασισμένο σε ένα μαθηματικό πρόβλημα που ονομαζόταν Superincreasing Knapsack Problem. Μερικά χρόνια μετά βρέθηκε ένας μαθηματικός τρόπος για να αποκτάται το μυστικό κλειδί από το δημόσιο μέσα σε πολύ λίγο χρόνο.

2.12 ΘΩΡΑΚΙΣΗ ΤΩΝ ΑΛΓΟΡΙΘΜΩΝ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Ο μόνος πραγματικός τρόπος για να καθορίσουμε εάν ένας κρυπτογραφικός αλγόριθμος είναι δυνατός είναι να τον δημοσιεύσουμε και να περιμένουμε από κάποιον να βρει μια αδυναμία του. Αυτή η διαδικασία εξέτασης λαθών δεν είναι τέλεια αλλά είναι καλύτερη από το να μην πράξουμε τίποτα. Δεν πρέπει να εμπιστευόμαστε ανθρώπους που λένε ότι έχουν αναπτύξει έναν νέο αλγόριθμο κρυπτογράφησης, αλλά δεν μας λένε με ποιον ακριβώς τρόπο δουλεύει για το λόγο του ότι θα εκτεθεί η δύναμη του αλγόριθμου. Εάν ο αλγόριθμος χρησιμοποιείται για να αποθηκεύσει πληροφορίες που είναι πολύτιμες, τότε ένας επιτιθέμενος θα αγοράσει ή θα κλέψει ένα αντίγραφο του προγράμματος που εφαρμόζει τον αλγόριθμο και θα αποσυνθέσει το πρόγραμμα βλέποντας έτσι με ποιον τρόπο δουλεύει. Η αληθινή κρυπτογραφική ασφάλεια εξαρτάται από την ειλικρίνεια και από την ερευνητική εξέταση.

ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ

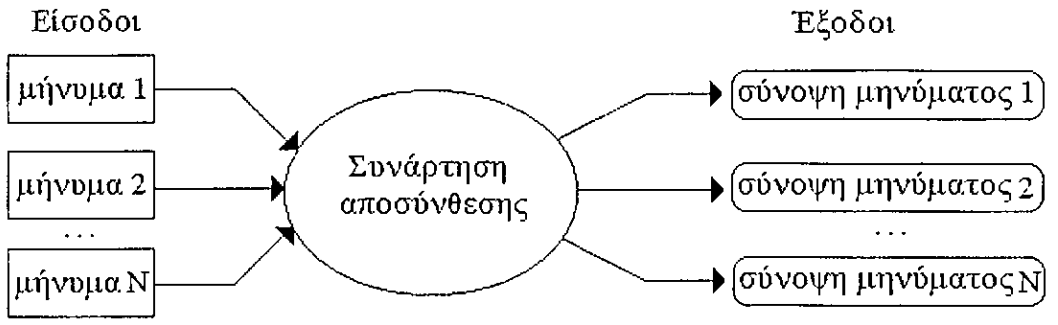
ΑΠΟΣΥΝΘΕΣΗ ΜΗΝΥΜΑΤΩΝ

Στο τρίτο κεφάλαιο αναφερόμαστε σε μια σημαντική έννοια στην αποσύνθεση μηνυμάτων. Μια αποσύνθεση μηνύματος όπως θα παρατηρήσει και ο αναγνώστης από τον ορισμό αυτής της έννοιας είναι το συνοπτικό περιεχόμενο ενός μηνύματος, το οποίο χρησιμεύει για τον έλεγχο ακεραιότητας των μηνυμάτων και αρχείων, για έλεγχο αυθεντικότητας των χρηστών και για δημιουργία ψηφιακών υπογραφών. Επιπλέον, στο παρόν κεφάλαιο κατηγοριοποιούμε την αποσύνθεση μηνυμάτων και αναφερόμαστε σε διάφορες χρησιμοποιούμενες συναρτήσεις αποσύνθεσης μηνυμάτων.

3.0 ΑΠΟΣΥΝΘΕΣΗ ΜΗΝΥΜΑΤΩΝ

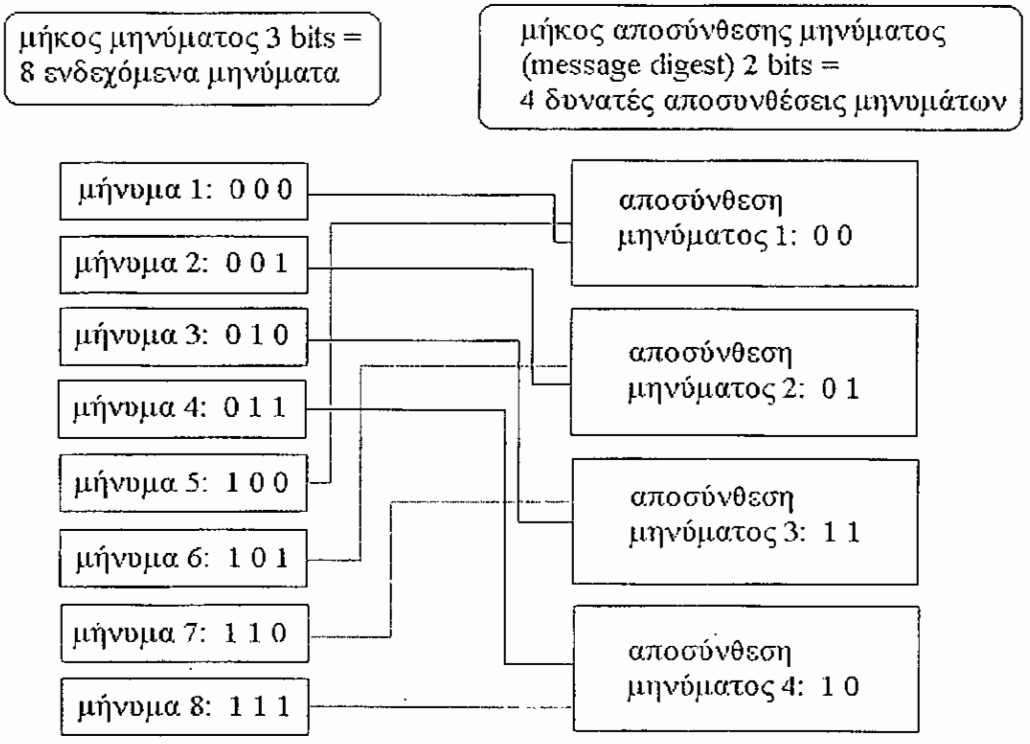
Μια αποσύνθεση μηνύματος (message digest ή hash function), που λέγεται και 'κώδικας ανακατέματος' (hash – code), δεν είναι τίποτα περισσότερο από έναν αριθμό, έναν ειδικό αριθμό που προκύπτει όταν βάλουμε ως είσοδο ένα μήνυμα σε μια συνάρτηση αποσύνθεσης μηνυμάτων (message digest function ή hash function). Η αποσύνθεση μηνύματος που προκύπτει σε κάθε περίπτωση πρέπει να είναι μοναδική (unique), δηλαδή από κάθε διαφορετικό μήνυμα να προκύπτει μια διαφορετική αποσύνθεση μηνύματος και κάθε αποσύνθεση μηνύματος μπορεί να προκύψει από ένα και μόνο συγκεκριμένο μήνυμα. [44] – [46]

Το σχήμα που ακολουθεί είναι μια συνοπτική περιγραφή των όσων αναφέρονται παραπάνω.



Στην πραγματικότητα δεν είναι δυνατόν αυτό να γίνει επειδή το μήκος της αποσύνθεσης ενός μηνύματος είναι γενικά μικρότερο του αρχικού μηνύματος. Έτσι, υπάρχουν περισσότερα ενδεχόμενα μηνύματα από ότι δυνατές αποσυνθέσεις μηνυμάτων οπότε δεν είναι δυνατόν να προκύψει από κάθε μήνυμα μια διαφορετική αποσύνθεση αλλά κάποια θα έχουν την ίδια. Για παράδειγμα, ας υποθέσουμε ότι το μήκος ενός μηνύματος είναι 3 bits (δηλαδή ισοδυναμεί με $2^3 = 8$ ενδεχόμενα μηνύματα) και η αποσύνθεση μηνυμάτων (message digest) που προκύπτει από τη συνάρτηση αποσύνθεσης (hash function) είναι 2 bits (δηλαδή ισοδυναμεί με $2^2 = 4$ δυνατές αποσυνθέσεις μηνυμάτων), τότε κάποια μηνύματα θα έχουν την ίδια αποσύνθεση μηνυμάτων.

Το παράδειγμα που αναφέραμε μπορεί να απεικονισθεί με το παρακάτω σχήμα.



Η αποσύνθεση ενός μηνύματος έχει συνήθως 128 με 256 bits μήκος.

Μια καλή συνάρτηση αποσύνθεσης μηνύματος πρέπει να συνδυάζει μερικές ιδιότητες:

- Έχοντας ένα αρχείο εισόδου και την ανάλογη συνάρτηση αποσύνθεσης του, θα πρέπει να είναι αδύνατο να βρεθεί κάποιο άλλο αρχείο που θα έχει τον ίδιο αριθμό αποσύνθεσης, ή τουλάχιστον αυτό να μην είναι υπολογιστικά εφικτό. Όταν έχουμε δυο μηνύματα με την ίδια αποσύνθεση μηνύματος τότε λέμε πως έχουμε μια **σύγκρουση (collision)** και η ιδιότητα που περιγράψαμε προηγουμένως λέγεται **αντοχή στις συγκρούσεις (collision resistance)**.
- Θα πρέπει να είναι θεωρητικά, ή έστω πρακτικά, αδύνατον να βρεθεί από μια αποσύνθεση μηνύματος το αρχικό μήνυμα. Άρα ο αλγόριθμος που χρησιμοποιείται για την αποσύνθεση μηνύματος να είναι **μονόδρομος (one way).**

Η πρώτη ιδιότητα πρέπει να ισχύει για να μην είναι δυνατόν να βρεθεί κάποιο μήνυμα που να έχει τον ίδια αποσύνθεση μηνύματος με κάποιο άλλο καθώς τότε ακυρώνεται η προστασία που μας παρέχει η λειτουργία της αποσύνθεσης μηνύματος. Για

παράδειγμα, ας υποθέσουμε πως γνωρίζουμε το username ενός χρήστη (δεν είναι απαραίτητα κρυφά και σε κάθε περίπτωση αποθηκεύονται στους υπολογιστές με τους οποίους γίνονται οι συνδέσεις) και την αποσύνθεση μηνύματος του password του. Τότε, ακόμα και αν ο αλγόριθμος αποσύνθεσης μηνύματος που χρησιμοποιήθηκε είναι μονόδρομος και δε μπορούμε να βρούμε το password του, θα μπορέσουμε να ανακαλύψουμε κάποιο άλλο password που θα έχει την ίδια αποσύνθεση μηνύματος και έτσι, εισάγοντας το username του και το άλλο password, θα μπορέσουμε να εισέλθουμε στο σύστημα αντί για αυτόν.

Η δεύτερη ιδιότητα έχει αναφερθεί και παραπάνω και συνδέεται με την ανάγκη να είναι κάθε περίπτωση αποσύνθεσης μηνύματος εντελώς διαφορετική από κάθε άλλη, ακόμα και αν τα αρχικά μηνύματα είναι πάρα πολύ όμοια. Αυτό μειώνει την πιθανότητα όταν κάποιος γνωρίζει περίπου το αρχικό μήνυμα να μπορέσει να ελέγξει πρώτα τις αποσυνθέσεις των παραπλήσιων μηνυμάτων και να περιορίσει έτσι σε πάρα πολύ μεγάλο βαθμό τον αριθμό των δοκιμών που θα κάνει μέχρι να βρει το μήνυμα που θα έχει την κατάλληλη αποσύνθεση.

Οι χρήσεις των αλγορίθμων αποσύνθεσης μηνυμάτων μπορεί να είναι οι παρακάτω:

- Έλεγχος ακεραιότητας μηνυμάτων και αρχείων
- Έλεγχος αυθεντικότητας των χρηστών
- Δημιουργία ψηφιακών υπογραφών

Όπως αναφέραμε παραπάνω, η αποσύνθεση μηνύματος χρησιμεύει για τον έλεγχο ακεραιότητας των μηνυμάτων. Ο τρόπος με τον οποίο γίνεται αυτό είναι ο εξής: όταν θέλουμε να στείλουμε ένα μήνυμα του οποίου να μπορεί να ελέγξει ο δέκτης την ακεραιότητα τότε από το μήνυμα χρησιμοποιώντας μια συνάρτηση αποσύνθεσης μηνύματος παίρνουμε την αποσύνθεσή του. Αυτή είναι όπως είπαμε μοναδική και αυτό το μήνυμα μπορεί να συνοδευτεί από τη συγκεκριμένη αποσύνθεσή του και μόνο. Στη συνέχεια στέλνουμε το μήνυμα μαζί με την αποσύνθεσή του στον παραλήπτη. Αυτός τότε παίρνει το μήνυμα και με χρήση της ίδιας συνάρτησης αποσύνθεσης μηνύματος εξάγει την αποσύνθεση του ληφθέντος μηνύματος. Αν αυτή είναι ίδια με αυτή που συνόδεψε το μήνυμα τότε ο δέκτης είναι βέβαιος πως το μήνυμα δεν έχει αλλοιωθεί στην πορεία. Με παρόμοιο τρόπο μπορεί να γίνει και ο

έλεγχος ακεραιότητας των αρχείων: όταν αποθηκεύεται ένα αρχείο υπολογίζεται η αποσύνθεση μηνύματος του και αποθηκεύεται μαζί του ή σε κάποιο άλλο σημείο για λόγους ασφάλειας. Όταν θελήσουμε να το ανακτήσουμε υπολογίζουμε το μήνυμα αποσύνθεσής του και το συγκρίνουμε με την αποθηκευμένη τιμή του. Αν τα δυο τους ταυτίζονται τότε το αρχείο είναι διατηρημένο σωστά αλλιώς έχει αλλοιωθεί.

Ο έλεγχος αυθεντικότητας μπορεί να πραγματοποιηθεί από το login. Το login χρηστών σε ένα υπολογιστικό σύστημα όπως ξέρουμε γίνεται εισάγοντας ένα username ή login κείμενο που είναι φανερό και γνωστό στον διαχειριστή του συστήματος και ένα password που πρέπει να το γνωρίζει μόνο ο χρήστης. Βασική απαίτηση είναι ο κεντρικός υπολογιστής στον οποίο συνδέεται ο χρήστης να μπορεί να επαληθεύσει το σωστό συνδυασμό των username και password χωρίς να έχει αποθηκευμένο το password του χρήστη ώστε να είναι απολύτως αδύνατο ακόμα και στο διαχειριστή του συστήματος να το βρει! Πως θα ελεγχθεί τότε η ορθότητα του login; Αυτό γίνεται με το να αποθηκεύεται μια σύνοψη μηνύματος του password στον κεντρικό υπολογιστή αντί για το ίδιο το password. Έτσι, κάθε φορά το username χρησιμεύει ως δείκτης για το που έχει γίνει η καταχώρηση και εκεί συγκρίνεται η τιμή της αποσύνθεσης μηνύματος του password που εισήχθη με την αποθηκευμένη. Το να βρει κάποιος την αποθηκευμένη αποσύνθεση μηνύματος του password δεν έχει νόημα αφού αν την εισάγει κατά τη διαδικασία του login φυσικά δε θα γίνει δεκτός από το σύστημα.

Τέλος έχουμε τη δημιουργία ψηφιακών υπογραφών που είναι και η σημαντικότερη εφαρμογή των αποσυνθέσεων μηνυμάτων. Λόγω της ιδιαίτερης σημασίας αυτής της εφαρμογής ασχολούμαστε μαζί της αναλυτικά στο επόμενο κεφάλαιο.

