ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΣΥΜΜΕΤΡΙΚΗ ΚΑΙ ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΗ: ΧΡΙΣΤΟΦΟΡΟΣ ΜΑΓΚΑΦΑΣ
ΕΠΟΠΤΕΥΟΥΣΑ ΚΑΘΗΓΗΤΡΙΑ: ΑΛΕΚΑ ΚΑΛΑΠΟΔΗ

ΠΑΤΡΑ 2013

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω θερμά την κυρία Αλέκα Καλαπόδη για την συνεργασία μας ώστε να υλοποιηθεί η παρούσα εργασία, για την προθυμία και την πολύτιμη βοήθειά της σε οτιδήποτε χρειάστηκα. Επίσης ένα μεγάλο ευχαριστώ στον καθηγητή μου Ιωάννη Κουτσονίκο για την μεγάλη προσφορά του στη σχολή μου καθώς και στους αξιόλογους καθηγητές που γνώρισα κατα τη διάρκεια των σπουδών μου. Επίσης, ευχαριστώ τους γονείς μου, τον αδερφό μου, τη Χριστίνα και τους φίλους μου.

ΠΡΟΛΟΓΟΣ

Η εποχή στην οποία βρισκόμαστε και τα πάντα γύρω μας αλλάζουν με ραγδαία ταχύτητα. Οι νέες τεχνολογίες καλύπτουν ολοένα και μεγαλύτερο μέρος τόσο της εργασιακής όσο και της καθημερινής μας ζωής. Ο σύγχρονος άνθρωπος προσπαθεί να προσαρμοστεί στο καινούριο, το νέο, το σύγχρονο που συνεχώς μεταβάλλεται. Η τεχνολογία και οι ηλεκτρονικοί υπολογιστές εξελίσσονται ραγδαία. Αρχικά οι ηλεκτρονικοί υπολογιστές ήταν μεγάλα υπολογιστικά συστημάτων τύπου Main Frame τα οποία έδωσαν τη σειρά τους σε μικρότερα, μόνο για επαγγελματική χρήση. Έπειτα, έκαναν την εμφάνιση τους οι προσωπικοί υπολογιστές οι οποίοι εισέβαλαν με γοργούς ρυθμούς τόσο στην εργασία όσο και σε κάθε σπίτι. Σήμερα, διανύουμε την εποχή της δικτύωσης και της διασύνδεσης των υπολογιστικών συστημάτων σε παγκόσμιο επίπεδο.

Η ψηφιοποίηση της πληροφορίας και η διάχυση της μέσω των ηλεκτρονικών δικτύων στον τελικό χρήστη την καθιστά ως το σημαντικότερο συστατικό στοιχείο του νέου μοντέλου κοινωνικής και οικονομικής οργάνωσης. Για το λόγο αυτό, στη σημερινή εποχή, οι βασικότερες προτεραιότητες που τίθενται αφορούν στην ασφάλεια και στην ταχύτητα των ηλεκτρονικών διόδων και μέσων μεταφοράς της πληροφορίας με σκοπό την βέλτιστη διαχείριση, την δυναμική επεξεργασία και την άρτια μετάδοσή της.

Σε οικονομικό και κατ’επέκταση επιχειρηματικό επίπεδο, η πληροφορία αποκτά πλέον άλλες διαστάσεις, καθώς είναι απαλλαγμένη από γεωγραφικούς και χρονικούς περιορισμούς και έχει αναχθεί σε ένα εμπορικό προϊόν, με παραγωγούς, διακινητές και καταναλωτές. Υπό αυτήν την έννοια υπάγεται στους νόμους της προσφοράς και της ζήτησης. Στις μέρες μας, το ηλεκτρονικό εμπόριο αποτελεί αναπόσπαστο κομμάτι του παγκοσμίου εμπορίου. Για πολλούς θεωρείται ίσως η δεύτερη μεγαλύτερη τεχνολογική εξέλιξη μετά τη βιομηχανική επανάσταση, καθώς εξοικονομεί χρόνο και χρήμα και μπορεί να μεταμορφώσει μια μικρή εταιρεία ακόμα και σε κολοσσό. Το ηλεκτρονικό εμπόριο περιλαμβάνει τη συνδιαλλαγή είτε μεταξύ επιχείρησης και καταναλωτή, είτε μεταξύ επιχειρήσεων, είτε μεταξύ των δημόσιων φορέων και των πολιτών (επιχειρηματίες ή μη), δίνοντας τη δυνατότητα πληροφόρησης, ανταλλαγής πληροφοριών και διεκπεραίωσης συναλλαγών.

Η ανάγκη για τη δημιουργία ασφαλών διαύλων για το απόρρητο των επικοινωνιών και των παράνομων ψηφιακών δεδομένων δημιουργεί την ανάγκη αξιόπιστων και ασφαλών μεθόδων για την απόκρυψη δεδομένων, την προστασία και τον έλεγχο τους καθώς και τη διασφάλιση των δικαιωμάτων πνευματικής ιδιοκτησίας. Έτσι, η νέα ψηφιακή κοινωνία οφείλει και είναι επιτακτική ανάγκη να παρέχει μηχανισμούς προστασίας για το απαραβίαστο του επαγγελματικού και προσωπικού απορρήτου. Βασική τεχνολογία στον τομέα της ασφάλειας για την επίτευξη των στόχων αυτών είναι η κρυπτογράφηση.

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία έχει ως θέμα την συμμετρική και ασύμμετρη κρυπτογράφηση. Αρχικά γίνεται αναδρομή στην ιστορία της κρυπτογραφίας από τις προϊστορικές γραφές μέχρι και σήμερα. Ακολουθεί η παρουσίαση των βασικών εννοιών της καθώς και των κρυπτοσυστημάτων με τα οποία υλοποιείται. Τονίζεται ο σκοπός και οι μέθοδοι της κρυπτογραφίας οι οποίοι καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Έπειτα, παρουσιάζεται αναλυτικά ο τρόπος λειτουργίας της συμμετρικής και ασύμμετρης κρυπτογράφησης και πραγματοποιείται σύγκριση των πλεονεκτημάτων και μειωνεκτημάτων τους. Περιγράφονται τα είδη και τα βασικά χαρακτηριστικά των αντίστοιχων κρυπτογραφικών αλγορίθμων. Επίσης, αναφορά γίνεται στις ψηφιακές υπογραφές, στα ψηφιακά πιστοποιητικά και την υβριδική κρυπτογραφία ψηφιακού φακέλου για επίτευξη ασφαλούς επικοινωνίας μεταξύ δύο μερών. Τέλος, παρουσιάζονται οι βασικοί τομείς στους οποίους βρίσκει εφαρμογή η κρυπτογράφηση και αναλύεται ενδεικτικά η διαδικασία των τραπεζικών συναλλαγών μέσω ATM, οι έξυπνες κάρτες και η ηλεκτρονική δημοπρασία.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1

ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Στο κεφάλαιο αυτό παρουσιάζεται η διαχρονική εξέλιξη της κρυπτογραφίας καθώς και τα στάδια στα οποία κατατάσσεται ανάλογα με την ιστορική καταγραφή και τις μεθόδους υλοποίησής της.
Για το κεφάλαιο αυτό χρησιμοποιήθηκαν στοιχεία από τις πηγές [2], [11].

1.1 Η ιστορία της κρυπτογραφίας

Οι προσπάθειες για την διατήρηση της μυστικότητας εμφανίζεται από τη γέννηση της ανθρωπότητας. Η κρυπτογραφία προέκυψε ως ιδεολογική προσέγγιση και έννοια σχεδόν από την επινόηση της γραφής. Η ιστορία της κρυπτογραφίας μπορεί κατά προσέγγιση να διαιρεθεί σε τρία στάδια.

Στο πρώτο στάδιο οι διαδικασίες κρυπτογράφησης αφορούσαν τον τρόπο της έντυπης απεικόνισης (μελάνι και χαρτί) και εντάσσονται χρονολογικά στην περίοδο 1900 π.Χ. – 1900 μ.Χ.

Στο δεύτερο στάδιο κυριαρχεί η εμφάνιση των κρυπτογραφικών μηχανών, ιδίως την περίοδο του Β’ παγκοσμίου πολέμου και την δημιουργία της μηχανής Enigma. Το στάδιο αυτό εντάσσεται χρονολογικά στην περίοδο 1900 μ.Χ. – 1950 μ.Χ.

Στο τρίτο στάδιο υπάγεται το σύγχρονο κρυπτογραφικό σύστημα το οποίο είναι απόρροια της αμοιβαίας αλληλεπίδρασης των μαθηματικών και των ηλεκτρονικών υπολογιστών. Τα μαθηματικά προσέφεραν τον σχεδιασμό και οι ηλεκτρονικοί υπολογιστές επέτρεψαν τη χρήση περίπλοκων αλγορίθμων κρυπτογράφησης. Το σύγχρονο κρυπτογραφικό σύστημα εντάσεται χρονολογικά στην περίοδο 1950 μ.Χ. – Σήμερα.