3.1 ΚΑΤΗΓΟΡΙΕΣ ΣΥΝΑΡΤΗΣΕΩΝ ΑΠΟΣΥΝΘΕΣΗΣ ΜΗΝΥΜΑΤΩΝ

α) Ανάλογα με τη χρήση κλειδιού:

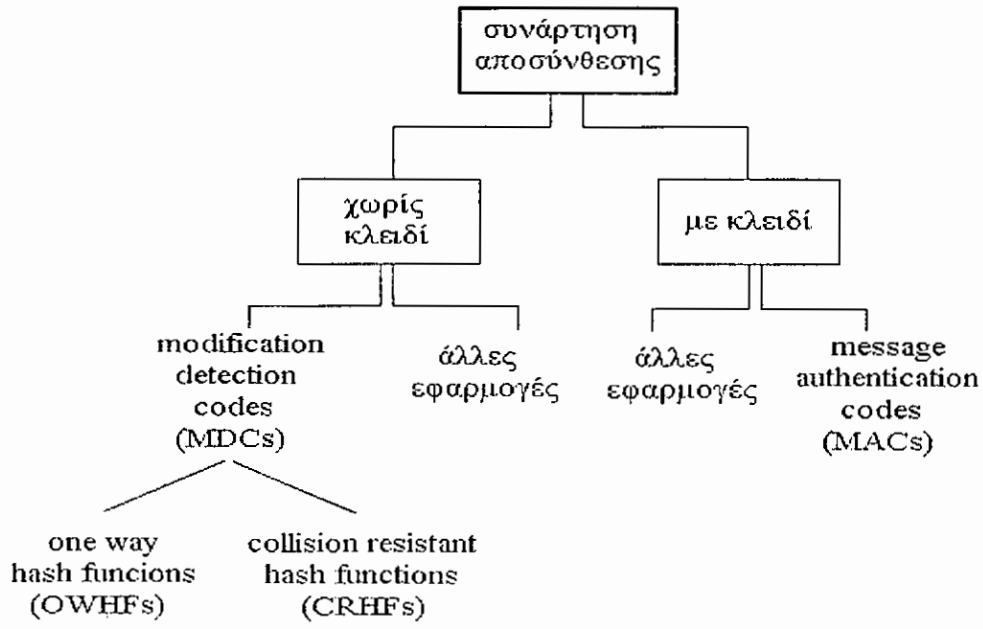
1) Χωρίς κλειδί: Είναι οι κλασσικές συναρτήσεις αποσύνθεσης μηνυμάτων. Ως είσοδό τους έχουν το μήνυμα του οποίου θέλουμε να βρούμε μια αποσύνθεση μηνύματος.

2) **Με κλειδί (keyed hash functions):** Είναι συναρτήσεις αποσύνθεσης μηνυμάτων που έχουν δυο εισόδους – το μήνυμα και ένα μυστικό κλειδί.

β) Ανάλογα με τη λειτουργικότητά τους:

1) **Κώδικες ανίχνευσης τροποποιήσεων (modification detection codes - MDCs):** Ο σκοπός τους είναι να δίνουν μια αντιπροσωπευτική και μοναδική εικόνα του μηνύματος ώστε να χρησιμοποιηθεί στη συνέχεια από επόμενες λειτουργίες που θα εγγυηθούν τον έλεγχο ακεραιότητας του μηνύματος. Η κατηγορία αυτή υποδιαιρείται σε δυο υποκατηγορίες:
   i) **Μονόδρομές συναρτήσεις αποσύνθεσης μηνυμάτων (one way hash functions – OWFs):** Είναι αυτές που είναι δύσκολο με γνωστή μια αποσύνθεση μηνύματος να βρεθεί το αρχικό μήνυμα.
   ii) **Ανθεκτικές στη σύγκρουση συναρτήσεις αποσύνθεσης μηνυμάτων (collision resistant hash functions – CRHFs):** Σε αυτές είναι δύσκολο να προκύψουν από δυο διαφορετικά μηνύματα οι ίδιες αποσυνθέσεις.
2) **Κώδικες αυθεντικοποίησης μηνυμάτων (message authentication codes – MACs):** Είναι οι συναρτήσεις που ως σκοπό τους έχουν την διασφάλιση τόσο της ακεραιότητας των δεδομένων όσο και της αυθεντικοποίησης της πηγής του μηνύματος. Γενικά είναι συναρτήσεις με κλειδί.

Στο παρακάτω σχήμα βλέπουμε τις κατηγορίες συναρτήσεων αποσύνθεσης μηνυμάτων όπως τις περιγράψαμε παραπάνω.



3.2 ΣΥΝΑΡΤΗΣΕΙΣ ΑΠΟΣΥΝΘΕΣΗΣ ΜΗΝΥΜΑΤΩΝ

Πολλές συναρτήσεις αποσύνθεσης μηνυμάτων έχουν σχεδιαστεί και χρησιμοποιούνται σήμερα. Μερικές από αυτές είναι οι εξής: [47]

3.2.1 HMAC (Hashed Message Authentication Code)

Είναι μια τεχνική που χρησιμοποιεί ένα προσωπικό κλειδί και μια συνάρτηση αποσύνθεσης για να δημιουργήσει ένα μυστικό κώδικα επικύρωσης μηνύματος. Είναι πιο ανθεκτικό ακόμα και αν η συνάρτηση αποσύνθεσης είναι αδύνατη.

3.2.2 MD2, MD4 και MD5

Οι αλγόριθμοι Message Digest αναπτύχθηκαν από τον Ronald Rivest. Οι αλγόριθμοι αυτοί χρησιμοποιούνται για εφαρμογές ψηφιακών υπογραφών και λειτουργούν ως εξής: ένα αρχικό μήνυμα πρέπει να είναι συμπιεσμένο με ένα σίγουρο τρόπο πριν αυτό συνοδευτεί με το ιδιωτικό κλειδί. Και οι τρεις αυτοί αλγόριθμοι παίρνουν ένα μήνυμα αυθαίρετου μήκους και δημιουργούν μια σύνοψη μηνύματος 128 bits. Παρόλο που η δομή των τριών αυτών αλγορίθμων είναι περίπου ίδια, ο σχεδιασμός του αλγορίθμου MD2 είναι λίγο διαφορετικός από τους MD4 και MD5. Ο MD2 έχει βελτιστοποιηθεί για υπολογιστές αρχιτεκτονικής 8 bits, ενώ οι MD4 και MD5 απευθύνονται για υπολογιστές αρχιτεκτονικής 32 bits.

Ο αλγόριθμος MD2 αναπτύχθηκε το 1989. Το μήνυμα συμπληρώνεται με μήκος που να είναι ακέραιο πολλαπλάσιο των 16 bytes. Το άθροισμα ελέγχου των 16 bytes συνοδεύεται στο μήνυμα και η τιμή hash υπολογίζεται στο αποτέλεσμα του μηνύματος. Οι Rogier και Chauvaud έχουν διαπιστώσει ότι μπορεί να προκύψουν συγκρούσεις στον MD2 εάν ο υπολογισμός του ελέγχου αθροίσματος παραλειφθούν. Αυτό είναι το μοναδικό κρυπταναλυτικό αποτέλεσμα που είναι γνωστό για τον αλγόριθμο MD2.

Ο αλγόριθμος MD4 αναπτύχθηκε το 1990. Το μήνυμα είναι συμπληρωμένο για να εξασφαλιστεί ότι το μήκος του σε bits συν 448 είναι ακέραιο πολλαπλάσιο του 512. Μια δυαδική αντιπροσώπευση 64 bits αρχικού μήκους του μηνύματος συνδέεται έπειτα στο μήνυμα.. Οι επιθέσεις στην έκδοση MD4 αναπτύχθηκαν πολύ γρήγορα από τους Den Boer και Bosselaers. Οι συγκρούσεις για την πλήρη έκδοση MD4 μπορούν να βρεθούν σε λιγότερο από ένα λεπτό σε ένα τυπικό PC. Προφανώς, ο αλγόριθμος MD4 πρέπει πλέον να θεωρηθεί σπασμένος.

Ο αλγόριθμος MD5 είναι επίσης αναπτυγμένος από τον Ronald Rivest. Ο αλγόριθμος αυτός αποτελεί μια βελτιωμένη έκδοση του MD4, αν και είναι λίγο αργότερος. Το μέγεθος της αποσύνθεσης μηνύματος και η συμπλήρωση μήκους του μηνύματος είναι ίδια με του MD4. Ο αλγόριθμος MD5 είναι αρκετά ασφαλής και ευρέως χρησιμοποιούμενος, αν και μπορεί να σπάσει με ισχυρά μηχανήματα σε εύλογο χρονικό διάστημα.

3.2.3 SHA (Secure Hash Algorithm)

Αναπτυγμένη από την NSA και σχεδιασμένη για χρήση με την National Institute for Standards and Technology's Digital Signature Standard (NIST's DSS). Λίγο μετά την δημοσίευση της θεωρήθηκε ανασφαλής από την NIST. Παράγει μήνυμα αποσύνθεσης μήκους 160 bit.

2.2.4 SHA-1 (Secure Hash Algorithm – 1)

Αναθεωρημένη έκδοση της SHA. Δεν είναι γνωστό αν είναι ασφαλέστερη από την προηγούμενη έκδοση. Παράγει μήνυμα αποσύνθεσης μήκους 160 bit. Ο αλγόριθμος αυτός είναι πιο αργός από τον MD5 αλλά το μεγαλύτερο μήκος του μηνύματος αποσύνθεσης τον κάνει πιο ασφαλή ενάντια σε επιθέσεις.

ΚΕΦΑΛΑΙΟ ΤΕΤΑΡΤΟ

ΟΛΟΚΛΗΡΩΜΕΝΟ ΠΛΑΙΣΙΟ ΑΣΦΑΛΕΙΑΣ

Στο τέταρτο κεφάλαιο θα αναφερθούμε στους μηχανισμούς εκείνους που μπορούν να συμβάλλουν στην *επίτευξη περισσότερης ασφάλειας στις ηλεκτρονικές συναλλαγές* και στους μηχανισμούς εκείνους που προσφέρουν *ασφάλεια σε ένα εταιρικό δίκτυο*. Όταν υλοποιούνται και οι δυο αυτοί μηχανισμοί τότε μπορούμε να μιλήσουμε για ένα ολοκληρωμένο πλαίσιο ασφαλείας. Επιπλέον, αναφερόμαστε σε ορισμένα σημαντικά πρωτόκολλα ασφαλείας ηλεκτρονικών συναλλαγών.

4.0 ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

Αρχικά θα αναφερθούμε στην δημιουργία ενός ολοκληρωμένου πλαισίου ασφαλείας ηλεκτρονικών συναλλαγών. Αυτό το πλαίσιο περιλαμβάνει τρία διαφορετικά μέρη τα οποία δουλεύουν μαζί και δημιουργούν μια βάση ασφαλείας για τις ηλεκτρονικές συναλλαγές. Αυτά τα τρία μέρη είναι η κρυπτογράφηση δημόσιου κλειδιού, η ψηφιακή υπογραφή και τα ψηφιακά πιστοποιητικά και όλα μαζί αποτελούν την **υποδομή του δημόσιου κλειδιού**. Συγκεκριμένα, για την κρυπτογράφηση δημόσιου κλειδιού έχουμε ήδη μιλήσει στο δεύτερο κεφάλαιο.

Σε αυτό το κεφάλαιο απομένει να αναφερθούμε για τα άλλα δυο μέρη. Συνεπώς, δίνουμε έναν ορισμό της ψηφιακής υπογραφής καθώς επίσης αναλύουμε τον τρόπο με τον οποίο επιτυγχάνεται η δημιουργία και η επαλήθευση της ψηφιακής υπογραφής. Επιπλέον, δίνουμε και ορισμό για τα ψηφιακά πιστοποιητικά, για το ποιος εκδίδει τα πιστοποιητικά και για την διαδικασία κατασκευής ενός ψηφιακού πιστοποιητικού. Τέλος, μιλάμε για την σημαντικότητα ύπαρξης πιστοποιητικών τόσο από την μεριά του χρήστη όσο και από τη μεριά ενός δικτυακού τόπου. [48] - [54]

4.1 ΥΠΟΔΟΜΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Η **Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure, PKI)** είναι μια βάση ασφαλείας που βεβαιώνει ότι οι συναλλαγές μέσω του Web μπορεί να είναι αξιόπιστες και πιστοποιεί την εγκυρότητα του κάθε φυσικού προσώπου που εμπλέκεται σε μια συναλλαγή στο Διαδίκτυο, και παράλληλα προστατεύει την ασφάλεια της συναλλαγής.

4.1.1 Ψηφιακές Υπογραφές

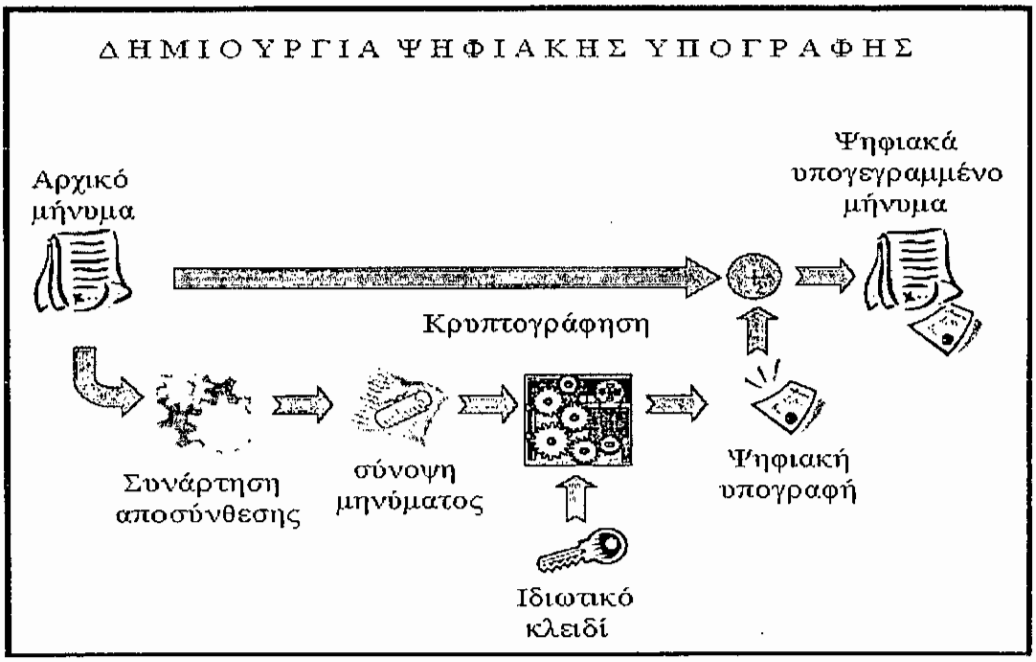
Η **ψηφιακή υπογραφή (digital signature)** είναι μια ποσότητα δεδομένων η οποία συνοδεύει ένα κρυπτογραφημένο μήνυμα. Η χρησιμοποίησή της σε ένα σύστημα ασφαλείας ενός δικτύου είναι απαραίτητη γιατί μπορεί να εγγυηθεί για την ταυτότητα του αποστολέα και να διασφαλίσει την ακεραιότητα των μηνυμάτων.

Οι ψηφιακές υπογραφές βασίζονται στην κρυπτογραφία δημόσιου κλειδιού. Δηλαδή, κάθε χρήστης έχει στην κατοχή του ένα ζεύγος κλειδιών, ένα δημόσιο κι ένα ιδιωτικό, τα οποία έχουν κάποιο μαθηματικό συσχετισμό μεταξύ τους. Κι όπως έχουμε αναφέρει, τα δημόσια κλειδιά γίνονται γνωστά στο κοινό ενώ τα ιδιωτικά είναι γνωστά μόνο στον κάτοχο τους. Η δημιουργία υπογραφής μπορεί να γίνει μόνο από τον κάτοχο του ιδιωτικού κλειδιού και ο οποιοσδήποτε μπορεί να επιβεβαιώσει /επαληθεύσει την υπογραφή ενός χρήστη με τη χρησιμοποίηση της δημόσιας υπογραφής εκείνου του χρήστη. Η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο.

Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής εμπλέκεται και η έννοια της συνάρτησης αποσύνθεσης. Εφαρμόζοντας την συνάρτηση αποσύνθεσης (συνάρτηση hash) σε ένα μήνυμα ανεξαρτήτως μεγέθους παράγεται μια συνοπτική έκδοση του μηνύματος, η οποία είναι μια σειρά από bits συγκεκριμένου μεγέθους, συνήθως 128 ή 160 bits. Η σύνοψη του μηνύματος (message digest) είναι μια ψηφιακή αναπαράσταση του μηνύματος και είναι μοναδική για το μήνυμα και το αντιπροσωπεύει. Επίσης, όπως έχουμε αναφέρει, η συνάρτηση αποσύνθεσης είναι μονόδρομη (one way hash), διότι από την σύνοψη του μηνύματος είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα.

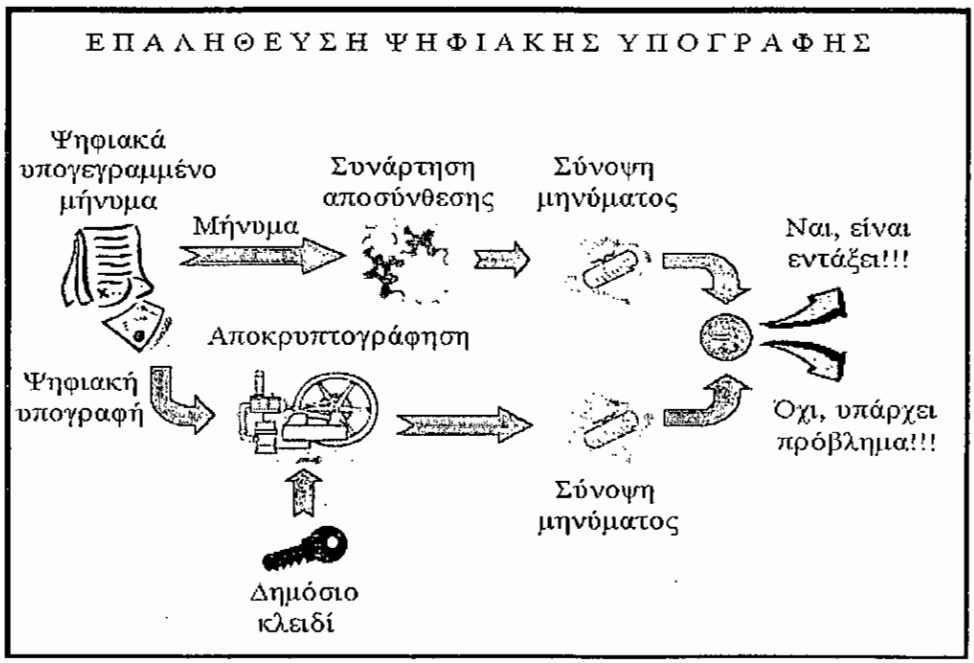
Για να δημιουργήσει κανείς μια ψηφιακή υπογραφή κρυπτογραφεί την σύνοψη του μηνύματος (message digest) και όχι το ίδιο το μήνυμα. Η σύνοψη μηνύματος εισάγεται στον αλγόριθμο ψηφιακής υπογραφής (digital signature algorithm, DSA) μαζί με το ιδιωτικό κλειδί για να δημιουργηθεί η ψηφιακή υπογραφή, που δεν είναι τίποτα άλλο από την κρυπτογραφημένη έκδοση της αποσύνθεσης του μηνύματος. Η ψηφιακή υπογραφή στέλνεται στον παραλήπτη για έλεγχο μαζί με το υπογεγραμμένο πλέον μήνυμα. Αυτός επιβεβαιώνει το μήνυμα ελέγχοντας την υπογραφή. Ο τρόπος που γίνεται αυτός είναι ο εξής: με το δημόσιο κλειδί του αποστολέα αποκρυπτογραφείται η ληφθείσα υπογραφή και έτσι προκύπτει μια σύνοψη μηνύματος. Αυτή συγκρίνεται με τη σύνοψη του μηνύματος που προκύπτει από την εφαρμογή της hash συνάρτησης στο μήνυμα που ελήφθη. Βέβαια, η hash συνάρτηση που χρησιμοποιείται για επιβεβαίωση θα πρέπει να είναι η ίδια με αυτή που χρησιμοποιήθηκε από τον αποστολέα Αν αυτές είναι ίδιες τότε είμαστε σίγουροι ότι το μήνυμα προέρχεται από τον κάτοχο του συγκεκριμένου δημοσίου κλειδιού και παράλληλα δεν αλλοιώθηκε στην πορεία. Αν όμως δεν είναι ίδιες οι δυο συνόψεις μηνύματος τότε είτε έχει παραποιηθεί το μήνυμα είτε έχει χρησιμοποιηθεί διαφορετικό ιδιωτικό κλειδί για την κρυπτογράφηση της σύνοψης από αυτό που θα έπρεπε, δηλαδή η ταυτότητα του αποστολέα δεν είναι αυτή που εκείνος υποστηρίζει, γιατί θα γνώριζε ποιο είναι το ιδιωτικό κλειδί που του αναλογεί και θα το χρησιμοποιούσε. Αυτός είναι ο τρόπος με τον οποίο οι ψηφιακές υπογραφές παρέχουν τον έλεγχο της αυθεντικότητας της ταυτότητας των χρηστών και της ακεραιότητας των μηνυμάτων.

Παρακάτω, θα αναφέρουμε βήμα προς βήμα τις ενέργειες του αποστολέα και του παραλήπτη καθώς επίσης και τα σχήματα που ακολουθούν βοηθούν ώστε να γίνει κατανοητός ο μηχανισμός της δημιουργίας και επαλήθευσης της ψηφιακής υπογραφής.



Αποστολέας

1. Ο αποστολέας χρησιμοποιώντας κάποιον αλγόριθμο αποσύνθεσης δημιουργεί από το αρχικό μήνυμα που επιθυμεί να στείλει μια σύνοψη του μηνύματος αυτού (message digest).
2. Με το ιδιωτικό του κλειδί, ο αποστολέας κρυπτογραφεί τη σύνοψη κι αυτό που παράγεται είναι η ψηφιακή υπογραφή.
3. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με την ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου.



Παραλήπτης

1. Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή, η οποία είναι κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα.
2. Ο παραλήπτης εφαρμόζει τον ίδιο αλγόριθμο αποσύνθεσης στο μήνυμα που έλαβε και τότε δημιουργεί την σύνοψη του μηνύματος.
3. Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).

4. Τέλος, συγκρίνει τις δυο συνόψεις και αν βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης γίνεται αποδεκτό, αλλιώς απορρίπτεται.

4.1.2 Ψηφιακά Πιστοποιητικά

Όπως μπορούμε να παρατηρήσουμε ότι καθημερινά πιστοποιούμε την ταυτότητα μας ανεπαίσθητα, για παράδειγμα όταν χρειάζεται να υπογράψουμε ένα έγγραφο και δείχνουμε την ταυτότητα μας. Επειδή όμως ο κόσμος εξελίσσεται σε ένα περιβάλλον που όλες οι αποφάσεις και οι συναλλαγές πραγματοποιούνται ηλεκτρονικά, υπάρχουν λοιπόν ηλεκτρονικές τεχνικές οι οποίες αποδεικνύουν την πιστοποίηση της ταυτότητας μας και μέσω των ψηφιακών πιστοποιητικών μπορεί να αποδειχθεί η ταυτότητα μας ηλεκτρονικά.

Ο σημαντικότερος τύπος ψηφιακών πιστοποιητικών είναι το **πιστοποιητικό δημοσίου κλειδιού (public key certificate)**, το οποίο στηρίζεται στην ασύμμετρη κρυπτογράφηση. Το αδύνατο σημείο στην επικοινωνία με ασύμμετρη κρυπτογράφηση είναι ότι δεν μπορούμε να είμαστε σίγουροι όταν μας ανακοινώνει κάποιος το δημόσιο κλειδί του και ισχυρίζεται ότι έχει μια συγκεκριμένη ταυτότητα ότι έχει όντως αυτή την ταυτότητα. Θα πρέπει λοιπόν με κάποιον τρόπο να βεβαιωθούμε ότι η σχέση κλειδιού – ταυτότητας είναι όντως αυτή. Το πρόβλημα αυτό μπορεί να λυθεί αν με κάποιο τρόπο ο κάτοχος του δημοσίου κλειδιού (το άτομο το οποίο κατέχει και το ιδιωτικό κλειδί) συσχετιστεί με το δημόσιο κλειδί. Αυτό παρέχουν τα ψηφιακά πιστοποιητικά, τα οποία είναι ηλεκτρονικά αρχεία και πιστοποιούν την ταυτότητα ενός προσώπου.

Δηλαδή, μια κοινώς αποδεκτή αρχή εκδίδει τα πιστοποιητικά για τα ζεύγη δημόσιου – ιδιωτικού κλειδιού. Κάθε πιστοποιητικό περιέχει το δημόσιο κλειδί και πληροφορία που χαρακτηρίζει τον ιδιοκτήτη του, ο οποίος είναι ο κάτοχος του αντίστοιχου ιδιωτικού κλειδιού. Στο τέλος το ψηφιακό πιστοποιητικό υπογράφεται από την εκδίδουσα αρχή χρησιμοποιώντας το ιδιωτικό κλειδί της.

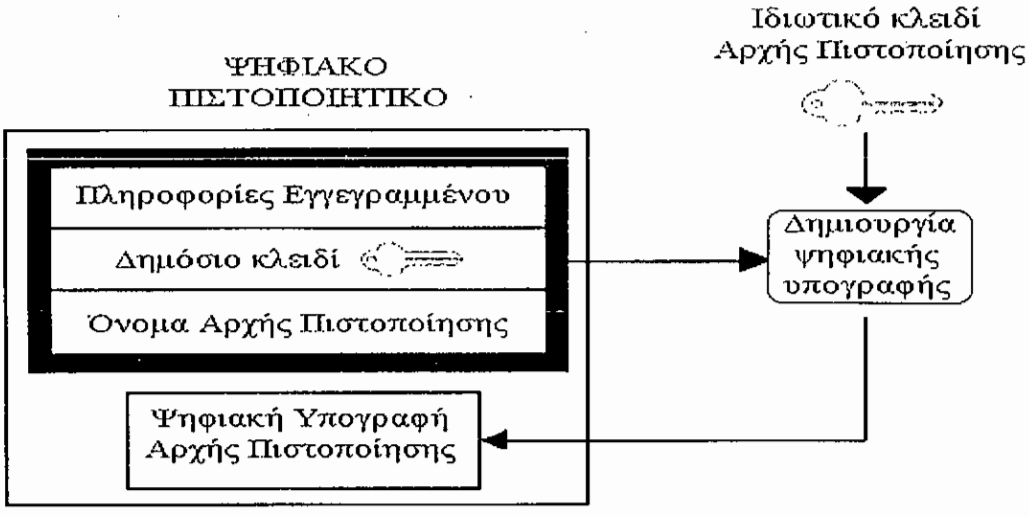
Η εμπλεκόμενη αυτή οντότητα που εγγυάται την ταυτότητα του κατόχου που διαθέτει το ζεύγος κλειδιών είναι γνωστή ως **Έμπιστη Τρίτη Οντότητα (ΕΤΟ)** ή αλλιώς **Αρχή Πιστοποίησης** (Certificate Authority, CA) ή **Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ).**

Αναλυτικότερα, μια Αρχή Πιστοποίησης υπογράφει ψηφιακά με ένα ιδιωτικό κλειδί ένα πιστοποιητικό το οποίο περιέχει το όνομα της Αρχής Πιστοποίησης που το εξέδωσε, το δημόσιο κλειδί του εγγεγραμμένου, το όνομα και διάφορες πληροφορίες του εγγεγραμμένου (δηλαδή την ταυτότητα του). Με τον τρόπο αυτό επιβεβαιώνει η Αρχή Πιστοποίησης ότι το συγκεκριμένο πρόσωπο που αναφέρεται στο πιστοποιητικό είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού. Το σημείο-κλειδί είναι η εμπιστοσύνη στην Αρχή Πιστοποίησης. Αν ένας χρήστης εμπιστεύεται την Αρχή Πιστοποίησης τότε εμπιστεύεται και το πιστοποιητικό που η Αρχή Πιστοποίησης του έχει εκδώσει. Ο λόγος είναι πως αν είμαστε σίγουροι πως ένα δημόσιο κλειδί αντιστοιχεί σίγουρα σε κάποιον τότε κάθε υπογεγραμμένο μήνυμα που προέρχεται από αυτόν και περνάει τον έλεγχο ψηφιακής υπογραφής είμαστε

σίγουροι πως προέρχεται από αυτόν και επίσης πως το περιεχόμενό του είναι έγκυρο. Κανένας άλλος δεν μπορεί να προσποιηθεί πως είναι η Αρχή Πιστοποίησης αφού δεν διαθέτει το ιδιωτικό της κλειδί και έτσι κανένας άλλος δεν μπορεί να υπογράψει ψεύτικα πιστοποιητικά.

Έτσι ο παραλήπτης που λαμβάνει ένα ψηφιακό πιστοποιητικό από οποιονδήποτε μπορεί να είναι σίγουρος για την ορθότητα του περιεχομένου του, δηλαδή για την ταυτότητα και το δημόσιο κλειδί του χρήστη τον οποίο το πιστοποιητικό αφορά.

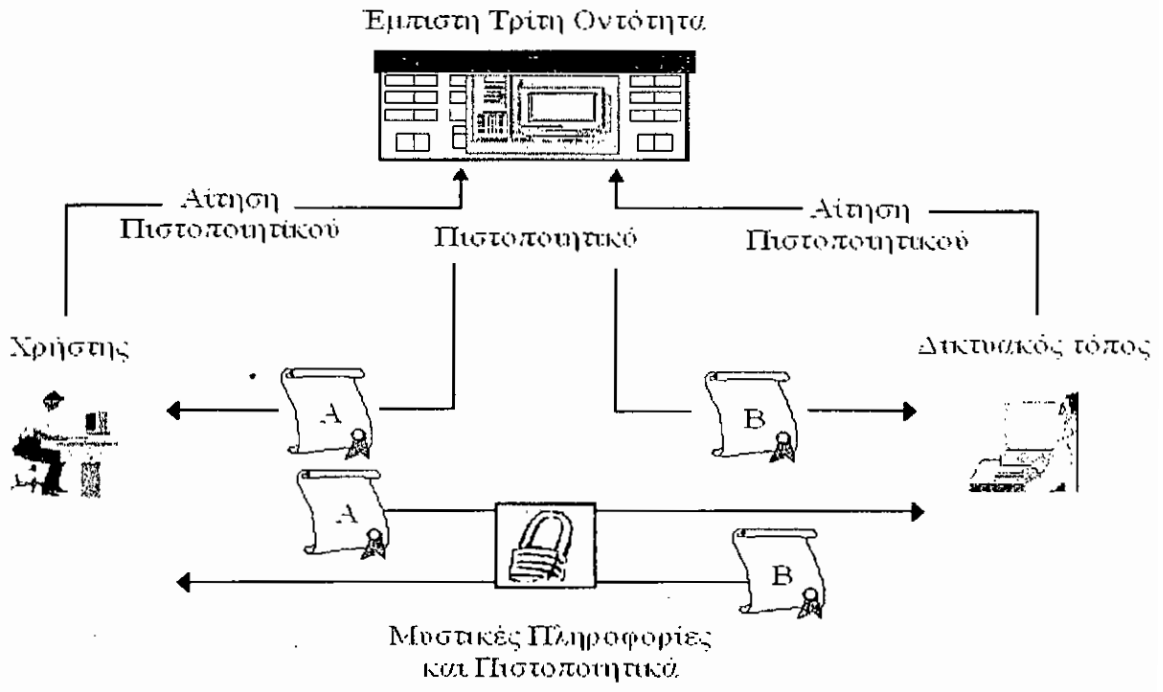
Παρακάτω, φαίνεται η διαδικασία κατασκευής του ψηφιακού πιστοποιητικού καθώς επίσης και το τι περιέχει ένα ψηφιακό πιστοποιητικό.