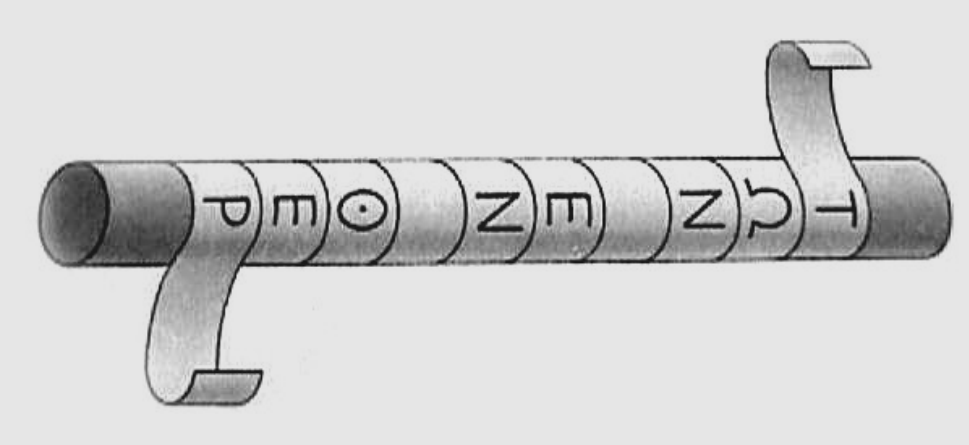
1.2 Πρώτο στάδιο κρυπτογραφίας

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

Όπως προκύπτει από μία μικρή σφηνοειδή επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, οι πολιτισμοί που αναπτύχθηκαν στη Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία ήδη από το 1500 π.Χ. Η επιγραφή αυτή περιγράφει μία μέθοδο κατασκευής σμάλτων για αγγειοπλαστική και θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο (με βάση τον Kahn). Επίσης, ως το αρχαιότερο βιβλίο κρυπτοκωδικών στον κόσμο, θεωρείται μία σφηνοειδής επιγραφή στα Σούσα της Περσίας. η οποία περιλαμβάνει τους αριθμούς 1 έως 8

και από το 32 έως το 35, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καθένα σφηνοειδή σύμβολα.

Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Γύρω στον 5ο π.Χ. αιώνα εφηύραν την «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποίησαν για την κρυπτογράφηση τη μέθοδο της μετάθεσης. Όπως αναφέρει ο Πλούταρχος, η «Σπαρτιατική Σκυτάλη» , ήταν μια ξύλινη ράβδος, ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα, όταν δε ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της αναδιάταξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης (Εικόνα 1).



Εικόνα 1: Η Σπαρτιατική Σκυτάλη

Στην αρχαιότητα χρησιμοποιήθηκαν κυρίως συστήματα, τα οποία βασίζονταν στη στεγανογραφία και όχι τόσο στην κρυπτογραφία. Οι Έλληνες συγγραφείς δεν αναφέρουν αν και πότε χρησιμοποιήθηκαν συστήματα γραπτής αντικατάστασης γραμμάτων, αλλά τα βρίσκουμε στους Ρωμαίους, κυρίως την εποχή του Ιουλίου Καίσαρα. Ο Ιούλιος Καίσαρας έγραφε στον Κικέρωνα και σε άλλους φίλους του, αντικαθιστώντας τα γράμματα του κειμένου, με γράμματα, που βρίσκονται 3 θέσεις μετά, στο Λατινικό Αλφάβητο. Έτσι, σήμερα, το σύστημα κρυπτογράφησης που στηρίζεται στην αντικατάσταση των γραμμάτων του αλφαβήτου με άλλα που βρίσκονται σε καθορισμένο αριθμό θέσης πριν ή μετά, λέγεται κρυπτοσύστημα αντικατάστασης του Καίσαρα. Ο Καίσαρας χρησιμοποίησε και άλλα, πιο πολύπλοκα συστήματα κρυπτογράφησης, για τα οποία έγραψε ένα βιβλίο ο Valerius Probus, το οποίο δυστυχώς δεν διασώθηκε, αλλά αν και χαμένο, θεωρείται το πρώτο βιβλίο κρυπτολογίας. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες.

Στη διάρκεια του Μεσαίωνα, η κρυπτολογία ήταν κάτι το απαγορευμένο και αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας, κάτι που συντέλεσε στην καθυστέρηση της ανάπτυξης της. Η εξέλιξη, τόσο της κρυπτολογίας, όπως και των μαθηματικών, συνεχίζεται στον Αραβικό κόσμο. Στο γνωστό μυθιστόρημα «Χίλιες και μία νύχτες» κυριαρχούν οι λέξεις-αινίγματα, οι γρίφοι, τα λογοπαίγνια και οι αναγραμματισμοί. Έτσι, εμφανίστηκαν βιβλία που περιείχαν κρυπταλφάβητα, όπως το αλφάβητο «Dawoudi» που πήρε το όνομα του από τον βασιλιά Δαυίδ. Οι Άραβες είναι οι πρώτοι που επινόησαν αλλά και χρησιμοποίησαν μεθόδους κρυπτανάλυσης. Το κυριότερο εργαλείο στην κρυπτανάλυση, η χρησιμοποίηση των συχνοτήτων των γραμμάτων κειμένου, σε συνδυασμό με τις συχνότητες εμφάνισης στα

κείμενα των γραμμάτων της γλώσσας, επινοήθηκε από αυτούς γύρω στον 14ο αιώνα. Η κρυπτογραφία, λόγω των στρατιωτικών εξελίξεων, σημείωσε σημαντική ανάπτυξη στους επόμενους αιώνες. Ο Ιταλός Giovanni Batista Porta, το 1563, δημοσίευσε το περίφημο για την κρυπτολογία βιβλίο «De furtivis literarum notis», με το οποίο έγιναν γνωστά τα πολυαλφαβητικά συστήματα κρυπτογράφησης και τα διγραφικά κρυπτογραφήματα, στα οποία, δύο γράμματα αντικαθίστανται από ένα. Σημαντικός εκπρόσωπος εκείνης της εποχής είναι και ο Γάλλος Vigenere, του οποίου ο πίνακας πολυαλφαβητικής αντικατάστασης, χρησιμοποιείται ακόμη και σήμερα.

Ο C.Wheatstone, γνωστός από τις μελέτες του στον ηλεκτρισμό, παρουσίασε την πρώτη μηχανική κρυπτοσυσκευή, η οποία απετέλεσε τη βάση για την ανάπτυξη των κρυπτομηχανών της δεύτερης ιστορικής περιόδου της κρυπτογραφίας. Η μεγαλύτερη αποκρυπτογράφηση ήταν αυτή των αιγυπτιακών ιερογλυφικών τα οποία, επί αιώνες, παρέμεναν μυστήριο και οι αρχαιολόγοι μόνο εικασίες μπορούσαν να διατυπώσουν για τη σημασία τους. Ωστόσο, χάρη σε μία κρυπταναλυτική εργασία, τα ιερογλυφικά εν τέλει αναλύθηκαν και έκτοτε οι αρχαιολόγοι είναι σε θέση να διαβάζουν ιστορικές επιγραφές. Τα αρχαιότερα ιερογλυφικά χρονολογούνται περίπου από το 3000 π.Χ. Τα σύμβολα των ιερογλυφικών ήταν υπερβολικά πολύπλοκα για την καταγραφή των συναλλαγών εκείνης της εποχής. Έτσι, παράλληλα με αυτά, αναπτύχθηκε για καθημερινή χρήση η ιερατική γραφή, που ήταν μία συλλογή συμβόλων, τα οποία ήταν εύκολα τόσο στο γράψιμο όσο και στην ανάγνωση. Τον 17ο αιώνα αναθερμάνθηκε το ενδιαφέρον για την αποκρυπτογράφηση των ιερογλυφικών, έτσι το 1652 ο Γερμανός Ιησουΐτης Αθανάσιος Κίρχερ εξέδωσε ένα λεξικό ερμηνείας τους, με τίτλο «Oedipus Aegyptiacus». Με βάση αυτό προσπάθησε να ερμηνεύσει τις αιγυπτιακές γραφές, αλλά η προσπάθεια του αυτή ήταν κατά γενική ομολογία αποτυχημένη. Για παράδειγμα, το όνομα του Φαραώ Απρίη, το ερμήνευσε σαν «τα ευεργετήματα του θεϊκού Όσιρι εξασφαλίζονται μέσω των ιερών τελετών της αλυσίδας των πνευμάτων, ώστε να επιδαψιλεύσουν τα δώρα του Νείλου». Παρόλα αυτά, η προσπάθεια του άνοιξε τον δρόμο προς τη σωστή ερμηνεία των ιερογλυφικών, που προχώρησε χάρη στην ανακάλυψη της «Στήλης της Ροζέτας». Ήταν μια πέτρινη στήλη που βρήκαν τα στρατεύματα του Ναπολέοντα στην Αίγυπτο και είχε χαραγμένο πάνω της το ίδιο κείμενο τρεις φορές. Μια με ιερογλυφικά, μια στα ελληνικά και μια στην ιερατική γραφή. Δύο μεγάλοι αποκρυπτογράφοι της εποχής, ο Γιάνγκ και ο Σαμπολιόν, μοιράστηκαν τη δόξα της ερμηνείας τους.

1.3 Προϊστορικές γραφές και κρυπτογραφία

Οι προϊστορικοί πληθυσμοί χρησιμοποίησαν τρεις γραφές μέχρι να επινοήσουν αλφάβητο, γύρω στο 850 π.Χ. Οι γραφές αυτές αποτέλεσαν ουσιαστικά ένα είδος κρυπτογραφικών κειμένων. Χρονολογικά κατατάσσονται ως εξής:

1) 3000 - 1600 π.Χ. : Εικονογραφική (Ιερογλυφική) γραφή
2) 1850 - 1450 π.Χ.: Γραμμική γραφή Α
3) 1450 - 1200 π.Χ.: Γραμμική Γραφή Β

Η Κρητική εικονογραφική ή ιερογλυφική γραφή, δεν μας έχει αποκαλύψει τον κώδικα της, γνωρίζουμε ωστόσο ότι δεν πρόκειται για γραφή που χρησιμοποιεί εικόνες ως σημεία, αλλά για φωνητική γραφή, η οποία εξαντλείται σε περίπου διακόσιους σφραγιδόλιθους και συνυπήρχε με τη γραμμική γραφή Α, τόσο χρονικά όσο και τοπικά, όπως προκύπτει από τις ανασκαφές στο ανάκτορο των Μαλίων της Κρήτης. Εμφανίζεται στον Δίσκο της Φαιστού

(Εικόνα 2), που ανακαλύφθηκε το 1908 στη νότια Κρήτη και σε άλλα αντικείμενα όπως σφραγίδες και πέλεκεις. Ο δίσκος της Φαιστού είναι μια κυκλική πινακίδα, που χρονολογείται γύρω στο 1700 π.Χ. και φέρει γραφή με τη μορφή δύο σπειρών. Τα σύμβολα δεν είναι χειροποίητα, αλλά έχουν χαραχθεί με τη βοήθεια μίας ποικιλίας σφραγίδων, καθιστώντας τον Δίσκο ως το αρχαιότερο δείγμα στοιχειοθεσίας. Δεν υπάρχει άλλο ανάλογο εύρημα και έτσι η αποκρυπτογράφηση στηρίζεται σε πολύ περιορισμένες πληροφορίες. Μέχρι σήμερα δεν έχει αποκρυπτογραφηθεί και παραμένει η πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή.

Εικόνα 2: Ο δίσκος της Φαιστού

Οι πρώτες επιγραφές με Γραμμική γραφή ανακαλύφθηκαν από τον Άρθουρ Έβανς (Sir Arthur Evans), τον μεγάλο Άγγλο αρχαιολόγο, που ανάσκαψε συστηματικά την Κνωσό το 1900. Ο ίδιος ονόμασε αυτή τη γραφή γραμμική, επειδή τα γράμματα της είναι γραμμές (ένα γραμμικό σχήμα) και όχι σφήνες, όπως στη σφηνοειδή γραφή ή εικόνες όντων, όπως στην αιγυπτιακή ιερατική. Η γραμμική γραφή Α είναι μάλλον η γραφή των Μινωιτών (από το μυθικό Μίνωα, βασιλιά της Κνωσού), των κατοίκων της αρχαίας Κρήτης και από αυτή ίσως να προήλθε το σημερινό ελληνικό αλφάβητο. Τα γράμματα της γραμμικής γραφής χαράζονταν με αιχμηρό αντικείμενο πάνω σε πήλινες πλάκες, οι οποίες κατόπιν ξεραίνονταν σε φούρνους. Οι περισσότερες από τις επιγραφές με Γραμμική γραφή Α (περίπου 1500) είναι λογιστικές και περιέχουν εικόνες ή συντομογραφίες των εμπορεύσιμων προϊόντων και αριθμούς για υπόδειξη της ποσότητας ή οφειλής.

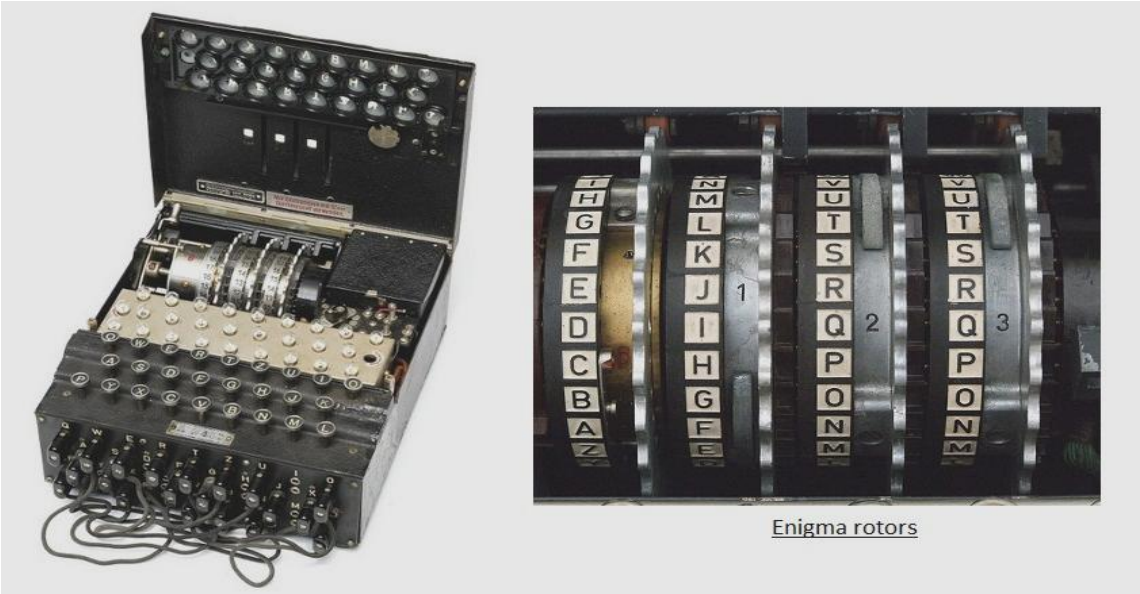
Ο Έβανς κατέγραψε 135 σύμβολα της. Χρησιμοποιήθηκε κυρίως στην Κρήτη, αν και ορισμένα πρόσφατα ευρήματα καταδεικνύουν ότι μπορεί να αποτέλεσε μέσο γραφής και

αλλού, αφού επιγραφές με Γραμμική Α έχουν βρεθεί στην Κνωσό και Φαιστό της Κρήτης, αλλά και στη Μήλο και τη Θήρα. Πλάκες με επιγραφές σε γραμμική Α, εκτίθενται στο Μουσείο Ηρακλείου. Παρά την πρόοδο που έχει σημειωθεί, η γραμμική γραφή Α δεν έχει αποκρυπτογραφηθεί ακόμη. Ο Evans έδωσε και την ονομασία στη Γραμμική Γραφή Β, επειδή αναγνώρισε ότι πρόκειται για συγγενική γραφή με τη γραμμική Α, πιο πρόσφατη ωστόσο και εξελιγμένη. Με βάση όσα γνωρίζουμε σήμερα, η γραφή αυτή υιοθετήθηκε αποκλειστικά για λογιστικούς σκοπούς. Πινακίδες χαραγμένες με τη γραμμική γραφή Β βρέθηκαν στην Κνωσό, στα Χανιά αλλά και στην Πύλο, τις Μυκήνες, τη Θήβα και την Τίρυνθα. Σήμερα αποτελούν ένα σύνολο 10.000 τεμαχίων. Τα σχήματα των πινακίδων της γραφής αυτής ποικίλουν, επικρατούν όμως οι φυλλοειδείς και «σελιδόσχημες», οι οποίες διαφέρουν ως προς τις διαστάσεις, ανάλογα με τις προτιμήσεις του κάθε γραφέα. Έπλαθαν πηλό σε σχήμα κυλίνδρου, τον τοποθετούσαν σε λεία επιφάνεια και την πίεζαν μέχρι να γίνει επίπεδη, επιμήκης και συμπαγής πινακίδα, σαφώς διαφοροποιημένη σε δύο επιφάνειες: μία επίπεδη λειασμένη, που επρόκειτο να αποτελέσει την κύρια γραφική επιφάνεια και μία κυρτή, που συνήθως έμενε άγραφη. Πολλές φορές, όταν τα κείμενα απαιτούσαν περισσότερες από μία πινακίδες, έχουμε τις αποκαλούμενες «ομάδες» ή «πολύπτυχα» πινακίδων, οι οποίες εμφανίζουν κοινά χαρακτηριστικά και ως προς την αποξήρανση και το μίγμα του πηλού και κυρίως, ως προς το γραφικό χαρακτήρα του ίδιου του γραφέα. Τα πολύπτυχα αυτά φυλάσσονταν σε αρχειοφυλακεία και ταξινομούνταν κατά θέματα σε ξύλινα κιβώτια. Για να γνωρίζει ο ενδιαφερόμενος το περιεχόμενο των καλαθιών, κυρίως, χρησιμοποιούσαν ετικέτες: ένα σφαιρίδιο πηλού, εντυπωμένο στην πρόσθια πλευρά, στο οποίο καταγράφονταν συνοπτικές πληροφορίες. Συστηματικά, με τη γραφή αυτή, με την οποία είχε πραγματικό πάθος, ασχολήθηκε ο Άγγλος αρχιτέκτονας και ερασιτέχνης αρχαιολόγος Μ. Βέντρις. Ήταν ο πρώτος που κατάλαβε ότι επρόκειτο για κάποιο είδος ελληνικής γραφής, αλλά η άποψη του αυτή δεν έγινε δεκτή αρχικά από τους ειδικούς. Στη συνέχεια, όμως, αρκετοί προσχώρησαν στην άποψή του. Ένας από αυτούς ήταν ο κρυπταναλυτής Τζον Τσάντγουικ, ο οποίος, στη διάρκεια του πολέμου, είχε εργασθεί στην ανάλυση της γερμανικής κρυπτομηχανής Enigma. Προσπάθησε να μεταφέρει την πείρα του στην κρυπτανάλυση της Γραμμικής Β, αλλά χωρίς επιτυχία μέχρι τότε. Όμως, ο συνδυασμός των δύο επιστημόνων έφερε το πολυπόθητο αποτέλεσμα. Το 1953 κατέγραψαν τα συμπεράσματά τους στο μνημειώδες έργο «Μαρτυρίες για την ελληνική διάλεκτο στα μυκηναϊκά αρχεία», που έγινε το πιο διάσημο άρθρο κρυπτανάλυσης. Η αποκρυπτογράφηση της Γραμμικής Β απέδειξε ότι επρόκειτο για ελληνική γλώσσα, ότι οι Μινωίτες της Κρήτης μιλούσαν ελληνικά και ότι η δεσπόζουσα δύναμη εκείνη την εποχή ήταν οι Μυκήνες. Η αποκρυπτογράφηση της Γραμμικής Β θεωρήθηκε επίτευγμα ανάλογο της κατάκτησης του Έβερεστ, που συνέβη την ίδια ακριβώς εποχή. Για αυτό και έγινε γνωστή σαν το «Έβερεστ της Ελληνικής αρχαιολογίας».