Για την πιστοποίηση της ταυτότητας ενός δικτυακού τόπου χρησιμοποιούνται και τα **πιστοποιητικά ασφαλείας δικτυακών τόπων**, που σε σχέση με τα απλά πιστοποιητικά επιπλέον εγγυώνται και την ασφάλεια του περιεχομένου ενός δικτυακού τόπου. Τα πιστοποιητικά ασφάλειας δικτυακών τόπων περιέχουν πληροφορίες που πιστοποιούν ότι η συγκεκριμένη ιστοσελίδα είναι γνήσια και ασφαλής. Αυτό σημαίνει ότι κανένα άλλο site δεν μπορεί να παρουσιαστεί με την συγκεκριμένη ταυτότητα της γνήσιας τοποθεσίας. Επίσης, τα πιστοποιητικά ασφάλειας δικτυακών τόπων εξασφαλίζουν την εγκυρότητα και την ασφάλεια του περιεχομένου τους. Δηλαδή, δεν αρκεί να λάβει ένας δικτυακός τόπος ένα πιστοποιητικό από μια αρχή πιστοποίησης που θα βεβαιώνει την ταυτότητά του αλλά

θα πρέπει να βεβαιώνει πως το περιεχόμενο του τόπου είναι αυτό που ισχυρίζεται. Για παράδειγμα, μπορεί ένας δικτυακός τόπος να έλαβε κάποια στιγμή που ασχολούνταν με τραπεζικές συναλλαγές ένα πιστοποιητικό. Κάποια στιγμή όμως λόγω ελλιπούς συντήρησης και κακής διαχείρισης μπορεί το περιεχόμενό του να παραβιάστηκε από κάποιον hacker ώστε κάθε φορά που δίνουμε προσωπικά μας στοιχεία ή κάνουμε διάφορες συναλλαγές αυτός να τις αλλοιώνει με δικό του όφελος. Έτσι, θα πρέπει με κάποιον τρόπο να είμαστε βέβαιοι όχι μόνο για την εγκυρότητα της ταυτότητας ενός δικτυακού τόπου αλλά και για το περιεχόμενό του. Για το σκοπό αυτό κάθε φορά που γίνονται μεγάλες αλλαγές στο περιεχόμενο ενός δικτυακού τόπου αυτό θα πρέπει να αντικατοπτρίζεται στην έκδοση ενός νέου πιστοποιητικού. Επίσης, αν κάποιος τόπος σταματήσει τη λειτουργία του η διεύθυνσή του μετά από κάποιο διάστημα που μένει ανενεργή διατίθεται σε όποιον θέλει να τη χρησιμοποιήσει. Φυσικά σε αυτή την περίπτωση κάθε πιστοποιητικό που έχει εκδοθεί δεν είναι αληθές. Για τους παραπάνω λόγους, τα πιστοποιητικά ασφαλείας χρονολογούνται κατά την έκδοσή τους και έχουν μια ημερομηνία λήξης πέρα από την οποία δεν ισχύουν. Κάθε φορά που συνδεόμαστε με το web site ενός οργανισμού, το πρόγραμμα ανάγνωσης επαληθεύει τη διεύθυνση Internet που είναι αποθηκευμένη στο πιστοποιητικό και ελέγχει την ημερομηνία λήξης του. Εάν οι πληροφορίες αυτές δεν είναι έγκυρες ή εάν έχει παρέλθει η ημερομηνία λήξης, εμφανίζεται προειδοποιητικό μήνυμα (Warning).

Το παρακάτω σχήμα που ακολουθεί απεικονίζει από την μια πλευρά έναν χρήστη και έναν δικτυακό τόπο, τα πιστοποιητικά που έχουν προμηθευτεί από μια Αρχή Πιστοποίησης και τον τρόπο που τα χρησιμοποιούν.



4.2 ΠΡΩΤΟΚΟΛΛΑ ΑΣΦΑΛΕΙΑΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

4.2.1 Το πρωτόκολλο SECURE SOCKETS LAYER (SSL)

Γενικά

Το πρωτόκολλο **Secure Socket Layer (SSL)** είναι ένα υβριδικό πρωτόκολλο επικοινωνίας το οποίο εφαρμόζει μεθόδους συμμετρικής κι ασύμμετρης κρυπτογράφησης. Συγκεκριμένα, χρησιμοποιείται για να εξασφαλίσει ασφαλής σύνδεση μεταξύ του χρήστη και του κεντρικού διακομιστή. Το πρωτόκολλο SSL παρέχει ακεραιότητα και ασφάλεια στα δεδομένα που διακινούνται, μεταξύ του καταναλωτή και του εμπόρου. Αναπτύχθηκε από την **Netscape Communications Corporation** για την ασφαλή επικοινωνία ευαίσθητων πληροφοριών όπως προσωπικά στοιχεία και αριθμούς πιστωτικών καρτών και αργότερα υιοθετήθηκε από την Internet Engineering Task Force (IETF) σαν γενικό πρωτόκολλο ασφαλείας. Η πρώτη σχεδίαση του πρωτοκόλλου έγινε τον Ιούλιο του 1994 και αποτελούσε την πρώτη έκδοση (version 1.0) και τον Οκτώβριο του ίδιου χρόνου δημοσιοποιήθηκε υπό την μορφή RFC (Request For Comments). Τον Δεκέμβριο του 1994 εκδίδεται μια

αναθεώρηση του πρωτοκόλλου, η δεύτερη έκδοση (version 2.0) και στα τέλη του 1995, παρουσιάστηκε στο κοινό η τρίτη έκδοση του SSL (version 3.0). Από τα μέσα του 1995 άρχισε να εφαρμόζεται σε προϊόντα της εταιρίας, όπως τον **Netscape Navigator**. [55] - [56]

Εισαγωγή στο πρωτόκολλο SSL

Θα μπορούσαμε να πούμε ότι τα περισσότερα προγράμματα προβολής ιστοσελίδων (Web browsers), χρησιμοποιούν το πρωτόκολλο SSL για να αυθεντικοποιούν και να κρυπτογραφούν τα δεδομένα που διακινούνται. Επίσης, το πρωτόκολλο SSL σχεδιάστηκε προκειμένου να παρέχεται απόρρητη επικοινωνία μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί σαν πελάτης (client) και το άλλο σαν εξυπηρετητής (server). Η εξασφάλιση του απόρρητου γίνεται με την κρυπτογράφηση όλων των μηνυμάτων. Επιπλέον, η πιστοποίηση της ταυτότητας του server είναι υποχρεωτική και του client προαιρετική. Τέλος, εξασφαλίζει την ακεραιότητα των δεδομένων, ώστε κανείς να μην μπορεί να αλλοιώσει την πληροφορία.

Άρα οι υπηρεσίες που παρέχει το πρωτόκολλο SSL είναι:

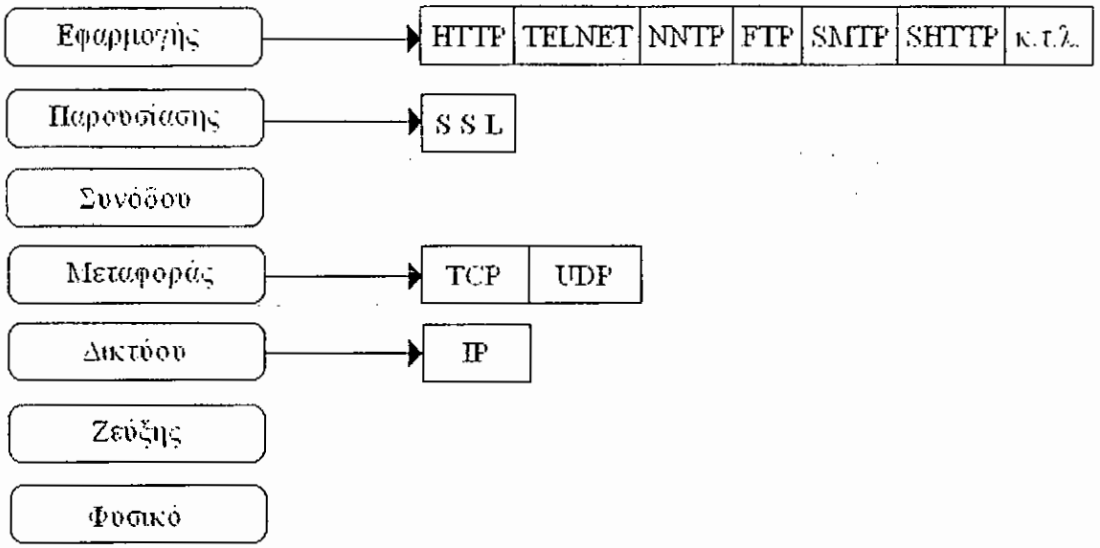
- **Αυθεντικότητα του server:** Ο server αυθεντικοποιείται στον client επιδεικνύοντας το πιστοποιητικό του.
- **Αυθεντικότητα του client:** Ο πελάτης αυθεντικοποιείται στον server επιδεικνύοντας το πιστοποιητικό του. Η υπηρεσία αυτή είναι προαιρετική στις ηλεκτρονικές αγορές (Internet shopping) διότι δεν έχουν όλοι οι πελάτες ψηφιακά πιστοποιητικά. Περισσότερο χρησιμοποιείται σε περιπτώσεις Internet Banking όπου παίζει πολύ σημαντικό ρόλο.
- **Ακεραιότητα των δεδομένων:** Τα δεδομένα που μεταδίδονται προστατεύονται ώστε οποιαδήποτε προσπάθεια αλλοίωσης τους να γίνει αντιληπτή.
- **Εμπιστευτικότητα:** Τα δεδομένα που μεταδίδονται είναι κρυπτογραφημένα από το πρωτόκολλο.

Το SSL και το μοντέλο OSI

Στη διαστρωματοποιημένη λογική του OSI το Secure Socket Layer βρίσκεται ακριβώς επάνω από το επίπεδο μεταφοράς και κάτω από το επίπεδο εφαρμογής,

οπότε μπορεί κανείς να πει πως ανήκει στο **στρώμα παρουσίασης**. Αυτό σημαίνει ότι η μεγάλη πλειοψηφία των εφαρμογών του Διαδικτύου, όπως το Web (HTTP), οι ομάδες ειδήσεων UseNet (NNTP), και το e-mail (SMTP και POP) μπορούν να διασφαλιστούν από το πρωτόκολλο SSL.

Το παρακάτω σχήμα που ακολουθεί παρουσιάζει το μοντέλο OSI και ορισμένα πρωτόκολλα που συναντάμε στα στρώματά του. Μπορούμε να διακρίνουμε επακριβώς ότι το πρωτόκολλο SSL βρίσκεται στο στρώμα παρουσίασης.

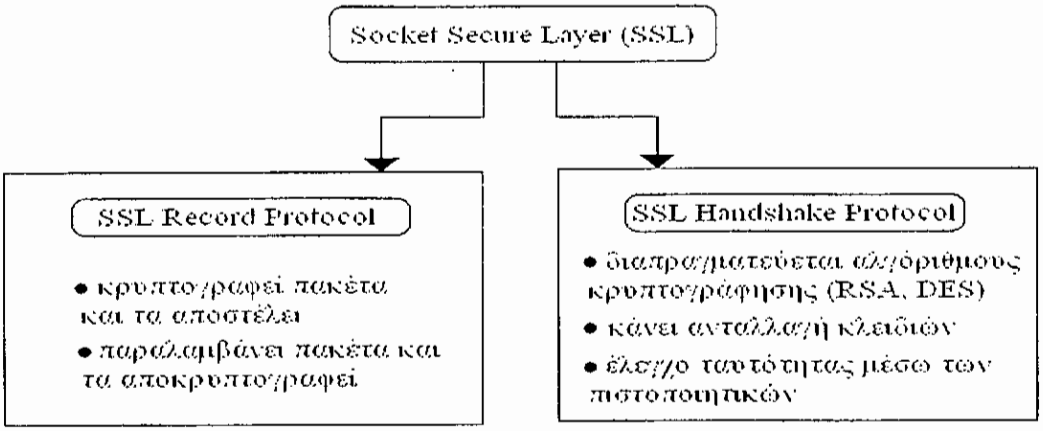


Μοντέλο OSI

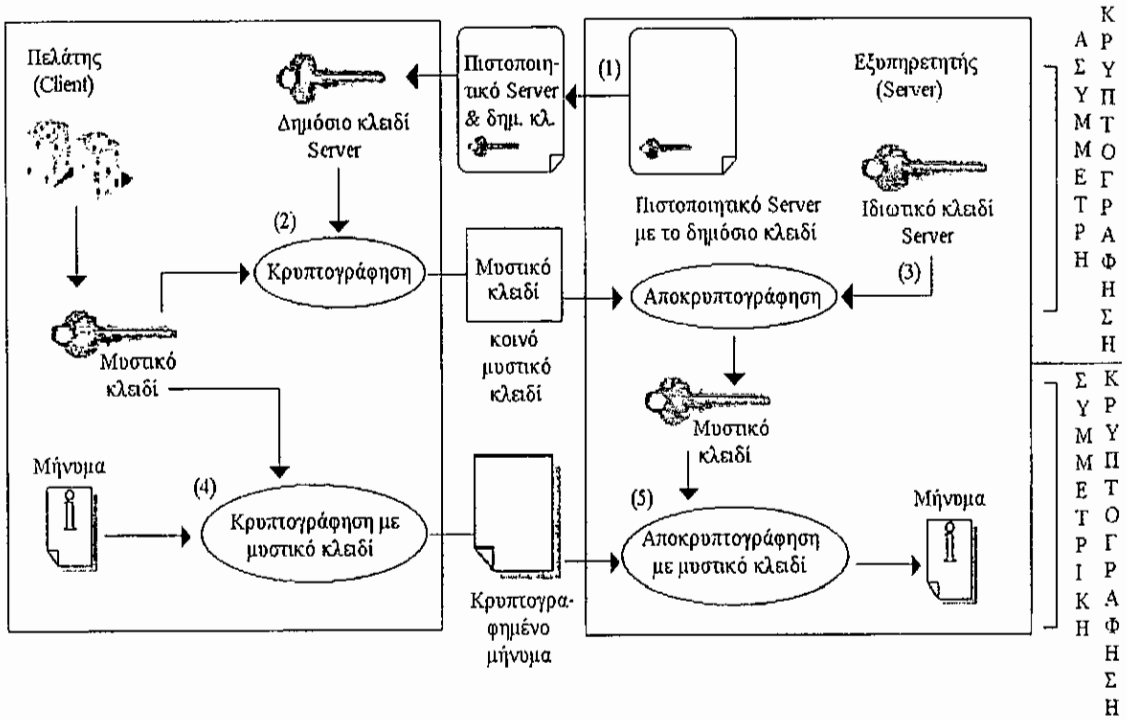
Λειτουργία του SSL

Το SSL αποτελείται από δύο υπό-πρωτόκολλα, το **SSL Record Protocol (SSLRP)** και το **SSL Handshake Protocol (SSLHP).** Το SSL Record Protocol συλλέγει τα δεδομένα σε πακέτα και αφού τα κρυπτογραφήσει τα μεταδίδει και αποκρυπτογραφεί τα παραλαμβανόμενα πακέτα. Προκειμένου, το SSL Record Protocol να κάνει την κρυπτογράφηση ενός πακέτου θα πρέπει ο client και ο server να γνωρίζουν τα κρυπτογραφικά κλειδιά. Αυτό επιτυγχάνεται μέσω του SSL Handshake Protocol (SSLHP) το οποίο χρησιμοποιείται για τη διαπραγμάτευση των αλγορίθμων κρυπτογράφησης που θα χρησιμοποιηθούν (αυτοί οι αλγόριθμοι μπορεί να είναι οι RSA, DES), την ανταλλαγή κλειδιών και πραγματοποιεί έλεγχο της ταυτότητας του server (μέσω των ψηφιακών πιστοποιητικών) και αν ζητηθεί και του client, όπως αναφέραμε και προηγουμένως.

Ο παρακάτω πίνακας περιέχει μια συνοπτική αναφορά της λειτουργίας του πρωτοκόλλου SSL.



Ο παρακάτω πίνακας αναπαριστά την διαδικασία που ακολουθεί ο Server κι ο Client προκειμένου να συμφωνήσουν για το κλειδί που θα χρησιμοποιήσουν αλλά και για τον τρόπο με τον οποίο θα μεταφέρουν μια έμπιστη πληροφορία.



Για να συμφωνηθεί το μυστικό κλειδί χρησιμοποιούν την ασύμμετρη κρυπτογράφηση.