1.4 Δεύτερο στάδιο κρυπτογραφίας

Το δεύτερο στάδιο της κρυπτογραφίας όπως προαναφέρθηκε τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950. Καλύπτει, επομένως, τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων (λόγω της εξαιρετικά μεγάλης ανάγκης που υπήρξε για ασφάλεια κατά τη μετάδοση ζωτικών πληροφοριών μεταξύ των στρατευμάτων των χωρών) αναπτύχθηκε η κρυπτογραφία τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές». Η κρυπτανάλυση τους, απαιτεί μεγάλο αριθμό προσωπικού, το οποίο εργαζόταν επί μεγάλο χρονικό διάστημα ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη

υπολογιστική ισχύ. Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά τη διάρκεια αυτής της περιόδου η κρυπτανάλυση τους είναι συνήθως επιτυχημένη. Οι Γερμανοί έκαναν εκτενή χρήση (σε διάφορες παραλλαγές) ενός συστήματος γνωστού ως Enigma (Εικόνα 3).



Εικόνα 3: Η Μηχανή Enigma

Η μηχανή Αίνιγμα χρησιμοποιήθηκε ευρέως στη Γερμανία Ο Marian Rejewski, στην Πολωνία, προσπάθησε και, τελικά, παραβίασε την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma (που χρησιμοποιούσε μια ηλεκτρομηχανική κρυπτογραφική συσκευή) χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ήταν η μεγαλύτερη σημαντική ανακάλυψη στην κρυπτολογική ανάλυση της εποχής. Οι Πολωνοί συνέχισαν να αποκρυπτογραφούν τα μηνύματα που βασιζόταν στην κρυπτογράφηση με το Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε ορισμένες σημαντικές αλλαγές και οι Πολωνοί δεν μπόρεσαν να τις παρακολουθήσουν, επειδή η αποκρυπτογράφηση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν. Έτσι, εκείνο το καλοκαίρι μεταβίβασαν τη γνώση τους, μαζί με μερικές μηχανές που είχαν κατασκευάσει, στους Βρετανούς και τους Γάλλους. Ακόμη και ο Rejewski και οι μαθηματικοί και κρυπτογράφοι του, όπως ο Biuro Szyfrow, κατέληξαν σε συνεργασία με τους Βρετανούς και τους Γάλλους μετά από αυτή την εξέλιξη. Η συνεργασία αυτή συνεχίστηκε από τον Άλαν Τούρινγκ (Alan Turing), τον Γκόρντον Ουέλτσμαν (Gordon Welchman) και από πολλούς άλλους στο Μπλέτσλεϊ Παρκ (Bletchley Park), κέντρο της Βρετανικής Υπηρεσίας απο/κρυπτογράφησης και οδήγησε σε συνεχείς αποκρυπτογραφήσεις των διαφόρων παραλλαγών του Enigma, με τη βοήθεια και ενός υπολογιστή, που κατασκεύασαν οι Βρετανοί επιστήμονες, ο οποίος ονομάσθηκε Colossus και, δυστυχώς, καταστράφηκε με το τέλος του Πολέμου. Οι κρυπτογράφοι του αμερικανικού ναυτικού (σε συνεργασία με Βρετανούς και Ολλανδούς κρυπτογράφους μετά από το 1940) έσπασαν αρκετά κρυπτοσυστήματα του Ιαπωνικού ναυτικού. Το σπάσιμο ενός από αυτά, του JN-25, οδήγησε στην αμερικανική νίκη στη Ναυμαχία της Μιντγουέι καθώς και στην εξόντωση του Αρχηγού του Ιαπωνικού Στόλου Ιζορόκου Γιαμαμότο.

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

Οι συμμαχικές κρυπτομηχανές που χρησιμοποιήθηκαν στον δεύτερο παγκόσμιο πόλεμο περιλάμβαναν το βρετανικό TypeX και το αμερικανικό SIGABA (Εικόνα 4). Και τα δύο ήταν ηλεκτρομηχανικά σχέδια παρόμοια στο πνεύμα με το Enigma, με σημαντικές εν τούτοις βελτιώσεις. Κανένα δεν έγινε γνωστό ότι παραβιάστηκε κατά τη διάρκεια του πολέμου. Τα στρατεύματα στο πεδίο μάχης χρησιμοποίησαν το Μ-209 και τη λιγότερη ασφαλή οικογένεια κρυπτομηχανών Μ-94. Οι Βρετανοί πράκτορες της Υπηρεσίας "SOE" χρησιμοποίησαν αρχικά ένα τύπο κρυπτογραφίας που βασιζόταν σε ποιήματα (τα απομνημονευμένα ποιήματα ήταν τα κλειδιά). Οι Γερμανοί, ώρες πριν την Απόβαση της Νορμανδίας συνέλαβαν ένα μήνυμα - ποίημα του Πολ Βερλέν, για το οποίο, χωρίς να το έχουν αποκρυπτογραφήσει, ήταν βέβαιοι πως προανάγγελλε την απόβαση. Η Γερμανική ηγεσία δεν έλαβε υπόψη της αυτή την προειδοποίηση.

Εικόνα 4: Η Κρυπτομηχανή SIGABA

Οι Πολωνοί είχαν προετοιμαστεί για την εμπόλεμη περίοδο κατασκευάζοντας την κρυπτομηχανή LCD Lacida, η οποία κρατήθηκε μυστική ακόμη και από τον Rejewski. Όταν. τον Ιούλιο του 1941 ελέγχθηκε από τον Rejewski η ασφάλειά της, του χρειάστηκαν μερικές μόνον ώρες για να την "σπάσει" και έτσι αναγκάστηκαν να την αλλάξουν βιαστικά. Τα μηνύματα που εστάλησαν με Lacida δεν ήταν, εντούτοις, συγκρίσιμα με αυτά του Enigma, αλλά η παρεμπόδιση θα μπορούσε να έχει σημάνει το τέλος της κρίσιμης κρυπταναλυτικής Πολωνικής προσπάθειας.

1.5 Τρίτο στάδιο κρυπτογραφίας

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

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

Ο DES αντικαταστάθηκε επίσημα από τον AES το 2001 όταν ανήγγειλε ο NIST το FIPS 197. Μετά από έναν ανοικτό διαγωνισμό, ο NIST επέλεξε τον αλγόριθμο Rijndael, που υποβλήθηκε από δύο Φλαμανδούς κρυπτογράφους, για να είναι το AES. Ο DES και οι ασφαλέστερες παραλλαγές του όπως ο 3DES ή TDES χρησιμοποιούνται ακόμα σήμερα, ενσωματωμένος σε πολλά εθνικά και οργανωτικά πρότυπα. Εντούτοις, το βασικό μέγεθος των 56-bit έχει αποδειχθεί ότι είναι ανεπαρκές να αντισταθεί στις επιθέσεις ωμής βίας (μια τέτοια επίθεση πέτυχε να σπάσει τον DES σε 56 ώρες ενώ το άρθρο που αναφέρεται ως το σπάσιμο του DES δημοσιεύτηκε από τον O'Reilly and Associates). Κατά συνέπεια, η χρήση απλής κρυπτογράφησης με τον DES είναι τώρα χωρίς την αμφιβολία επισφαλής για χρήση στα νέα σχέδια των κρυπτογραφικών συστημάτων και μηνύματα που προστατεύονται από τα παλαιότερα κρυπτογραφικά συστήματα που χρησιμοποιούν DES, και όλα τα μηνύματα που έχουν αποσταλεί από το 1976 με τη χρήση DES, διατρέχουν επίσης σοβαρό κίνδυνο αποκρυπτογράφησης. Ανεξάρτητα από την έμφυτη ποιότητά του, το βασικό μέγεθος του DES (56-bit) ήταν πιθανά πάρα πολύ μικρό ακόμη και το 1976, πράγμα που είχε επισημάνει ο Whitfield Diffie. Υπήρξε επίσης η υποψία ότι κυβερνητικές οργανώσεις είχαν ακόμα και τότε ικανοποιητική υπολογιστική δύναμη ώστε να σπάσουν μηνύματα που είχαν κρυπτογραφηθεί με τον DES.

ΚΕΦΑΛΑΙΟ 2

ΚΡΥΠΤΟΓΡΑΦΙΑ

Στο κεφάλαιο αυτό γίνεται ανάλυση της έννοιας της Κρυπτογραφίας, παρουσιάζονται ο αντικειμενικός της σκοπός, η αναγκαιότητα χρήσης της και τα κρυπτογραφικά εργαλεία - κρυπτοσυστήματα με τα οποία μπορεί να υλοποιηθεί. Επίσης, παρουσιάζονται η κεντρική ιδέα και οι βασικοί όροι της Κρυπτογράφησης.

Για το κεφάλαιο αυτό χρησιμοποιήθηκαν στοιχεία από τις πηγές [2], [3], [8], [11], [12].

2.1 Εισαγωγή - Η έννοια της Κρυπτογραφίας

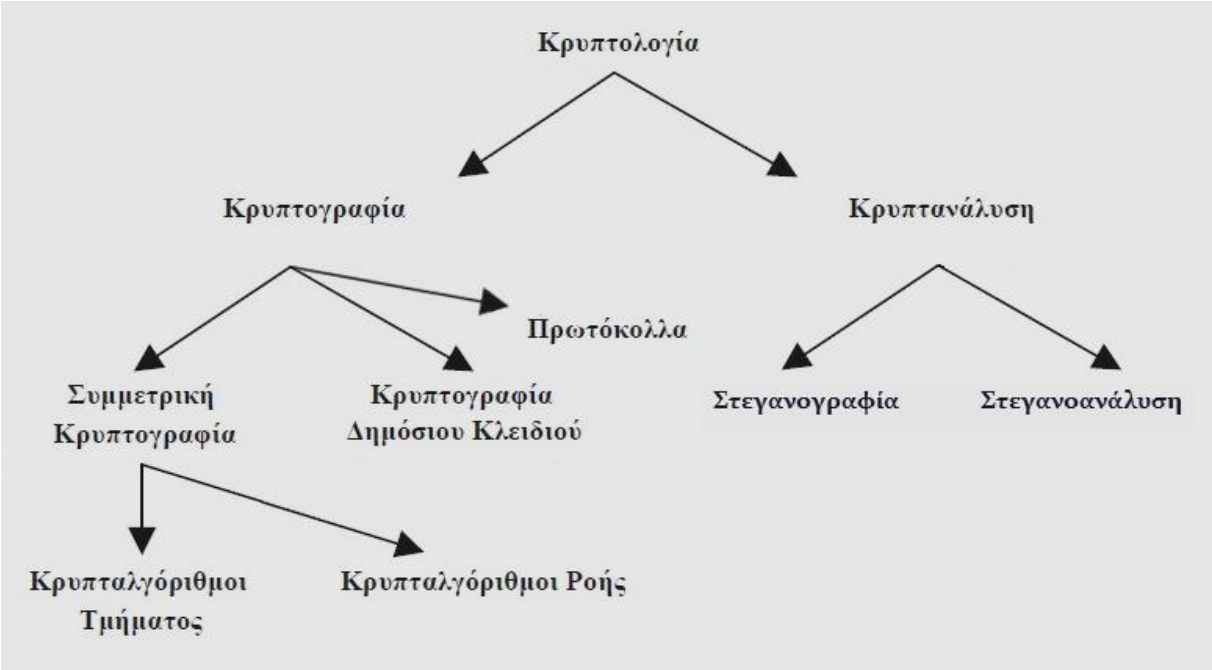
Κρυπτογραφία (encryption) ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.

Η Κρυπτογραφία έρχεται να εξασφαλίσει το απόρρητο των προσωπικών πληροφοριών. Πρόκειται για μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογραφίας καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών.

Σε νομικό και κοινωνικό επίπεδο, τίθεται ζήτημα προστασίας του απορρήτου σε όλες τις εκδοχές δικτυακής συναλλαγής (e-mail, εμπορικές συναλλαγές, τραπεζικό και ιατρικό απόρρητο) και γενικότερα ζήτημα προστασίας προσωπικών δεδομένων του κάθε χρήστη του Internet. Για το λόγο αυτό αποτελεί το Α και το Ω της δικτυακής ασφάλειας.

Η Κρυπτογραφία είναι ένας επιστημονικός κλάδος που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Ανήκει στον κλάδο της επιστήμης της Κρυπτολογίας (Εικόνα 5), η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς για δύο ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάζει την πληροφορία εκτός από τα μέλη.

Η λέξη κρυπτολογία αποτελείται από την ελληνική λέξη "κρυπτός" και τη λέξη "λόγος" και χωρίζεται σε δύο κλάδους: Την Κρυπτογραφία και την Κρυπτανάλυση με παρεμφερή κλάδο την Στεγανογραφία και αντίστοιχα την Στεγανοανάλυση.
Πιο συγκεκριμένα, Κρυπτογραφία είναι η επιστήμη που ασχολείται με τους μαθηματικούς μετασχηματισμούς για την εξασφάλιση της ασφάλειας της πληροφορίας και Κρυπτανάλυση είναι η επιστήμη που ασχολείται με την ανάλυση και την διάσπαση των Κρυπτοσυστημάτων. Τα είδη των Κρυπτοσυστημάτων αυτών παρουσιάζονται αναλυτικότερα παρακάτω.



Εικόνα 5: Ο επιστημονικός κλάδος της Κρυπτολογίας

2.2 Αντικειμενικός σκοπός

Ο αντικειμενικός σκοπός της κρυπτογραφίας είναι να ανακαλύψει και να αποτρέψει οποιαδήποτε προσπάθεια εξαπάτησης ή κακόβουλης ενέργειας. Ένας από τους βασικούς στόχους της είναι να εξασφαλίσει την καλύτερη δυνατή ικανοποίηση των τεσσάρων παρακάτω χαρακτηριστικών τόσο στην θεωρία όσο και στην πράξη ,αντιμετωπίζοντας τους αντίστοιχους κινδύνους.

α) Εμπιστευτικότητα (Confidentiality): Η πληροφορία να πηγαίνει μόνο στα χέρια του ενδιαφερομένου.

β) Ακεραιότητα (Integrity): Υποδηλώνει ότι το μήνυμα δεν θα αλλοιωθεί. Δηλαδή την Προστασία από μετατροπή, διαγραφή ή/ και δημιουργία του.

γ) Πιστοποίηση ή Αυθεντικοποίηση (authentication): Ο αποστολέας και ο παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές της καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές αυτές δεν είναι πλαστές.

δ) Μη απάρνηση ή Μη αποποίηση (non-repudation): Η δυνατότητα να αποδειχθεί ότι κάποιος έλαβε ένα μήνυμα ή ότι πραγματικά έστειλε αυτός ένα μήνυμα και όχι κάποιος άλλος.

Αναλυτικότερα έχουμε:

α) Εμπιστευτικότητα (Confidentiality)

Εμπιστευτικότητα είναι η ιδιότητα των δεδομένων ή πληροφοριών να είναι προσπελάσιμα μόνο από τις εξουσιοδοτημένες οντότητες. Η εμπιστευτικότητα αναφέρεται στο περιεχόμενο

ηλεκτρονικών εγγράφων ή, γενικά, αρχείων και μηνυμάτων, στην ύπαρξή τους και στην ταυτότητα αυτών που εκτελούν ενέργειες και ανταλλάσσουν μηνύματα. Επίσης, αναφέρεται στο χρόνο και την ποσότητα μηνυμάτων που ανταλλάσσονται. Η εμπιστευτικότητα, μερικές φορές, καλείται και ιδιωτικότητα ή μυστικότητα ή προστασία του απορρήτου.

β) Ακεραιότητα (Integrity)

Η ακεραιότητα είναι η ιδιότητα των δεδομένων και πληροφοριών και των υπολογιστικών και επικοινωνιακών πόρων να τροποποιούνται μόνο από εξουσιοδοτημένες οντότητες κατά εξουσιοδοτημένο τρόπο. Η ακεραιότητα έχει να κάνει με την ακρίβεια και τη συνέπεια στη λειτουργία συστημάτων και διεργασιών. Τα δεδομένα σε κάθε σύστημα πρέπει να παραμένουν πλήρη και ορθά. Η ακεραιότητα διατηρείται όταν διατηρούνται και οι ιδιότητες: η ακρίβεια, η μη τροποποίηση ή τροποποίηση από εξουσιοδοτημένους χρήστες ή διεργασίες, με συνέπεια, κατά αποδεκτό τρόπο. Έχουν αναγνωριστεί τρεις καθοριστικές συνιστώσες του όρου «ακεραιότητα»: οι εξουσιοδοτημένες ενέργειες, ο διαχωρισμός και η προστασία αγαθών και η ανίχνευση και διόρθωση σφαλμάτων.

γ) Πιστοποίηση ή Αυθεντικοποίηση (authentication)

Πιστοποίηση ή Αυθεντικοποίηση είναι η εξασφάλιση του ότι γνωρίζουμε το χρήστη ή γενικότερα την οντότητα που επικοινωνούμε (user/ entity authentication). Έτσι εξακριβώνεται ότι ένα μήνυμα προέρχεται πράγματι από τον αποστολέα που πιστεύουμε ότι το έστειλε.

δ) Μη απάρνηση ή Μη αποποίηση (non-repudation)

Είναι η υπηρεσία κατά την οποία ο παραλήπτης δεν μπορεί να απαρνηθεί ότι έλαβε το μήνυμα δηλαδή, μη απάρνηση προορισμού (non-repudiation of destination). Επίσης είναι η υπηρεσία κατά την οποία ο αποστολέας δεν μπορεί να απαρνηθεί ότι έστειλε το μήνυμα δηλαδή, μη απάρνηση προέλευσης (non-repudiation of origin).

2.3 Αναγκαιότητα χρήσης της κρυπτογραφίας

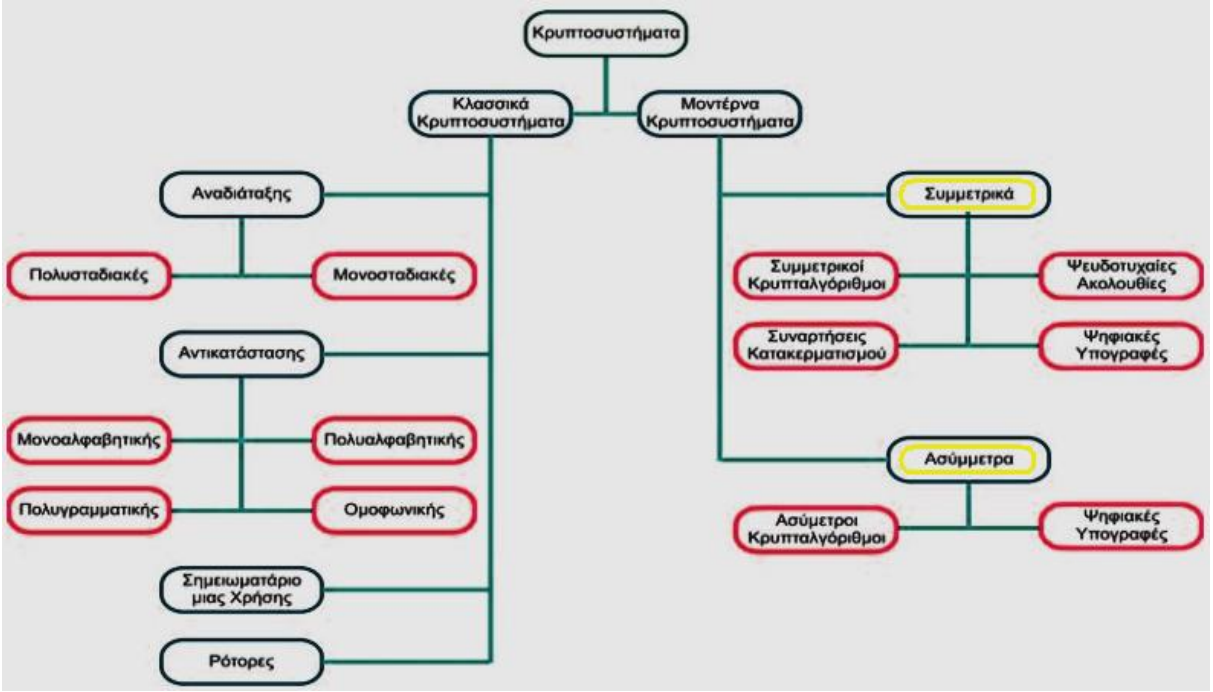
Όταν κάποιος αποστέλλει ένα προσωπικό e-mail ή ανταλλάσσει εμπιστευτικές εμπορικές πληροφορίες για ένα έργο μέσω του ηλεκτρονικού ταχυδρομείου, οφείλει να γνωρίζει ότι, εάν δεν έχει κρυπτογραφηθεί, είναι σαν να το στέλνει με καρτ-ποστάλ: μπορεί να το διαβάσει σχεδόν οποιοσδήποτε. Έτσι, η χρήση κρυπτογραφικών εργαλείων δεν αφορά μόνο κατασκόπους ή μανιώδεις χρήστες υπολογιστών όπου αρκετοί συνηθίζουν να πιστεύουν.