1. Ο Server στέλνει το πιστοποιητικό του στο οποίο βρίσκεται και το δημόσιο κλειδί του για να αποδείξει την ταυτότητα (αυθεντικότητα) του στον Client.
2. Ο Client αφού λάβει το δημόσιο κλειδί του Server θα το χρησιμοποιήσει προκειμένου να κρυπτογραφήσει το μυστικό κλειδί, το οποίο προκύπτει από ένα τυχαίο αριθμό και θα χρησιμοποιηθεί στη συνέχεια για να σταλεί ένα μήνυμα με ασφάλεια.
3. Ο Server θα αποκρυπτογραφήσει το μήνυμα με το ιδιωτικό του κλειδί για να μάθει το μυστικό κλειδί.

Το πρωτόκολλο SSL, όπως έχουμε προαναφέρει συνδυάζει ασύμμετρη και συμμετρική κρυπτογράφηση. Προκειμένου, να σταλεί ένα μήνυμα με ασφάλεια μπορεί να χρησιμοποιείται η συμμετρική κρυπτογραφία.

4. Ο Client κρυπτογραφεί ένα μήνυμα με το μυστικό κλειδί (που έχει ήδη προσυμφωνήσει με τον Server).
5. Ο Server με τη σειρά του το αποκρυπτογραφεί με το ίδιο μυστικό κλειδί.

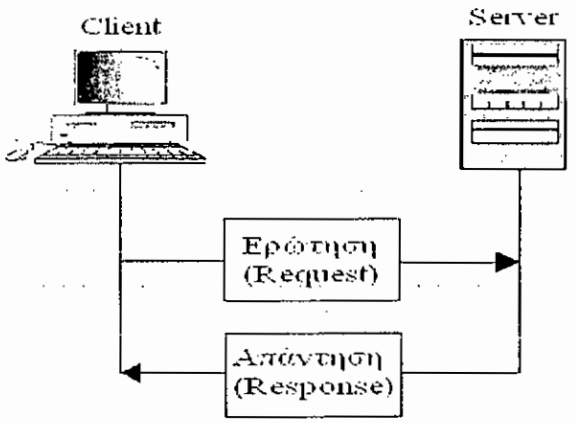
4.2.2 Πρωτόκολλο μεταφοράς Secure – Hyper Text Transaction Protocol (S-HTTP)

Γενικά

Το πρωτόκολλο HTTP πραγματοποιούσε έλεγχο πρόσβασης ο οποίος στηριζόταν σε UserIDs και passwords. Ο server διέθετε λίστες οι οποίες περιλάμβαναν τους χρήστες (clients) και τα passwords τους σε κρυπτογραφημένη μορφή. Όμως το πρωτόκολλο αυτό εμφάνισε κάποιες δυσκολίες. Η διαχείριση του σε μεγάλα δίκτυα παρουσίασε δυσκολίες και τα passwords μεταφέρονταν σε 'καθαρή' μορφή χωρίς όμως να κρυπτογραφούνται.

Προκειμένου λοιπόν να εξαλειφθούν οι αδυναμίες του HTTP, αναπτύχθηκε το **S-HTTP (Secure - Hypertext Transfer Protocol)** το οποίο ενεργεί στο **στρώμα εφαρμογής** παρέχει κρυπτογράφηση, αυθεντικοποίηση και υπογραφή καθώς και συνδυασμό αυτών. Επίσης, αποτελεί ένα υπερσύνολο με επεκτάσεις ασφαλείας του HTTP, που είναι το γνωστό πρωτόκολλο μοντέλου ερώτησης – απάντησης (request –

response transaction protocol) που υλοποιεί το γνωστό μας Web με την λήψη και ανάγνωση των ιστοσελίδων μέσω του Διαδικτύου. Αναπτύχθηκε από τους E. Rescorla και A. Schiffman της Enterprise Integration Technologies και διανεμήθηκε ως εμπορικό προϊόν από την Terisa Systems. Ο κύριος ρόλος του S-HTTP είναι να προστατεύει την κίνηση που υπάρχει ανάμεσα σε ένα χρήστη ή πελάτη (client) και έναν εξυπηρετητή (server), δηλαδή τα requests και τα responses του πρωτοκόλλου. Στόχος της σχεδίασης ήταν ένα ευέλικτο πρωτόκολλο που διαθέτει πολλαπλούς μηχανισμούς και αλγόριθμους, και την δυνατότητα διαπραγμάτευσης αυτών. [57] – [59]



Βασικά χαρακτηριστικά του S-HTTP

1. Το S-HTTP υποστηρίζει μία ποικιλία μηχανισμών ασφαλείας στους πελάτες (clients) και τους εξυπηρετητές (servers) του HTTP. Το πρωτόκολλο παρέχει συμμετρικές δυνατότητες στον client και τον server που σημαίνει ότι τα μηνύματα και οι αποκρίσεις και των δύο πλευρών αντιμετωπίζονται με τον ίδιο τρόπο.

2. Το πρωτόκολλο S-HTTP δεν απαιτεί πιστοποιητικά δημοσίων κλειδιών από την μεριά του client, καθ' ότι υποστηρίζει και τα συμμετρικά κλειδιά. Αυτό είναι σημαντικό γιατί οι ιδιωτικές συναλλαγές μπορούν να λάβουν χώρα χωρίς την απαίτηση από τους χρήστες να έχουν αποκτήσει ένα έγκυρο ζεύγος δημόσιου – ιδιωτικού κλειδιού από ένα οργανισμό πιστοποιητικών, όπως από τη Verisign. Βέβαια, το S-HTTP είναι σε θέση να αξιοποιήσει την υπάρχουσα υποδομή πιστοποιητικών και ασύμμετρων κλειδιών για καλύτερα αποτελέσματα.

3. Το S-HTTP υποστηρίζει από άκρη σε άκρη ασφαλής συναλλαγές και σε καμία περίπτωση ευαίσθητα δεδομένα δεν μεταδίδονται στο δίκτυο απροστάτευτα.

4. Η κρυπτογράφηση και οι αλγόριθμοι που θα χρησιμοποιηθούν μπορούν να γίνουν αντικείμενο διαπραγμάτευσης. Δηλαδή, ένας πελάτης μπορεί να διευκρινίσει ότι μια σύνοδος επικοινωνίας ιστού (web session) απαιτεί την εμπιστευτικότητα μέσω της βασικής συμμετρικής κρυπτογράφησης, κι ένας κεντρικός υπολογιστής μπορεί να απαιτήσει την επικύρωση των πελατών μέσω του συστήματος δημόσιου κλειδιού. Οι ιδιότητες ασφάλειας για μία συναλλαγή διαπραγματεύονται μεταξύ του πελάτη και του εξυπηρετητή (server) κατά τη διάρκεια της αρχικοποίησης (initialization) μιας σύνδεσης, δηλαδή του ορισμού των παραμέτρων που θα χρησιμοποιηθούν στη συνέχεια για τη μεταξύ τους επικοινωνία. Κατά τη διαπραγμάτευση ο πελάτης και ο server μπορούν να προσδιορίσουν αν μια συγκεκριμένη ιδιότητα ασφαλείας είναι απαιτούμενη, προαιρετική ή απορριπτέα. Αν ένας συμμέτοχος καθορίσει ότι μια ιδιότητα ασφαλείας είναι απαιτούμενη, τότε αποδέχεται την σύνδεση με τον άλλο συμμέτοχο μόνο αν η ιδιότητα αυτή μπορεί να εφαρμοσθεί από το άλλο μέρος. Εν περίληψη, το S-HTTP παρέχει στο χρήστη τη δυνατότητα να επικοινωνήσει με ασφάλεια με έναν κεντρικό υπολογιστή δικτύου με την **διαπραγμάτευση των επιθυμητών ιδιοτήτων ασφαλείας της επικοινωνίας.**

Σύγκριση S-HTTP και SSL

Αυτό που κάνε το πρωτόκολλο S-HTTP να διαφέρει ριζικά από το πρωτόκολλο SSL είναι πως το S-HTTP είναι μια αυτόνομη εφαρμογή που βρίσκεται στο στρώμα εφαρμογής, ενώ το SSL είναι ένα πρωτόκολλο το οποίο παρέχει τις υπηρεσίες του στις εφαρμογές (εννοείται του στρώματος εφαρμογής) και βρίσκεται στο στρώμα παρουσίασης.

Οι υπηρεσίες που παρέχονται και από τα δυο πρωτόκολλα είναι περίπου ίδιες. Το S-HTTP και το SSL παρέχουν τη δυνατότητα να επικοινωνήσουν με ασφάλεια με τους κεντρικούς υπολογιστές ενός δικτύου. Επιπλέον, και τα δύο μπορούν να χρησιμοποιηθούν για να **εξασφαλίσουν την εμπιστευτικότητα, και την ακεραιότητα των δεδομένων**. Όμως, το πρωτόκολλο S-HTTP παρέχει τη

δυνατότητα χρήσης ψηφιακής υπογραφής, χαρακτηριστικό που συμβάλλει σε περισσότερη ασφάλεια και μη απαρνησιμότητα.

Το S-HTTP είναι ένα δυνατό πρωτόκολλο αλλά θεωρείται δύσκολο ως προς τη συντήρηση του για την ανάπτυξη των ιστοχώρων γι' αυτό το SSL κυριαρχεί περισσότερο.

Ο παρακάτω πίνακας που ακολουθεί παρουσιάζει περιληπτικά την σύγκριση μεταξύ του πρωτοκόλλου S-HTTP και του SSL.

	S-HTTP	**SSL**
Στρώμα εφαρμογής	•	
Στρώμα παρουσίασης		•
Εμπιστευτικότητα	•	•
Ακεραιότητα δεδομένων	•	•
Μη απαρνησιμότητα	•	
Ψηφιακή υπογραφή	•	
Ψηφιακά Πιστοποιητικά		•
Παροχή υπηρεσιών σε άλλες εφαρμογές		•

Χρήσεις του S-HTTP

Η πιο κοινή του εφαρμογή είναι για την διασφάλιση HTTP επικοινωνιών μεταξύ του browser και του web server. Η ασφαλή έκδοση του HTTP χρησιμοποιεί URL (Uniform Resource Locator) που ξεκινούν με 'https' αντί του κανονικού 'http' (για παράδειγμα, https://www.ups.com/ σε αντίθεση με το http://www.ups.com/). Από εκεί και ύστερα η επικοινωνία τους είναι κρυπτογραφημένη.

4.2.3 Το πρωτόκολλο SECURE ELECTRONIC TRANSACTIONS (SET)

Γενικά

Στα πρώτα στάδια του ηλεκτρονικού εμπορίου, οι καταναλωτές απλά έστελναν τον αριθμό της πιστωτικής τους κάρτας και την ημερομηνία λήξης της στους εμπόρους με την μορφή απλού μηνύματος χωρίς κρυπτογράφηση. Σύντομα όμως αυτός ο τρόπος χρήσης της πιστωτικής κάρτας στο διαδίκτυο εγκαταλείφθηκε καθώς το μήνυμα ήταν πολύ εύκολο να υποκλαπεί με αποτέλεσμα να παρατηρηθούν κρούσματα απάτης με πιστωτικές κάρτες. Προκειμένου να λυθούν τα προβλήματα απάτης οι οργανισμοί

πιστωτικών καρτών προχώρησαν στη δημιουργία ενός προτύπου, του **Secure Electronic Transaction (SET)** που αναπτύχθηκε από τους οργανισμούς της Visa και της MasterCard. Το πρότυπο ήταν ο μόνος τρόπος για ασφαλές ηλεκτρονικό εμπόριο και προστασία των αριθμών των πιστωτικών καρτών από κλοπή κι εκμετάλλευση. Συγκεκριμένα, το πρωτόκολλο SET σχεδιάστηκε ώστε να επιτρέπει στους χρήστες του Internet να αγοράζουν προϊόντα από εμπόρους του Web, κατά τέτοιο τρόπο ώστε ο έμπορος να μη βλέπει τον κωδικό της πιστωτικής κάρτας του πελάτη, και η τράπεζα να μη μαθαίνει το προϊόν που επιθυμεί να αποκτήσει ο πελάτης. Άρα από αυτό μπορούμε να συμπεράνουμε ότι το πρωτόκολλο SET εξασφάλιζε την **μυστικότητα των συναλλαγών**.

Δυστυχώς όμως δεν έτυχε ευρείας αποδοχής λόγω του ότι ήταν ένα ακριβό σύστημα και η διαδικασία εισαγωγής του σε έναν οργανισμό αρκετά περίπλοκη. Απέτρεπε τόσο τους εμπόρους όσο και τους κατόχους πιστωτικών καρτών να το χρησιμοποιήσουν και σαν επακόλουθο, το 2001 οι οργανισμοί Visa και MasterCard προχώρησαν στην υλοποίηση νέων συστημάτων αυθεντικοποίησης, για την ασφάλεια των ηλεκτρονικών συναλλαγών. Έτσι, σχεδίασαν και υιοθέτησαν ένα νέο πρότυπο το **3D-Secure**, το οποίο και αντικατέστησε το SET. Για το πρότυπο αυτό θα μιλήσουμε αναλυτικά παρακάτω. [60]

Οντότητες που εμπλέκονται σε ένα πρωτόκολλο 3D-Secure

Υπάρχουν τέσσερις κύριες οντότητες που εμπλέκονται σε ένα πρωτόκολλο 3D-Secure και είναι οι εξής: ο κάτοχος της πιστωτικής κάρτας, ο έμπορος, ο μεσάζον και ο εκδότης. Και δυο δευτερεύουσες οντότητες η πύλη πληρωμών και οι αρχές πιστοποίησης. Πιο αναλυτικά:

1. **Ο κάτοχος πιστωτικής κάρτας (Cardholder):** Είναι ο κάτοχος μιας πιστωτικής κάρτας ο οποίος είναι εξουσιοδοτημένος από την τράπεζα να τη χρησιμοποιεί προκειμένου να πραγματοποιεί τις συναλλαγές που επιθυμεί.
2. **Ο έμπορος (Merchant):** Είναι ο πωλητής των αγαθών ή των υπηρεσιών και αποδέχεται τις ηλεκτρονικές πληρωμές.
3. **Ο μεσάζων (Acquirer):** Είναι ένας οικονομικός οργανισμός που υποστηρίζει τους εμπόρους παρέχοντας τους υπηρεσίες για ηλεκτρονικές πληρωμές μέσω πιστωτικών καρτών.

4. Ο εκδότης (Issuer): Είναι ένας οικονομικός οργανισμός που εκδίδει πιστωτικές κάρτες και τυπικά φέρνει την ονομασία (Visa, MasterCard).

Και οι δευτερεύουσες οντότητες είναι οι εξής:

1. Πύλη Πληρωμών (Payment Gateway): Είναι ένα σύστημα το οποίο επεξεργάζεται την πιστοποίηση των εμπόρων και των συναλλαγών.

2. Αρχές Πιστοποίησης (Certification Authorities): Αναλαμβάνει να πιστοποιεί τα δημόσια κλειδιά των κατόχων, των εμπόρων, των μεσαζόντων και των πυλών πληρωμών τους, όποτε ζητείται.

Λειτουργίες του πρωτοκόλλου 3D-Secure

Όταν κάποιος κάτοχος μιας πιστωτικής κάρτας αποφασίσει να αποκτήσει ένα προϊόν από έναν έμπορο ηλεκτρονικά τότε θα πρέπει να κρυπτογραφήσει δυο μηνύματα για να σταλούν οι πληροφορίες προστατευμένες και όχι εκτεθειμένες. Το πρώτο μήνυμα θα περιέχει τον αριθμό της πιστωτικής του κάρτας κρυπτογραφημένο και το δεύτερο μήνυμα θα περιέχει την πληροφορία που σχετίζεται με το προϊόν που επιθυμεί να αποκτήσει ηλεκτρονικά ο πελάτης (για παράδειγμα, την Τριλογία του Tolkien). Κατόπιν, και τα δύο μηνύματα υπογράφονται, κρυπτογραφούνται και στέλνονται στον έμπορο (για παράδειγμα, ένα ηλεκτρονικό βιβλιοπωλείο).

Στο σημείο αυτό θα πρέπει να αναφέρουμε ότι η κρυπτογράφηση των πληροφοριών γίνεται – όπως είναι αναμενόμενο – από τη μεριά του χρήστη. Δηλαδή στον προσωπικό υπολογιστή του χρήστη υπάρχει ένα ειδικό πρόγραμμα (στο οποίο βρίσκεται το πιστοποιητικό του) κι εκεί υπάρχει αποθηκευμένο ένα ζεύγος κλειδιών, ένα ιδιωτικό κι ένα δημόσιο. Αυτό το πρόγραμμα καλείται **«ηλεκτρονικό πορτοφόλι»** ή αλλιώς ψηφιακό πορτοφόλι και μέσα σε αυτό ο χρήστης κρυπτογραφεί με το ιδιωτικό του κλειδί τις πληροφορίες που θέλει να εισάγει για να αποσταλούν σε πρώτη φάση στον έμπορο.

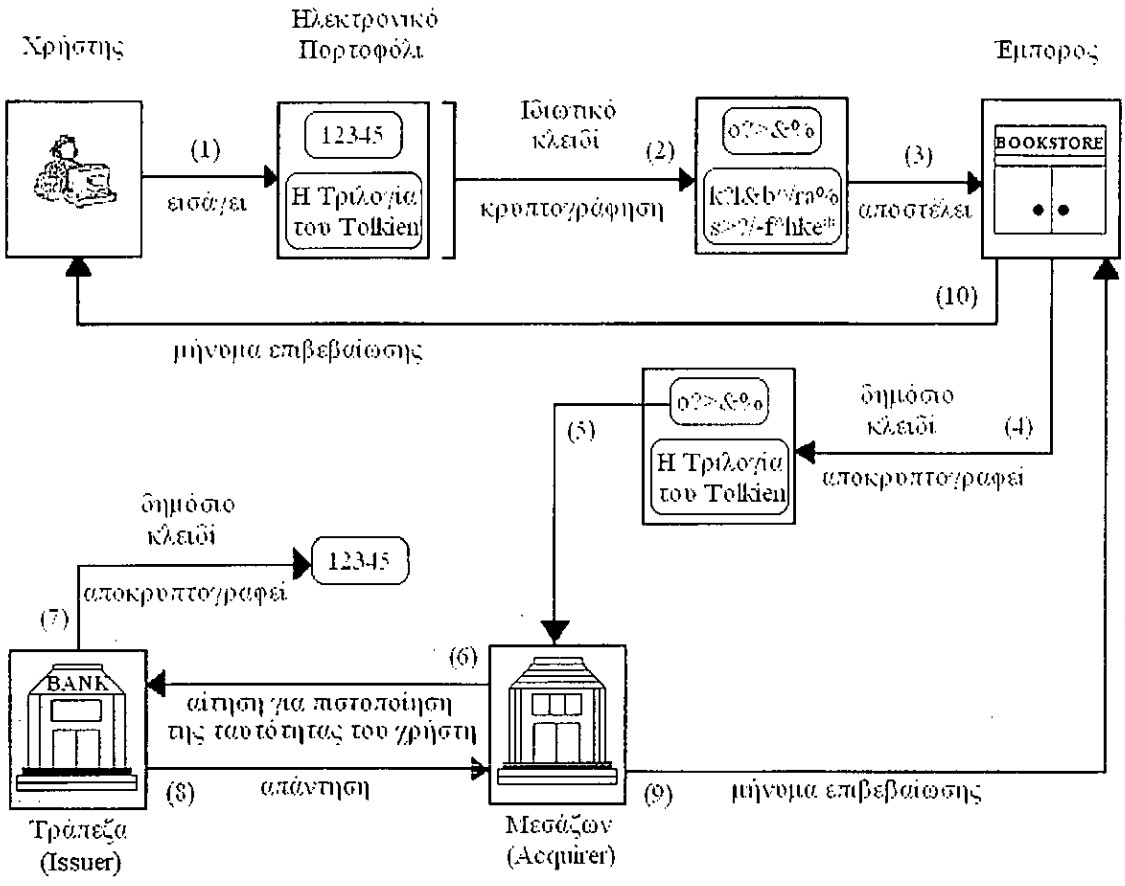
Ο έμπορος με τη σειρά του λαμβάνει τα δύο κρυπτογραφημένα μηνύματα και αποκρυπτογραφεί με το δημόσιο κλειδί του χρήστη **μόνο** το μήνυμα που περιέχει την πληροφορία για το προϊόν που θέλει να αγοράσει ο πελάτης και το άλλο το μήνυμα το προωθεί σε έναν οικονομικό οργανισμό (acquirer) ο οποίος όπως είπαμε παρέχει υπηρεσίες για πληρωμές μέσω των πιστωτικών καρτών κι εγκρίνει τις συναλλαγές

διαμέσου της τράπεζας (issuer). Η εταιρία που δημιουργεί το ηλεκτρονικό πορτοφόλι δεν εξουσιοδοτεί ποτέ τους εμπόρους ούτε κάποιον οικονομικό οργανισμό να επεξεργαστούν την κρυπτογραφημένη πληροφορία του αριθμού της πιστωτικής κάρτας. Αυτό το αναλαμβάνει αποκλειστικά η τράπεζα, όπως θα δούμε παρακάτω.
Στη συνέχεια, ο οικονομικός οργανισμός (acquirer) εφόσον έχει υλοποιήσει το πρότυπο λαμβάνει την κρυπτογραφημένη πληροφορία και την αποστέλλει ανεπεξέργαστη στην τράπεζα (issuer) ζητώντας να πιστοποιήσει την ταυτότητα του κατόχου της κάρτας.

Η τράπεζα (issuer) πιστοποιεί την ταυτότητα του κατόχου της κάρτας και απαντά αντίστοιχα στον οικονομικό οργανισμό (acquirer). Μετά την πιστοποίηση της ταυτότητας του κατόχου της κάρτας, η διαδικασία συνεχίζεται με τη λήψη έγκρισης για τη χρέωση της κάρτας και η τράπεζα στέλνει μια απάντηση στον οικονομικό οργανισμό (acquirer) σαν επιβεβαίωση ότι εγκρίνει τα προσωπικά και οικονομικά στοιχεία του πελάτη (δηλαδή του κατόχου της κάρτας). Αν η τράπεζα (issuer) δεν έχει δεν έχει υλοποιήσει το πρότυπο 3D-Secure, η διαδικασία πιστοποίησης δεν μπορεί να προχωρήσει.

Τέλος, ένα μήνυμα επιβεβαίωσης αποστέλλεται και από τον οικονομικό οργανισμό στον έμπορο έτσι ώστε ο έμπορος να σιγουρευτεί για την κίνηση της συναλλαγής και να αναμένει την πληρωμή του. Και με τη σειρά του ο έμπορος αποστέλλει μήνυμα επιβεβαίωσης στον κάτοχο της κάρτας ότι η συναλλαγή διεξήχθη σωστά.

Το παρακάτω σχήμα που ακολουθεί αναπαριστά τα όσα αναφέραμε παραπάνω



Μπορούμε να πούμε ότι το πρωτόκολλο 3D-Secure παρέχει υπηρεσίες **πιστοποίησης της ταυτότητας** του κατόχου μιας πιστωτικής κάρτας και του εμπόρου, **εμπιστευτικότητα** και διασφάλιση της **ακεραιότητα του μηνύματος**. Επιπροσθέτως, το πρωτόκολλο 3D-Secure παρέχει **προστασία** όταν μεταδίδονται οικονομικά δεδομένα, διασφαλίζει την ακεραιότητα του μηνύματος, παρέχει **αυθεντικότητα των κατόχων πιστωτικών καρτών** στους εμπόρους και στους μεσάζοντες για την αποφυγή χρήσης κλεμμένων καρτών, **αυθεντικότητα των εμπόρων** στους κατόχους πιστωτικών καρτών και στους μεσάζοντες για την αποφυγή περιπτώσεων εικονικών ηλεκτρονικών καταστημάτων που πραγματοποιούν ψευδείς συναλλαγές και τέλος διασφαλίζει την **ακεραιότητα του μηνύματος**.

4.3 ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΣΕ ΕΝΑ ΔΙΚΤΥΟ

Προκειμένου να επιτύχουμε ολοκληρωμένη ασφάλεια δεν αρκεί να εξετάζουμε μονομερώς τους μηχανισμούς που παρέχουν ασφάλεια στις ηλεκτρονικές συναλλαγές αλλά θα πρέπει να είμαστε σίγουροι ότι το δίκτυο μας (ας υποθέσουμε ότι μιλάμε για ένα εταιρικό δίκτυο) είναι καλά προστατευμένο από πιθανές επιθέσεις). Πρώτο μέλημα είναι να ενδυναμωθεί και να υποστηριχθεί ένα εταιρικό δίκτυο από μηχανισμούς προκειμένου να μπορεί να αντιμετωπίσει πιθανούς κινδύνους ώστε να κρίνετε αξιόπιστο και να είναι ασφαλές.

"Είναι εύκολο να έχεις ένα ασφαλές υπολογιστικό σύστημα. Το μόνο που χρειάζεται είναι να αποσυνδέσεις όλες τις τηλεφωνικές του συνδέσεις, να τοποθετήσεις το σύστημα σε ένα θωρακισμένο δωμάτιο και να στήσεις έναν φύλακα έξω από την πόρτα."

F. T. Gramp & R. H. Morris

4.4 ΚΙΝΔΥΝΟΙ ΕΝΟΣ ΕΤΑΙΡΙΚΟΥ ΔΙΚΤΥΟΥ

Όπως αναφέραμε προηγουμένως, θα πρέπει να σιγουρευτούμε πως εκτός από την ασφαλή διεκπεραίωση των πάσης φύσεως συναλλαγών μέσω των διάφορων ειδών δικτύων (όπως το Internet ή ένα εταιρικό δίκτυο) θα πρέπει να είμαστε σίγουροι και για την ασφάλεια των δεδομένων **εντός των εταιρικών δικτύων**. Τα κενά (ή οι τρύπες) ασφαλείας που υπάρχουν εντοπίζονται στο εσωτερικό των εταιρικών δικτύων, παρότι θα περίμενε κανείς το ελεγχόμενο αυτό περιβάλλον να προφυλάσσεται πάρα πολύ καλά. Η κλοπή 20.000 αριθμών πιστωτικών καρτών από την Netcom στις αρχές της δεκαετίας του '90 τονίζει την κρισιμότητα της ασφάλειας στα εταιρικά δίκτυα. Οι λόγοι που τα εταιρικά δίκτυα κινδυνεύουν είναι πολλοί.

Ο πρώτος λόγος είναι πως στο εσωτερικό των εταιρικών δικτύων συναντάμε **πολύπλοκες λογισμικές εγκαταστάσεις** οι οποίες είναι δύσκολο να ελεγχθούν 100%

ως προς την ασφάλειά τους και έτσι αφήνονται άθελα ανοικτές προσβάσεις (security holes), τις οποίες ανακαλύπτουν κι εκμεταλλεύονται διάφοροι επιτήδειοι.

Ο δεύτερος λόγος και ο πιο απρόβλεπτος αλλά και αυτός που ποτέ δε θα μπορέσουμε να εξαλείψουμε είναι **ο ανθρώπινος παράγοντας**. Αρκετές από τις αποτελεσματικότερες τεχνικές πρόσβασης σε υπολογιστές ελάχιστη σχέση έχουν με τεχνικές λεπτομέρειες. Οι υπάλληλοι που δεν ακολουθούν τις πολιτικές ασφαλείας που έχουν οριστεί είναι ένας μεγάλος κίνδυνος για την ασφάλεια ενός δικτύου. Η προθυμία ορισμένων ανθρώπων να αποκαλύπτουν τους κωδικούς πρόσβασης τους, να τους σημειώνουν σε χαρτιά ή ατζέντες, να ορίζουν ευκολομνημόνευτα γι' αυτούς passwords ή ακόμη να περιγράφουν τα μέτρα ασφαλείας που λαμβάνουν και να εμπιστεύονται ανθρώπους που ελάχιστα γνωρίζουν αποτελούν τις αιτίες πολλών παραβιάσεων στην ασφάλεια συστημάτων.

Όμως, μια χειρότερη κατηγορία υπαλλήλων από τους αμελείς είναι αυτοί που θέλουν εσκεμμένα να προκαλέσουν προβλήματα ασφάλειας στο σύστημα μιας επιχείρησης. Αυτοί οι υπάλληλοι μπορεί να είναι δυσαρεστημένοι για κάποιο λόγο με τη διοίκηση της επιχείρησης (για παράδειγμα, δεν πήραν την αύξηση που περίμεναν) και να θέλουν να προκαλέσουν πρόβλημα ή μπορεί να είναι ακόμα και «βιομηχανικοί κατάσκοποι» (Industrial espionage) και να θέλουν να διοχετεύσουν μυστικά της επιχείρησης σε μια ανταγωνιστική της.

Επίσης, ένας άλλος λόγος που αξίζει να αναφέρουμε έχει να κάνει με την εμφάνιση **κακόβουλου λογισμικού**. Ένα τέτοιου είδους λογισμικό επιδιώκει να προκαλέσει ζημίες ή ακόμη να καταστρέψει αρχεία και προγράμματα ενός υπολογιστή. Οι ειδικοί στον χώρο της ασφάλειας των υπολογιστών και των δικτύων έχουν επίσημους ορισμούς για όλους τους τύπους κακόβουλου λογισμικού και ηλεκτρονικής απάτης. Παρακάτω ακολουθεί μια σύντομη ανάλυση των περισσότερων τύπων κακόβουλου λογισμικού.

<u>Πίσω πόρτες (Back doors)</u>

Οι πίσω πόρτες δεν αποτελούν κακόβουλο λογισμικό αυτό καθ' αυτό όμως είναι μια τροποποίηση νόμιμου λογισμικού με συχνά κακόβουλο σκοπό και επιτρέπουν μη εξουσιοδοτημένη πρόσβαση σε κάποιο σύστημα. Από την άλλη μπορούν να

χρησιμοποιηθούν και από ειδικούς ασφαλείας σαν «δόλωμα» για τον εντοπισμό και παγίδευση ιδιαίτερα ταλαντούχων εισβολέων. Ορισμένες φορές και οι ίδιοι σχεδιαστές λειτουργικών συστημάτων δημιουργούν σκόπιμα «πίσω πόρτες» που τους δίνουν την δυνατότητα να κάνουν αλλαγές σε οτιδήποτε θέλουν.

Ιοί (Viruses)

Ένας πραγματικός Ιός στην κλασική του έννοια είναι ένα κομμάτι κώδικα που προσαρτάται σε κάποιο άλλο εκτελέσιμο κώδικα, έτσι ώστε όταν εκτελείται το «μολυσμένο» πρόγραμμα να εκτελείται και ο Ιός μαζί του. Αφού εκτελεστεί ο Ιός μεταφέρεται στην κύρια μνήμη του ηλεκτρονικού υπολογιστή και μπορεί να έχει τον πλήρη έλεγχο του συστήματος. Συνήθως το πρώτο μέλημα του είναι να παράγει πιστά αντίγραφα του εαυτού του να τα συνδέει σε άλλα εκτελέσιμα προγράμματα έτσι ώστε να εξαπλώνεται. Οι Ιοί δεν είναι αυτόνομα προγράμματα – δεν μπορούν να εκτελεστούν από μόνοι τους και απαιτούν για την ενεργοποίησή τους την εκτέλεση κάποιου προγράμματος που περιέχει τον Ιό μέσα στον κώδικά του.

Σκουλήκια (Worms)

Τα Σκουλήκια είναι αυθύπαρκτα προγράμματα που μεταφέρονται από υπολογιστή σε υπολογιστή σε ένα δίκτυο, προσαρτώντας αυτόνομα κομμάτια του κώδικά τους. Εξ ορισμού τα Σκουλήκια δεν τροποποιούν άλλα προγράμματα αλλά μπορεί να κουβαλούν μέσα τους κάποιο Ιό που μπορεί να το κάνει. Βασική φιλοδοξία ενός Σκουληκιού είναι η αναπαραγωγή του εαυτού του. Ιδιαίτερα δημοφιλές περιστατικό με λογισμικό τύπου σκουλήκι αποτελεί η περίφημη περίπτωση του "Internet worm" τον Νοέμβριο του 1988. Ο Robert T. Morris φοιτητής τότε στο Harvard εξαπέλυσε – κατά τα λεγόμενα του από λάθος – το διάσημο "Internet worm" το οποίο μόλυνε χιλιάδες υπολογιστές μέσα σε λίγες ώρες και υπερφόρτωσε με τους κλώνους του, εκατοντάδες δίκτυα συνδεδεμένα με το διαδίκτυο. Ο πατέρας του Robert ήταν τότε ένας από τους κορυφαίους επιστήμονες ασφάλειας του Internet που βοήθησε στην ανακάλυψη της ταυτότητας του δράστη.