Ένα e-mail, εκτός από τον αποστολέα και τον παραλήπτη, μπορεί να διαβαστεί εύκολα και από τους εργαζόμενους στον ISP (εταιρία παροχής Internet) του αποστολέα, τους εργαζόμενους στον ISP του παραλήπτη, από οποιονδήποτε ελέγχει τους routers από τους οποίους θα περάσουν τα "πακέτα" του μηνύματος και από οποιονδήποτε έχει πρόσβαση στον εξοπλισμό τηλεφωνίας στην τηλεφωνική εταιρία. Αν το μήνυμα αποστέλλεται ή παραλαμβάνεται από κινητό τηλέφωνο με σύνδεση στο Διαδίκτυο, τότε μπορεί να υποκλαπεί από άτομα με ειδικές συσκευές υποκλοπής συνομιλιών και μηνυμάτων κινητής τηλεφωνίας. Επιπλέον, είναι πολύ απλό να πλαστογραφηθεί η διεύθυνση αποστολής, ακόμα και με ένα τυπικό πρόγραμμα e-mail. Με λίγο περισσότερη δουλειά, κάποιος επιτήδειος μπορεί να αποκρύψει και άλλα σημάδια που δείχνουν από πού πραγματικά προέρχεται ένα μήνυμα.

Λύση στα παραπάνω προβλήματα δίνουν οι τεχνολογίες κρυπτογράφησης. Οι τεχνολογίες αυτές εξασφαλίζουν ότι το μήνυμα θα μπορεί να το διαβάσει μόνο ο παραλήπτης του, καθώς στα ενδιάμεσα στάδια το μήνυμα εμφανίζεται με ακατάληπτους χαρακτήρες, είναι δηλαδή μη αναγνώσιμο. Εκτός από την κρυπτογράφηση, μια άλλη τεχνολογία που παρέχει τέτοιου είδους ασφάλεια είναι η ηλεκτρονική ή ψηφιακή υπογραφή, τομέας με τον οποίο έχουμε θα ασχοληθούμε παρακάτω. Αξίζει, πάντως, να σημειώσουμε ότι είναι δυνατόν ένα μήνυμα να κρυπτογραφηθεί και ταυτόχρονα να υπογραφεί ηλεκτρονικά. Έτσι εξασφαλίζονται εξίσου η ασφάλεια στην επικοινωνία και η πιστοποίηση περιεχομένου και ταυτότητας αποστολέα.

2.4 Είδη κρυπτοσυστημάτων

Στην κρυπτογραφία, μια διαδικασία κρυπτογράφησης και η αντίστοιχη διαδικασία αποκρυπτογράφησης αποτελούν ένα κρυπτοσύστημα. Τα Κρυπτοσυστήματα χωρίζονται σε δυο μεγάλες κατηγορίες (Εικόνα 6) οι οποίες είναι:
α) τα Κλασσικά Κρυπτοσυστήματα,
β) τα Μοντέρνα Κρυπτοσυστήματα.
Τα Κλασσικά Κρυπτοσυστήματα αφορούν την επεξεργασία γλωσσικών μηνυμάτων και χρησιμοποιούν την μέθοδο της αναδιάταξης και της αντικατάστασης. Τα Κρυπτοσυστήματα αναδιάταξης αλλάζουν τη σειρά των συμβόλων, χωρίς να τα παραποιούν ενώ τα Κρυπτοσυστήματα αντικατάστασης διατηρούν τη σειρά των συμβόλων του καθαρού κειμένου αλλά παραποιούν τα ίδια τα σύμβολα.
Τα Μοντέρνα Κρυπτοσυστήματα αποτελούνται από τα Συμμετρικά και τα Ασύμμετρα τα οποία θα αναλύσουμε εκτενέστερα παρακάτω.



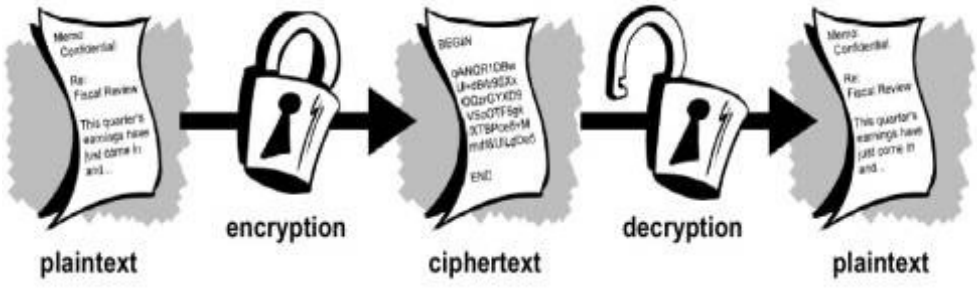
Εικόνα 6: Κρυπτοσυστήματα

2.5 Εισαγωγή στην Κρυπτογράφηση (encryption) – Βασικές έννοιες

Η κρυπτογραφία είναι μια διαδικασία που μπορεί να εκτελεστεί τόσο σε hardware όσο και σε software. Η ενσωμάτωση των μεθόδων της κρυπτογραφίας σε hardware επιταχύνει σε μεγάλο βαθμό την διεκπεραίωση της. Επίσης, οι χρήστες δεν γνωρίζουν, ούτε καν αντιλαμβάνονται την παρουσία της και πραγματοποιούν ανενόχλητοι τις εργασίες τους. Το γεγονός ότι ο χρήστης δεν ανακατεύεται καθόλου στις διαδικασίες της κρυπτογραφίας, αυξάνει την αποτελεσματικότητα του εργαλείου στην παρεχόμενη ασφάλεια. Παρ' όλα αυτά, δεν έχει καθιερωθεί η κρυπτογραφία σε hardware λόγω του υψηλού κόστους της, που απαγορεύει την αγορά και διατήρηση των ειδικών μηχανημάτων που χρειάζονται για την εφαρμογή της. Τα ειδικά αυτά μηχανήματα βρίσκονται τοποθετημένα σε στρατηγικά σημεία κάθε δικτύου. Η λογισμική κρυπτογραφία (σε software) είναι φτηνότερη, πράγμα που την κάνει ευρέως αποδεκτή και εύκολα πραγματοποιήσιμη. Βέβαια, δεν είναι το ίδιο γρήγορη με την εκτέλεση της σε hardware, αλλά η ολοένα αυξανόμενη ανάγκη για διασφάλιση των επικοινωνιών εδραίωσε την χρήση της.
Εφαρμογή της κρυπτογραφίας αποτελεί η Κρυπτογράφηση με τα αντίστοιχα Συμμετρικά και Ασύμμετρα Κρυπτοσυστήματα.
Κατά την Κρυπτογράφηση ο μετασχηματισμός των δεδομένων γίνεται σε μορφή που να είναι αδύνατον να διαβαστεί χωρίς την γνώση της σωστής ακολουθίας bit. Η ακολουθία bit καλείται «κλειδί» (key) και χρησιμοποιείται σε συνδυασμό με κατάλληλο αλγόριθμο / συνάρτηση. Η αντίστροφη διαδικασία είναι η αποκρυπτογράφηση και απαιτεί γνώση του κλειδιού. Σκοπός της κρυπτογράφησης είναι να εξασφαλίσει το απόρρητο των δεδομένων κρατώντας τα κρυφά από όλους όσους έχουν πρόσβαση σε αυτά. Η κρυπτογράφηση και η αποκρυπτογράφηση απαιτούν, την χρήση κάποιας μυστικής πληροφορίας, το κλειδί. Για μερικούς μηχανισμούς χρησιμοποιείται το ίδιο κλειδί και για την κρυπτογράφηση και για την αποκρυπτογράφηση, για άλλους όμως τα κλειδιά που χρησιμοποιούνται διαφέρουν. Για το λόγο αυτό, η κρυπτογράφηση αναλύεται σε συμμετρική και ασύμμετρη.

2.6 Η κεντρική ιδέα της Κρυπτογράφησης – Βασικές έννοιες

Η κεντρική ιδέα της Κρυπτογράφησης περιγράφεται στην Εικόνα 7 αναπαριστάνοντας την Κρυπτογράφηση ενός απλού κειμένου.



Εικόνα 7: Κρυπτογράφηση απλού κειμένου

Το αρχικό κομμάτι της πληροφορίας ονομάζεται απλό κείμενο (plaintext) ενώ το μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου, δηλαδή το κρυπτογραφημένο κείμενο ονομάζεται κρυπτογράφημα (ciphertext).