Δούρειοι Ίπποι (Trojan Horses)

Εν αντιθέσει, με τους Ιούς, οι Δούρειοι Ίπποι είναι αυτόνομα προγράμματα που απαιτούν την εκτέλεση τους από τον χρήστη για να ενεργοποιηθούν. Δηλαδή, παρουσιάζονται συνήθως σε διάφορες ιστοσελίδες ως πολύ χρήσιμα και

ενδιαφέροντα, με σκοπό να πείσουν τον χρήστη να τα εγκαταστήσει στον υπολογιστή του. Οι Δούρειοι Ίπποι παριστάνουν ένα χρήσιμο πρόγραμμα που ο χρήστης επιθυμεί να εκτελέσει (για παράδειγμα, ένα παιχνίδι). Ενώ το πρόγραμμα φαίνεται να κάνει αυτό που θέλει ο χρήστης στην πραγματικότητα κάνει και κάτι άλλο άσχετο με τον διαφημιζόμενο σκοπό του όπως για παράδειγμα, διαγραφή του σκληρού δίσκου, διαγραφή αρχείων, εύρεση αριθμών πιστωτικών καρτών και αποστολή αυτών στον δημιουργό του Δούρειου Ίππου. Οι Δούρειοι Ίπποι μεταμφιέζονται τόσο καλά που μπορεί να παραπλανήσουν ακόμη κι έναν έμπειρο χρήστη. Η αυξανόμενη χρήση του παγκόσμιου ιστού (World Wide Web) έχει δημιουργήσει ένα περιβάλλον όπου οι Ιοί και οι Δούρειοι Ίπποι μπορούν να ανθίσουν και να εξαπλωθούν πάρα πολύ εύκολα.

Ζόμπι ή προγράμματα λαγοί (Zombies or Rabbit programs)

Αυτά είναι προγράμματα που «κλωνοποιούν» τον εαυτό τους με στόχο να κατακλύσουν τους πόρους του «μολυσμένου» υπολογιστικού συστήματος με σκοπό την κατάρρευσή του.

4.5 ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΩΝ ΚΙΝΔΥΝΩΝ

Για όλους αυτούς τους λόγους λοιπόν θα πρέπει να θωρακίσουμε σε κάθε επίπεδο τα συστήματα μηχανοργάνωσης μιας επιχείρησης. Ένα ολοκληρωμένο σύστημα ασφάλειας δικτύου θα πρέπει να περιέχει οπωσδήποτε τα παρακάτω συστατικά:

4.5.1 Καταγραφέα συμβάντων (event logger).

Αποθηκεύει σε προστατευμένα αρχεία τις καταγραφές από έναν αριθμό «αισθητήρων» που μπορεί να είναι λογισμικό ή υλικό και βρίσκονται σε στρατηγικά σημεία του δικτύου. Ο σκοπός του είναι να είναι δυνατή η χρονική ανακατασκευή ενός γεγονότος παραβίασης της ασφάλειας του δικτύου ή απόπειρας για κάτι τέτοιο, ώστε να είναι δυνατή η ανάλυση του γεγονότος και η εύρεση του κενού ασφαλείας που υπήρξε. Αποτελεί τη βάση γνώσεων για τη δημιουργία ενός συστήματος ανίχνευσης εισβολής. Στα ιστορικά αρχεία του θα πρέπει να καταγράφεται κάθε γεγονός δυνατόν, όπως για παράδειγμα: κάθε είσοδος στο σύστημα, κάθε ανεπιτυχής απόπειρα σύνδεσης, κάθε κίνηση μηνυμάτων, κάθε διαχειριστική πράξη, κάθε έκδοση πιστοποιητικού κ.λ.π.

4.5.2 Συστήματα ανίχνευσης εισβολής (intrusion detection system – IDS).

Είναι συστήματα που αναλαμβάνουν να ανιχνεύσουν κάθε απόπειρα εισβολής ή κάθε εισβολή σε εξέλιξη. Ο προφανής στόχος τους είναι να παρέχουν έγκαιρη προειδοποίηση στο διαχειριστή του δικτύου ώστε αυτός να λάβει τα κατάλληλα μέτρα. Τα μέτρα αυτά είναι: 1) περιορισμός της εισβολής στο αρχικό σημείο, 2) αντιμετώπιση της εισβολής, 3) έλεγχος των γειτονικών συστημάτων για τυχόν επέκταση της εισβολής, 4) λήψη των απαραίτητων μέτρων για επαναφορά του συστήματος στην αρχική κατάσταση, 5) λήψη των απαραίτητων μέτρων για κλείσιμο του κενού ασφαλείας που επέτρεψε την εισβολή. Τα συστήματα IDS θέλουμε να έχουν όσο το δυνατόν περισσότερους αυτόματους μηχανισμούς για την άμεση αντίδραση σε κάθε εν δυνάμει πρόβλημα. Για το σκοπό αυτό θα πρέπει να αξιοποιήσουμε κατάλληλα τα ιστορικά στοιχεία που έχουν καταγραφεί στον καταγραφέα συμβάντων ώστε να οργανώσουμε εκ των προτέρων την αυτόματη αντίδρασή μας σε κάθε παρόμοια επίθεση.

Εκτός όμως από το να περιμένουμε να γίνει μια επίθεση για να διαπιστώσουμε με ποιο τρόπο έγινε και αν ο σχεδιασμός της άμυνάς μας ήταν σωστός, ο πιο αποτελεσματικός τρόπος είναι να ελέγξουμε την άμυνά μας άμεσα. Ο πιο απλός τρόπος είναι η χρήση ειδικών προγραμμάτων που λέγονται Network Scanners. Οι **Network Scanners** ελέγχουν το δίκτυο και μετά δημιουργούν αναφορές στις οποίες περιέχονται πολλά στοιχεία σχετικά με τις ενδεχόμενες αδυναμίες του δικτύου. Ο έλεγχος αυτού του τύπου λέγεται **Network Security Analysis**. Δυστυχώς, οι αναφορές που παράγουν αυτά τα προγράμματα περιέχουν πολλές λανθασμένες ή υπερεκτιμημένες επισημάνσεις ασφάλειας, ενώ αποτυγχάνουν να ανιχνεύσουν άλλες. Ο καλύτερος τρόπος για να ελέγξουμε την ανθεκτικότητα σε επιθέσεις ενός δικτύου είναι να προκαλέσουμε διάφορα σενάρια επιθέσεων και να δούμε ποια ήταν τα αποτελέσματα. Αυτό μπορεί να γίνει πραγματοποιώντας πραγματικές επιθέσεις με τεχνικές που χρησιμοποιούν οι πραγματικοί hackers. Βέβαια, αυτή η αντιμετώπιση απαιτεί εξαιρετικά εξειδικευμένες και ενημερωμένες γνώσεις (που πολλές φορές οι hackers κατέχουν σε μεγαλύτερο βαθμό από τους διαχειριστές των δικτύων!) και πολύ χρόνο, πράγματα που δεν είναι πάντα διαθέσιμα εν αφθονία. Ο έλεγχος αυτού του τύπου λέγεται «**έλεγχος διείσδυσης**» (**penetration testing**).

4.5.3 Firewalls (Πύρινοι Τοίχοι)

Τα **Firewalls** είναι ειδικά προγράμματα προστασίας από τα περισσότερα είδη επιθέσεων όπως Ιοί, Σκουλήκια, hackers. Χρησιμοποιούνται από οργανισμούς, επιχειρήσεις και ακαδημαϊκά ιδρύματα και τοποθετούνται μεταξύ του εσωτερικού και του εξωτερικού δικτύου μιας εταιρίας, παρέχουν έναν απλό τρόπο να ελεγχθεί το μέγεθος και το είδος των μεταφερόμενων πληροφοριών μεταξύ των δύο δικτύων.

Ο όρος Firewall προέρχεται από τον χώρο της κατασκευαστικής βιομηχανίας. Πολλά εργαστήρια, γραφεία και εργοστάσια όταν πρωτοφτιάχνονται εξοπλίζονται με Firewalls δηλαδή με ειδικά κατασκευασμένους πυρίμαχους τοίχους. Έτσι ώστε σε περίπτωση που ξεσπάσει μια πυρκαγιά στο κτίριο, είναι πολύ πιθανόν ότι θα είναι εκτός ελέγχου μόνο το συγκεκριμένο κομμάτι του κτιρίου που ξεκίνησε καθότι τα Firewalls θα σταματήσουν ή θά συγκρατήσουν την εξέλιξη της φωτιάς μέχρι να έρθει βοήθεια.

Η ίδια ακριβώς φιλοσοφία μπορεί να εφαρμοστεί και για την προστασία τοπικών δικτύων από εξωτερικές επιθέσεις. Ένα Firewall μπορεί να περιορίσει το μέγεθος της ζημιάς. Ένας εισβολέας για παράδειγμα, μπορεί να καταφέρει να διεισδύσει σε μια ομάδα μηχανημάτων ενός οργανισμού αλλά το Firewall θα προστατεύσει τις υπόλοιπες ομάδες.

Επίσης, το Firewall μπορεί να παρέχει σε έναν διαχειριστή δικτύου στοιχεία για τα είδη των δεδομένων και το ποσό κυκλοφορίας που πέρασε μέσω αυτού, για το πόσες απόπειρες παραβίασης έγιναν και άλλες υπηρεσίες. Ένα Firewall όχι μόνο αποτρέπει την ανεξέλεγκτη πρόσβαση, αλλά και δεν επιτρέπει στους ανιχνευτές δικτύου (προγράμματα, πολλές φορές αυτόματα – bots) να ψάχνουν για ανοικτές θύρες, και βοηθά επίσης στον προσδιορισμό εκείνων που προσπαθούν να παραβιάσουν την ασφάλειά ενός συστήματος. Το Firewall αρχικά καθορίζει εάν η εισερχόμενη μετάδοση είναι κάτι που ζητείται από έναν χρήστη στο δίκτυο και φυσικά οτιδήποτε εισέρχεται εξετάζεται περισσότερο. Ακόμη, ελέγχεται η διεύθυνση του πομπού για να εξασφαλιστεί ότι είναι από εμπιστευμένη περιοχή ή όχι κι ελέγχεται και το περιεχόμενο της μετάδοσης.

4.5.4 Αντι-ικό λογισμικό (Anti-virus software)

Η πιο διαδεδομένη άμυνα ενάντια σε σχεδόν όλους τους τύπους κακόβουλου λογισμικού αποτελούν αναμφίβολα τα **αντι-ικά προγράμματα**. Το λογισμικό αυτού τους είδους υπάρχει εδώ και αρκετά χρόνια και αν κάποιος χρήστης δεν χρησιμοποιεί συστηματικά κάποιο τέτοιο πρόγραμμα, τότε μάλλον παίρνει ένα μεγάλο ρίσκο. Ένα τυπικό πρόγραμμα αυτής της κατηγορίας αφού εγκατασταθεί (κατά προτίμηση σε κάποιο μηχάνημα που δεν έχει ακόμη συνδεθεί σε κάποιο δίκτυο) δίνει αρκετές επιλογές στον χρήστη του όπως τον έλεγχο των τοπικών μέσων αποθήκευσης για ιούς, δούρειους ίππους, καθώς επίσης και τον έλεγχο στο δίκτυο με το οποίο είναι συνδεμένο το μηχάνημα αρκεί φυσικά να υπάρχει η κατάλληλη πρόσβαση. Επίσης ο χρήστης μπορεί να ορίσει προγραμματισμένους ελέγχους του συστήματος για κακόβουλο λογισμικό, σε συγκεκριμένες ημερομηνίες και ώρες όπως επίσης και να αυτοματοποιήσει τον έλεγχο ώστε αυτός να γίνεται χωρίς την δική του παρέμβαση και να δρα μόνο όταν βρεθεί κάποιος ιός στο σύστημα.

Η βασική φιλοσοφία πίσω από τα αντι-ικά προγράμματα είναι η εξής: Κάθε ιός σαν πρόγραμμα που είναι έχει διαφορετικό κώδικα από όλους τους υπόλοιπους. Το αντι-ικό πρόγραμμα διαθέτει καταχωρημένα στην βάση δεδομένων του μοναδικά κομμάτια κώδικα που το κάθε ένα αντιστοιχεί σε κάποιον ιό. Αυτά τα κομμάτια λέγονται υπογραφές (signatures) και αποτελούν πλεονέκτημα αλλά και μειονέκτημα για την άμυνα του συστήματος. Πλεονέκτημα γιατί το αντι-ικό πρόγραμμα μπορεί να αναγνωρίσει και να "σκοτώσει" με μεγάλη ακρίβεια οποιαδήποτε ιό που είναι καταχωρημένος στην βάση του οπουδήποτε και αν βρίσκεται στο σύστημα. Μειονέκτημα γιατί απλά οποιοσδήποτε ιός δεν είναι καταχωρημένος στην βάση – δηλαδή δεν τον γνωρίζει το πρόγραμμα – δεν θα ανιχνευθεί με αποτέλεσμα να δώσει ένα λανθασμένο αίσθημα ασφάλειας στον χρήστη.

Οι κατασκευαστές τέτοιων προγραμμάτων αντιμετωπίζουν αυτό το πρόβλημα με την συνεχόμενη παραγωγή πρόσθετων συμπληρωμάτων (updates) για τα προγράμματα τους. Αυτά τα updates "μαθαίνουν" στα αντι-ικά προγράμματα πώς να αναγνωρίζουν τους νέους ιούς που παράγονται καθημερινά. Έτσι ο χρήστης θα πρέπει να τα προμηθεύεται σε μια τακτική βάση.

Υπάρχουν πολλές εταιρίες που δραστηριοποιούνται σε αυτό τον τομέα με το πρόγραμμα της κάθε μιας να κάνει σχεδόν παρόμοια δουλειά: Symantec's Norton Antivirus, McAfee ViruScan, Panda Software, Data Fellows F-PROT, Trend Micro, Computer Associates' Inoculan κ.α.

4.6 ΕΠΙΛΟΓΟΣ

Στην τεχνολογική εποχή που ζούμε, η σημασία της ασφάλειας των ηλεκτρονικών υπολογιστών και δικτύων είναι μέγιστη για τα προσωπικά δεδομένα του καθημερινού ανθρώπου.

Πρώτων, ένα μεγάλο μέρος των προσωπικών μιας πληροφοριών είναι αποθηκευμένο σε υπολογιστές. Αν αυτοί οι υπολογιστές δεν είναι ασφαλείς από περίεργα μάτια, τότε ούτε και τα δεδομένα που περιέχουν είναι (όπως, τραπεζικοί λογαριασμοί, στοιχεία κατόχων πιστωτικών καρτών).

Οι άνθρωποι αποτελούν ένα πολύ μεγάλο μέρος του προβλήματος αλλά και της λύσης. Η κατάσταση που επικρατεί στο χώρο της ασφάλειας των πληροφοριακών συστημάτων και των δικτύων σίγουρα θα αλλάξει με τη πάροδο του χρόνου ως προς το καλύτερο. Είναι όμως σίγουρο ότι η απόλυτη ασφάλεια είναι δυνατόν να μην υπάρξει ποτέ.

Η ασφάλεια των υπολογιστών και των δικτύων είναι τόσο σημαντική όσο σημαντικά ήταν και τα τείχη για τις πόλεις μια χιλιετηρίδα πριν.