Κατά την διαδικασία της Κρυπτογράφησης (encryption) εφαρμόζεται ένας αλγόριθμος ο οποίος ονομάζεται αλγόριθμος κρυπτογράφησης (encryption algorithm ή cypher) . Πρόκειται για μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση των πληροφοριών.
Όσο αυξάνει ο βαθμός πολυπλοκότητας του αλγόριθμου, τόσο μειώνεται η πιθανότητα να τον διαβάλλει κάποιος. Ο αλγόριθμος κρυπτογράφησης λειτουργεί σε συνδυασμό με ένα κλειδί, το μυστικό κλειδί (secret key), για την κρυπτογράφηση του απλού κειμένου, το οποίο εισάγεται στον αλγόριθμο κρυπτογράφησης. Οι ακριβείς αντικαταστάσεις και τα αποτελέσματα των μετασχηματισμών που επιτελούνται από τον αλγόριθμο εξαρτώνται από αυτό το μυστικό κλειδί. Το ίδιο απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν χρησιμοποιούνται διαφορετικά κλειδιά.
Κατά την διαδικασία της Αποκρυπτογράφησης (decryption) εφαρμόζεται ο αντίστροφος αλγόριθμος (decryption algorithm) με σκοπό να ανακτηθεί το απλό κείμενο από το κρυπτογράφημα. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, όταν μόνο τα άτομα που συμμετέχουν σε αυτή μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος.

ΚΕΦΑΛΑΙΟ 3

ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

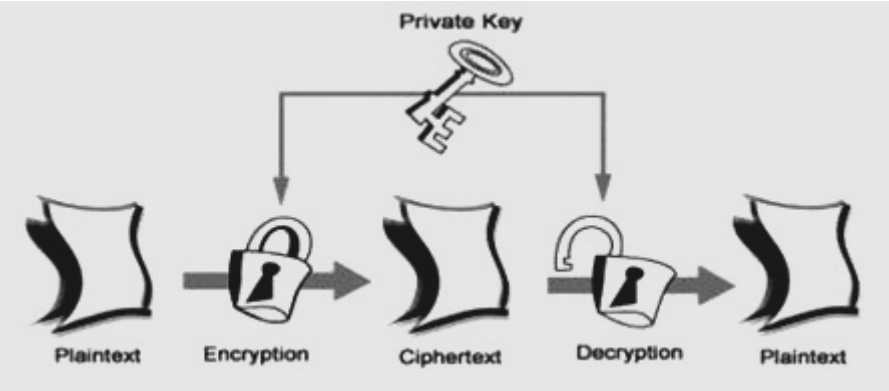
Στο κεφάλαιο αυτό γίνεται ανάλυση του τρόπου λειτουργίας της Συμμετρικής Κρυπτογράφησης και των αντίστοιχων κρυπτογραφικών αλγορίθμων που περιλαμβάνει.

Για το κεφάλαιο αυτό χρησιμοποιήθηκαν στοιχεία από τις πηγές [1], [4], [5], [6], [7], [9],[15].

3.1 Συμμετρική Κρυπτογράφηση ή Κρυπτογράφηση ιδιωτικού κλειδιού (Symmetric Cryptography ή Secret key Cryptography)

Στη συμμετρική κρυπτογράφηση ένος μηνύματος χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση του, όσο και για την αποκρυπτογράφηση του (Εικόνα 8). Αρχικά, το κλειδί αυτό πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη, οπότε, απαιτείται ασφαλές μέσο για τη μετάδοσή του.

Αρχικά είναι διαθέσιμο το μήνυμα προς κρυπτογράφηση, απλό κείμενο (plaintext) το οποίο θα αποσταλεί. Ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και κρυπτογραφεί το κείμενο. Έτσι προκύπτει το κρυπτογράφημα (ciphertext) το οποίο αποστέλλεται στον παραλήπτη. Με την αντίστροφη διαδικασία ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί μετατρέποντας το κρυπτογράφημα στο αρχικό κείμενο ολοκληρώνοντας με επιτυχία την μετάδοση του μηνύματος. Γενικά ισχύει ο κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς. Διαφορετικοί αλγόριθμοι απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.



Εικόνα 8: Συμμετρική Κρυπτογράφηση

Το ιδιωτικό κλειδί μπορεί να μεταδοθεί μέσα από μία προσωπική συνάντηση κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται και γενικότερα με τη φυσική παράδοσή του (π.χ. με courier ή με ηλεκτρονικό ταχυδρομείο). Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογράφηση είναι αναποτελεσματική.

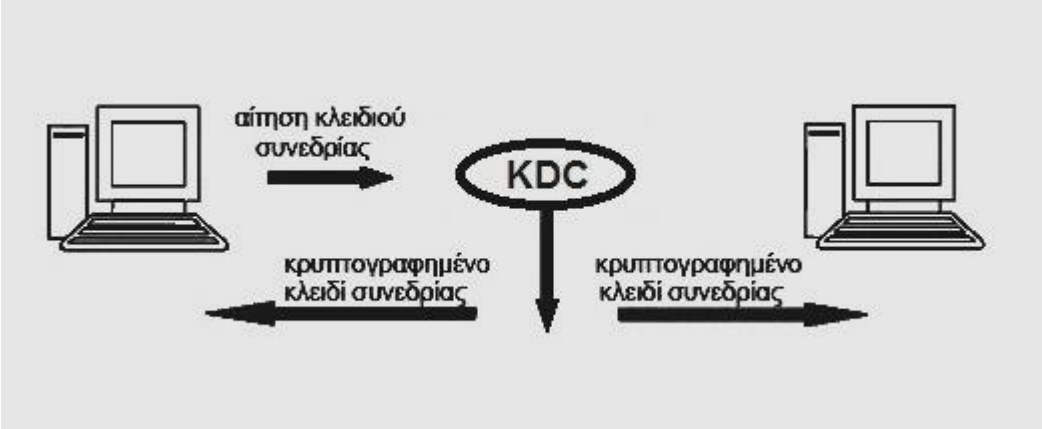
Ωστόσο έχουν αναπτυχθεί και ήδη χρησιμοποιούνται κάποια ασφαλή κανάλια (μια έμπιστη τρίτη οντότητα) για την ανταλλαγή των μυστικών κλειδιών με πιο διαδεδομένο το σύστημα Kerberos, του MIT (Massachusetts Institute of Technology).

Επίσης είναι διαθέσιμο και το Κέντρο Διανομής Κλειδιών (Key Distribution Center, KDC) (Εικόνα 9). Πρόκειται για μια κεντρική Αρχή η οποία μοιράζεται ένα διαφορετικό, μοναδικό και μόνιμο συμμετρικό κλειδί με κάθε χρήστη του δικτύου (πελάτη του). Το κλειδί που θα χρησιμοποιηθεί για την επικοινωνία ή τη συναλλαγή μεταξύ τους (των δύο μερών) (κλειδί συνεδρίας ή κλειδί συνόδου, session key) είναι μιας χρήσης, δημιουργείται από το KDC και διανέμεται ως εξής:

Το KDC δημιουργεί ένα κλειδί συνεδρίας και το κρυπτογραφεί με το συμμετρικό κλειδί που μοιράζεται με τον αποστολέα.

Το KDC αποστέλλει το ίδιο κλειδί συνεδρίας στον παραλήπτη, κρυπτογραφημένο με το μυστικό συμμετρικό κλειδί που ήδη μοιράζεται με αυτόν .

Ο αποστολέας και ο παραλήπτης είναι τώρα σε θέση να επικοινωνήσουν μεταξύ τους. Η κρυπτογράφηση των μηνυμάτων τους γίνεται με το κοινό κλειδί συνεδρίας που τους απέστειλε το KDC.



Εικόνα 9: Διαδικασία μετάδοσης ιδιωτικού κλειδιού μέσω KDC

Με τον τρόπο αυτό οι χρήστες έχουν σε κάθε συναλλαγή ένα νέο κλειδί συνεδρίας. Εννοείται ότι, αν παραβιαστεί η ασφάλεια του KDC, παραβιάζεται η ασφάλεια όλου του δικτύου.

3.2 Κρυπτογραφικοί αλγόριθμοι

Καθοριστικό ρόλο σε όλη την διαδικασία της συμμετρικής κρυπτογράφησης παίζουν οι αλγόριθμοι που χρησιμοποιούνται για την κωδικοποίηση του αρχικού μηνύματος. Με βάση λοιπόν τον τρόπο που κρυπτογραφούν, χωρίζονται σε αλγόριθμους «Τμήματος ή Δέσμης (Block Ciphers)» και αλγόριθμους «Ροής (Stream Ciphers)» (Εικόνα 10).

Κρυπτογραφικοί αλγόριθμοι		
Τμήματος (Block Ciphers)		**Ροής (Stream Ciphers)**
DES	MISTY	ORYX
IDEA	MMB	RC4
RC2	NewDES	SEAL
RC5	3-Way	
RC6	LOKI	
MARS	CMEA	
Serpent	REDOC	
Twofish	Rijndael	
Blowfish	MacGuffin	
CAST	DEAL FEAL	
Triple-DES	SQUARE	
Safer	Skipjack	
GOST	Lucifer	
Tiny Encryption Algorithm		

Εικόνα 10: Κρυπτογραφικοί αλγόριθμοι Τμήματος και Ροής

3.2.1 Κρυπτογραφικοί αλγόριθμοι Τμήματος ή Δέσμης (Block Ciphers)

Οι κρυπτογραφικοί αλγόριθμοι Τμήματος ή Δέσμης (Block Ciphers) χωρίζουν το μήνυμα σε κομμάτια και κρυπτογραφούν κάθε ένα από τα κομμάτια αυτά ξεχωριστά. Μετατρέπουν δηλαδή, ένα block μη κρυπτογραφημένου καθορισμένου μήκους κειμένου (plaintext), σε block κρυπτογραφημένου του ίδιου μήκους κειμένου (ciphertext). Αυτός ο μετασχηματισμός πραγματοποιείται με την βοήθεια ενός μυστικού κλειδιού που χορηγείται από τον χρήστη. Επίσης, λειτουργούν πάνω σε blocks δεδομένων συνήθως των 64 bits ή πολλαπλασίων τους.