4.7 ΕΡΕΥΝΑ ΓΙΑ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Σύμφωνα με μια πρόσφατη έρευνα που πραγματοποιήθηκε από το Capgemini and Chartered Institute of Purchasing and Supply (CIPS) στις Ηνωμένες Πολιτείες Αμερικής έδειξε μια σημαντική αύξηση στον αριθμό των εταιριών που τα τελευταία τέσσερα χρόνια χρησιμοποίησαν το Internet για αγορές ή πωλήσεις, αλλά φαίνεται ότι περισσότερο επωφελούνται οι μεγάλες επιχειρήσεις. Το 39% των επιχειρήσεων που απασχολούν περισσότερους από 500 υπαλλήλους παρατήρησε μια μείωση στα

έξοδα λόγω του ηλεκτρονικού εμπορίου ενώ το αντίστοιχο ποσοστό σε επιχειρήσεις με λιγότερους από 100 υπαλλήλους είναι 11,7%. Το ηλεκτρονικό εμπόριο είναι ιδιαιτέρως δημοφιλές για υπηρεσίες (κυρίως ταξιδιωτικές) που αποτελούν το 73% των συνολικών πωλήσεων ενώ η αγορά αγαθών αποτελεί μόλις το 20%. [61]

ΠΑΡΑΡΤΗΜΑ Α

ΑΚΡΩΝΥΜΙΑ

A

AES = Advanced Encryption Standard

B

B2B = Business to Business (Συναλλαγές μεταξύ επιχειρήσεων)

B2C = Business to Consumer (Συναλλαγές μεταξύ επιχειρήσεων και πελατών)

B2G = Business to Government (Συναλλαγές μεταξύ επιχειρήσεων και Κυβέρνησης)

C

CA = Certification Authorities (Αρχές Πιστοποίησης)

C2C = Consumer to Consumer (Συναλλαγές μεταξύ πελατών)

D

DES = Data Encryption Algorithm

DSS = Digital Signature Standard

E

E-Cat = Electronic Catalogue (Ηλεκτρονικός Κατάλογος)

EDI = Electronic Data Interchange (Ηλεκτρονική Ανταλλαγή Δεδομένων)

EDM = Electronic Documents Management (Ηλεκτρονική Διαχείριση Εγγράφων)

E-Forms = Electronic Forms (Ηλεκτρονικές Φόρμες)

EFT = Electronic Funds Transfer (Ηλεκτρονική Μεταφορά Κεφαλαίων)

E-mail = Electronic mail (Ηλεκτρονικό Ταχυδρομείο)

G

G2C = Government to Citizen (Συναλλαγές μεταξύ Κυβέρνησης και Πολιτών)

H

HMAC = Hashed Message Authentication Code

I

IDEA = International Data Encryption Algorithm

M

MD = Message Digest

P

PKI = Public Key Infrastructure

S

SET = Secure Electronic Transaction (Ασφάλεια Ηλεκτρονικών Συναλλαγών)

SHA = Secure Hash Function

S-HTTP = Secure Hyper Text Transfer Protocol (Ασφαλής Μεταφορά Υπερ Κειμένου)

SSL = Secure Sockets Layer

ΛΕΞΙΚΟ

A

Authentication = Αυθεντικότητα

Authorization = Εξουσιοδότηση

C

Cipher text = Κρυπτογραφημένο κείμενο

Confidentiality = Εμπιστευτικότητα

Cryptanalysis Attack = Επίθεση κρυπτανάλυσης

F

Factoring Attacks = Επίθεση παραγοντοποίησης

Firewall = Πύρινος Τοίχος

I

Integrity = Ακεραιότητα

K

Key Search Attack = Επίθεση αναζήτησης κλειδιού

N

Non – Repudiation = Μη αποποίηση της ευθύνης

P

Plain text = Καθαρό κείμενο (μη κρυπτογραφημένο)

S

System-bases Attacks = Επίθεση βασισμένη στο σύστημα κρυπτογράφησης

T

Trusted Third Party = Έμπιστη Τρίτη Οντότητα

Trojan Horses = Δούρειοι Ίπποι

V

Viruses = Ιοί

W

Worms = Σκουλήκια

ΠΑΡΑΡΤΗΜΑ Β

ΗΛΕΚΤΡΟΝΙΚΕΣ ΔΙΕΥΘΥΝΣΕΙΣ

Δε θα ήταν δυνατόν να πραγματοποιηθεί αυτή η πτυχιακή εργασία χωρίς την εκτενή αξιοποίηση των δυνατοτήτων του Διαδικτύου, τουλάχιστον στην μορφή που κατέληξε αυτή. Χρησιμοποιήθηκε ένας τεράστιος αριθμός από white papers, παρουσιάσεις κ.λ.π. Δεκάδες από αυτά μελετήθηκαν με προσοχή και καλύφθηκαν αρκετές απορίες σε συγκεκριμένα θέματα. Με απλή αναζήτηση στο Διαδίκτυο κανείς θα πέσει πάνω τους. Γι' αυτό, εδώ παρατίθενται μόνο μερικά πολύ ενδιαφέροντα.

- http://ebusinessforum.gr
- http://go-online.gr
- http://cert.com
- http://rsa.com
- http://www.getnetwise.org
- http://www.securityfocus.com
- http://www.trendmicro.com

ΒΙΒΛΙΟΓΡΑΦΙΑ

- **Handbook of Applied Cryptography**, A. Menezes, P. Oorschot and S. Vanstone, CRC Press
- **Δίκτυα υπολογιστών**, Andrew Tanenbaum, Παπασωτηρίου
- **Δελτίον Ένωσης Ελληνικών Τραπεζών (1928 - 2002) – Αφιέρωμα στο Internet Banking**, [Τεύχος: Ιούλιος – Αύγουστος – Σεπτέμβριος 2003, αριθμός:34], Γ. Αρώνης, Ν. Παυλίδης, Α. Τσάμης, Δ. Γεωργόπουλος, Κ. Γιαννακοπούλου
- **RAM** (μηνιαίο περιοδικό υπολογιστών), [Μάιος 2004, Τεύχος: 180], σελίδες 78 – 98

ΠΗΓΕΣ ΑΝΑΦΟΡΑΣ

[1] **Ε-επιχειρείν** (Κεφάλαιο 1°, σελ. 3), ΤΜΗΜΥΠ – Πανεπιστήμιο Πατρών

[2] **Ηλεκτρονικό Εμπόριο** (Κεφάλαιο 1°, σελ. 4 – 5), Βενάκης Περικλής – Καζαντζή Αθανασία – Κούρουπας Γεώργιος

[3] **Ηλεκτρονικό Εμπόριο** (Κεφάλαιο 1°, σελ. 7), Βενάκης Περικλής – Καζαντζή Αθανασία – Κούρουπας Γεώργιος

[4] **Ηλεκτρονικό Εμπόριο** (Κεφάλαιο 1°, σελ. 7), Βενάκης Περικλής – Καζαντζή Αθανασία – Κούρουπας Γεώργιος

[5] **Ε-επιχειρείν** (Κεφάλαιο 1°, σελ. 3), ΤΜΗΜΥΠ – Πανεπιστήμιο Πατρών

[6] **Handbook of Applied Cryptography** (Chapter 1°, p. 4), A. Menezes – P. Oorschot – S. Vanstone

[7] **Ασφάλεια Διαδικτυακής Διακίνησης Πληροφοριών** (Κεφάλαιο 1°, σελ. 1), Γκαδόλος Ιωάννης

[8] **Ηλεκτρονικό Εμπόριο (Κεφάλαιο 3°, σελ. 12 – 13), Βενάκης Περικλής – Καζαντζή Αθανασία** – Κούρουπας Γεώργιος

[9] **Ασφάλεια Διαδικτυακής Διακίνησης Πληροφοριών** (Κεφάλαιο 1°, σελ. 1), Γκαδόλος Ιωάννης

[10] **Ε-επιχειρείν** (Κεφάλαιο 5°, σελ. 11 – 13), ΤΜΗΜΥΠ – Πανεπιστήμιο Πατρών

[11] **Ασφάλεια Διαδικτυακής Διακίνησης Πληροφοριών** (Κεφάλαιο 1°, σελ. 5), Γκαδόλος Ιωάννης

[12] **Ασφάλεια στο Ηλεκτρονικό Εμπόριο** (σελ. 33 – 35), Θρήσκου Χρυσάνθη – Μήλιου Αικατερίνη

[13] **Ηλεκτρονικό Εμπόριο** (Κεφάλαιο 3°, σελ. 13 – 15), Βενάκης Περικλής – Καζαντζή Αθανασία – Κούρουπας Γεώργιος

[14] **Encryption and Security Tutorial**, Peter Gutmann (http://www.cs.aukland.nz/~pgut001)

[15] **An Overview of Cryptography**, Gary C. Kessler

[16] **Ε-επιχειρείν** (Κεφάλαιο 5°, σελ. 11 – 13), ΤΜΗΜΥΠ – Πανεπιστήμιο Πατρών

[17] **Ασφάλεια Διαδικτυακής Διακίνησης Πληροφοριών** (Κεφάλαιο 1°, σελ. 5), Γκαδόλος Ιωάννης

[18] **Ηλεκτρονική Διακίνηση αγαθών και Κρυπτογραφία**, Α. Βασιλακόπουλος

– Δ. Γούτας, PeLab – Τμ. Η. Υ. Σ. – ΤΕΙ ΠΕΙΡΑΙΑ: Μάρτιος 1998

[19] **Ασφάλεια στο Ηλεκτρονικό Εμπόριο** (σελ. 33 – 35), Θρήσκου Χρυσάνθη – Μήλιου Αικατερίνη

[20] **Ηλεκτρονικό Εμπόριο** (Κεφάλαιο 3°, σελ. 13 – 15), Βενάκης Περικλής – Καζαντζή Αθανασία – Κούρουπας Γεώργιος

[21] **Encryption and Security Tutorial**, Peter Gutmann (http://www.cs.aukland.nz/~pgut001)

[22] **An Overview of Cryptography**, Gary C. Kessler

[23] N = αριθμός χρηστών
2N = ασύμμετρη κρυπτογραφία
N*(N-1)/2 = συμμετρική κρυπτογραφία

Για N = 4, τότε 2N = 8 και N*(N-1)/2 = 6 (μοιράζονται λιγότερα κλειδιά στην συμμετρική κρυπτογραφία)
Για N = 5, τότε 2N = 10 και N*(N-1)/2 = 10 (δεν υπάρχει διαφορά)
Για N = 6, τότε 2N = 12 και N*(N-1)/2 = 15 (μοιράζονται λιγότερα κλειδιά στην ασύμμετρη κρυπτογραφία)
Για N = 100, τότε 2N = 200 και N*(N-1)/2 = 5000 (υπάρχει μεγάλη διαφορά)

[24] **Handbook of Applied Cryptography** (Chapter 7°, p. 223 – 266), A. Menezes – P. Oorschot – S. Vanstone

[25] **Handbook of Applied Cryptography** (Chapter 6°, p. 191 – 212), A. Menezes – P. Oorschot – S. Vanstone

[26] **Introduction to Modern Cryptography**, Lecture 2, Symmetric Encryption: Stream and Block Ciphers

[27] **Ασφάλεια στο Ηλεκτρονικό Εμπόριο** (σελ. 33 – 35), Θρήσκου Χρυσάνθη – Μήλιου Αικατερίνη

[28] **Ε-επιχειρείν** (Κεφάλαιο 5°, σελ. 11 – 13), ΤΜΗΜΥΠ – Πανεπιστήμιο Πατρών

[29] **Ασφάλεια Διαδικτυακής Διακίνησης Πληροφοριών** (Κεφάλαιο 1°, σελ. 5), Γκαδόλος Ιωάννης

[30] **Handbook of Applied Cryptography** (Chapter 8°, p. 283 – 294), A. Menezes – P. Oorschot – S. Vanstone

[31] **Encryption and Security: The Data Encryption Standard**, Stuart Allman – Cypress Semiconductor

[32] **Advanced Encryption Standard (AES)**, Cisco IOS Release 12.2 (13)

[33] **AES Encryption (FIPS-197) – Advanced Encryption Standard**, 2003 VOCAL Technologies, Ltd. (http://www.vocal.com)

[34] **Encryption and Security Tutorial**, Peter Gutmann (http://www.cs.aukland.nz/~pgut001)

[35] **Encryption Technologies Compared (A primer on Basic Cryptography Methods)**, David Garrett

[36] **The RC5 Encryption Algorithm**, Ronald L. Rivest

[37] **An Overview of Cryptography**, Gary C. Kessler

[38] **Ασφάλεια Διαδικτυακής Διακίνησης Πληροφοριών** (Κεφάλαιο 1°, σελ. 8 – 12), Γκαδόλος Ιωάννης
[39] **Encryption Technologies Compared (A primer on Basic Cryptography Methods)**, David Garrett
[40] **Handbook of Applied Cryptography** (Chapter 8°, p. 283 – 294), A. Menezes – P. Oorschot – S. Vanstone

[41] **Ασφάλεια Διαδικτυακής Διακίνησης Πληροφοριών** (Κεφάλαιο 1°, σελ. 8 – 12), Γκαδόλος Ιωάννης
[42] **Encryption Technologies Compared (A primer on Basic Cryptography Methods)**, David Garrett
[43] **Handbook of Applied Cryptography** (Chapter 8°, p. 283 – 294), A. Menezes – P. Oorschot – S. Vanstone

[44] **VLSI Implementation of the keyed – hash message authentication code for the wireless application protocol**, G. Selemis – N. Sklavos – O. Koufopavlou
[45] **Hashing and Message Authentication Codes**, Andreas Klappenecker
[46] **T-79.159 Cryptography and Data Security**, Lecture 4: Hashes and Message Digests, Markku-Juhani O. Saarinen

[47] **Analysis of SHA-1 in Encryption Mode** (Lecture Notes in Computer Science), Helen Handschuh – Lars Knudsen – Matthew Robshaw

[48] **Ηλεκτρονικές Υπογραφές και Ηλεκτρονικά Πιστοποιητικά Ταυτοποίησης** (Μέρος 2°, σελ. 9), Δ. Ματράκος – Ν. Κύρογλου – Α. Μητράκας
[49] **Digital Signatures and Trusted Third Parties**, N. Κύρογλου
[50] **Ψηφιακές Υπογραφές: Διεθνής εμπειρία, τάσεις και προοπτικές**, Στ. Γκρίτζαλής
[51] **Ο δεκάλογος για τις ηλεκτρονικές υπογραφές και τα ηλεκτρονικά πιστοποιητικά ταυτοποίησης**, E-Businessforum
[52] **Ασφάλεια στο Ηλεκτρονικό Εμπόριο** (Κεφάλαιο 3°, σελ. 77 – 83), Χρ. Γεωργιάδης
[53] **Ο ρόλος της Υποδομής Δημόσιου Κλειδιού στην ανάπτυξη ηλεκτρονικών αγορών**, Σωκράτης Κ. Κάτσικας
[54] **E-Business και Προστασία Προσωπικών Δεδομένων: Σεβασμός στον πολίτη στην Ψηφιακή Υπογραφή**, Κ. Μουλίνος – Κ. Καμπουράκη

[55] **Objected Oriented Realization of an Information System – Seminar Project (WS 1999 – 2000)**, Aiman Abu-Msameh – Muthana Al-Temimi – Ronaldo Armuelles
[56] **SSL: Theory and Practice**, Zeus Technology (June 2000, Version 1.0)

[57] **Ασφάλεια Διαδικτυακής Διακίνησης Πληροφοριών** (Κεφάλαιο 2°, σελ. 22), Γκαδόλος Ιωάννης

[58] **Ηλεκτρονικό Εμπόριο** (Κεφάλαιο 3°, σελ. 22), Βενάκης Περικλής – Καζαντζή Αθανασία – Κούρουπας Γεώργιος

[59] **Ασφάλεια στο Ηλεκτρονικό Εμπόριο** (Κεφάλαιο 3°, σελ. 4), Σαραπάρης Σωτήριος

[60] **Δελτίον Ένωσης Ελληνικών Τραπεζών (1928 - 2002) – Αφιέρωμα στο Internet Banking**, [Τεύχος: Ιούλιος – Αύγουστος – Σεπτέμβριος 2003, αριθμός:34], Γ. Αρώνης, Ν. Παυλίδης, Α. Τσάμης, Δ. Γεωργόπουλος, Κ. Γιαννακοπούλου

[61] http://www.e-businessforum.gr