Υπάρχουν διάφοροι τρόποι λειτουργίας των αλγορίθμων Τμήματος όπως το Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), Counter (CTR). Επίσης, βασικές δομές που χρησιμοποιούνται από αλγορίθμους τμημάτων αποτελούν οι δομές Feistel. Η ιδέα που είχε ο Feistel ήταν αρκετά απλή και είχε ως βασικό άξονα την απόδειξη της ασφάλειας ενός αλγορίθμου μέσω μη αντιστρέψιμων συναρτήσεων. Προσπάθησε να θέσει την ιδέα ότι τα μοντέλα των κρυπτογραφικών αλγορίθμων τμημάτων θα πρέπει να είναι όσο γίνεται πιο απλά. Το να προσθέτει κανείς μέρη τα οποία είναι ασφαλή, το καθένα ανεξάρτητα από το άλλο, δεν συνεπάγεται ότι το σύνολο είναι ασφαλές.

Παρακάτω ακολουθεί η αναλυτική περιγραφή Block Ciphers αλγορίθμων:

Αλγόριθμος DES (Data Encryption Standard)

Ο DES (Data Encryption Standard) είναι ένας αλγόριθμος Τμήματος (Block Cipher) και αποτελεί ένα από τα το πιο δημοφιλή συστήματα συμμετρικής κρυπτογράφησης. Ο αλγόριθμος DES αναπτύχθηκε από την IBM στις αρχές της δεκαετίας του 1970 και το 1977 το Εθνικό Κέντρο Πιστοποίησης των ΗΠΑ το υιοθέτησε ως το επίσημο πρότυπο

κρυπτογράφησης απόρρητων πληροφοριών. Χρησιμοποιεί ένα κλειδί μεγέθους 56 bits. Το προς κρυπτογράφηση κείμενο εισάγεται σε τμήματα μεγέθους 64-bit και παράγεται ένα 64 bits κρυπτογράφημα. Παρά τη πολυπλοκότητα της αρχιτεκτονικής του DES, ο αλγόριθμος αυτός αποτελεί ουσιαστικά έναν κώδικα μονοαλφαβητικής αντικατάστασης. Πλέον δεν θεωρείται ασφαλής, καθώς λόγω του περιορισμένου μήκους του κλειδιού του είναι πολύ ευάλωτος στις επιθέσεις "ωμής" βίας.
Κατά τις συγκεκριμένες επιθέσεις δοκιμάζονται όλα τα πιθανά κλειδιά και έχει αποδειχθεί ότι είναι δυνατόν να αποκρυπτογραφηθούν μηνύματα του συγκεκριμένου αλγόριθμου σε σχετικά μικρό χρονικό διάστημα. Το 1997, η εταιρεία RSA Security υποστήριξε μια σειρά διαγωνισμών με βραβείο 10.000 δολαρίων στην πρώτη ομάδα που θα "έσπαζε" ένα μήνυμα, το οποίο είχε κρυπτογραφηθεί με τον DES. Τον διαγωνισμό κέρδισε το πρόγραμμα DESCHALL, που δημιουργήθηκε από τους Rocke Verser, Matt Curtin, και Justin Dolske, χρησιμοποιώντας ιδανικούς κύκλους χιλιάδων υπολογιστών σε ολόκληρο το Διαδίκτυο.

Από το 1997 ξεκίνησαν από το NIST (National Institute for Standards and Technology) των ΗΠΑ, οι διαδικασίες προσδιορισμού του απογόνου του συστήματος DES, το οποίο καλείται AES (Advanced Encryption Standard). Επικρατέστεροι αλγόριθμοι για το πρότυπο AES είναι οι Twofish, RC6, SERPENT, SAFER, Rijnadel, MARS, DEAL, Crypton και CAST.

Αλγόριθμος Triple DES

Εφαρμόζοντας διάφορες τεχνικές επάνω στο DES, αυξήθηκε σημαντικά την ασφάλειά του. Εξέλιξή του αποτελεί ο Triple-DES, ο οποίος εκτελεί τρεις φορές την κρυπτογράφηση ή την αποκρυπτογράφηση του DES με αποτέλεσμα να κάνει καλύτερη κρυπτογράφηση από το κλασικό DES. Με αυτό το τρόπο μειώνονται οι ανησυχίες σχετικά με την ανθεκτικότητα του αλγορίθμου, λόγω του μικρού μεγέθους του κλειδιού. Το αρχικό κείμενο κρυπτογραφείται με τη χρήση ενός κλειδιού, στη συνέχεια αποκρυπτογραφείται με τη χρήση ενός δεύτερου και μετά κρυπτογραφείται με ένα τρίτο στον αποστολέα. Το αποτέλεσμα στέλνεται στο παραλήπτη που ακολουθεί την αντίστροφη διαδικασία. Πρώτα, αποκρυπτογραφεί με χρήση του τρίτου κλειδιού, στη συνέχεια κρυπτογραφεί με το δεύτερο και τέλος αποκρυπτογραφεί με το τρίτο. Ο Triple-DES αλγόριθμος μπορεί να υλοποιηθεί χρησιμοποιώντας δύο ή τρία κλειδιά μεγέθους 56 bits. Τέλος, συγκριτικά με τον αλγόριθμο DES μπορούμε να πούμε ότι ο Triple-DES παρέχει πολύ υψηλότερη ασφάλεια παρόλα αυτά παρουσιάζει ένα κύριο μειονέκτημα το οποίο είναι η ταχύτητα του καθώς είναι αργός σε υλοποιήσεις λογισμικού. Έτσι, αναζητώντας κάποιο προηγμένο πρότυπο κρυπτογράφησης, αναπτύχθηκε το AES (Advanced Encryption Standard).

AES (Advanced Encryption Standard) - Rijndael

Το 1997, ο NIST (National Institute of Standards and Technology) της Αμερικανικής κυβέρνησης προκύριξε διαγωνισμό για την εξεύρεση ενός νέου προτύπου κρυπτογράφησης. Οι βασικές προϋποθέσεις που τέθηκαν ήταν το ελάχιστο μήκος κλειδιού να είναι 128 bits, να υπάρχει δυνατότητα υλοποίησης σε επεξεργαστές 8 bit, να είναι εφικτή (και σχετικώς απλή) η υλοποίηση του αλγορίθμου τόσο με λογισμικό (software), όσο και με υλικό (hardware), να είναι ελεύθερη η χρήση του αλγορίθμου χωρίς να απαιτείται κάποια συγκεκριμένη άδεια και η πλήρης σχεδίαση θα έπρεπε να δημοσιοποιηθεί.

Τον Νοέμβριο του 2001, αντικατέστησε το πρότυπο DES (Data Encryption Standard) και τον Ιούνιο του 2003 η Αμερικανική κυβέρνηση (NSA) ανακοίνωσε πως το AES είναι ασφαλές να προστατεύει διαβαθμισμένη πληροφόρηση έως και σε επίπεδο απορρήτου / top secret. Το πρότυπο AES προσφέρει δυνατή κρυπτογράφηση και αποτελεί πλέον τον προτεινόμενο αλγόριθμο για εφαρμογές της και οι νεότερες εκδόσεις των PGP και GPG περιλαμβάνουν υποστήριξη για το AES. Ο επικρατέστερος αλγόριθμος ο οποίος χρησιμοποιείται είναι ο *αλγόριθμος **Rijndael*** και σχεδιάστηκε από τους Vincent Rijmen και Joan Daemen.
Το πρότυπο κρυπτογράφησης AES (Advanced Encryption Standard) περιγράφει μια διαδικασία κρυπτογράφησης ηλεκτρονικής πληροφορίας βασισμένη στην λογική της κωδικοποίησης ομάδων δεδομένων (τμημάτων) με κάποιο μυστικό κλειδί.
Η κρυπτογράφηση μυστικού κλειδιού κατά το πρότυπο AES υπάγεται στη κατηγορία αλγορίθμων Τμήματος (Block Ciphers). Το πρότυπο υποστηρίζει την χρήση κλειδιών μήκους 128, 192 και 256 bits. Ανάλογα με το ποιο μήκος κλειδιού χρησιμοποιείται, συνήθως χρησιμοποιείται η συντόμευση AES-128, AES-192 και AES-256 αντίστοιχα. Ανεξάρτητα από το μήκος κλειδιού, ο αλγόριθμος ενεργεί πάνω σε τμήματα (blocks) μήκους 128 bits. Η διαδικασία κρυπτογράφησης είναι επαναληπτική. Αυτό σημαίνει ότι σε κάθε block γίνεται μια επεξεργασία η οποία επαναλαμβάνεται έναν αριθμό από φορές ανάλογα με το μήκος κλειδιού. Κάθε επανάληψη ονομάζεται γύρος (round).
Ο Rijndael μπορεί εύκολα να υλοποιηθεί σε hardware. Με εξειδικευμένες μηχανές που δοκιμάζουν 2 κλειδιά ανά δευτερόλεπτο απαιτούνται 149 τρισεκατομμύρια έτη για να σπάσει ένα κλειδί των 128 bits. Εκτιμάται ότι θα επαρκέσει για 20 χρόνια.

Μια σημαντική διευκρίνηση που πρέπει να γίνει είναι ότι ο αλγόριθμος AES δεν είναι ακριβώς ο Rijndael αν και στην πράξη χρησιμοποιούνται εναλλακτικά. Ο Rijndael υποστηρίζει μια μεγαλύτερη γραμμή του τμήματος (block) και των μεγεθών του κλειδιού (key sizes). Πιο συγκεκριμένα, ο αλγόριθμος AES έχει ένα μέγεθος τμήματος των 128 bit και ένα μέγεθος κλειδιού των 128, 192 ή 256 bits, ενώ ο Rijndael μπορεί να χρησιμοποιήσει μεγέθη κλειδιών και τμήματος σε ένα οποιοδήποτε πολλαπλάσιο του 32 bit, με ένα ελάχιστο των 128 bit και ένα μέγιστο 256 bit, αντίστοιχα. Το κλειδί επεκτείνεται χρησιμοποιώντας το βασικό πρόγραμμα του Rijndael. Οι περισσότεροι από τους υπολογισμούς του αλγορίθμου AES γίνονται σε ένα πρόσθετο πεπερασμένο πεδίο.

Αλγόριθμος IDEA (International Data Encryption Algorithm)

Ο αλγόριθμος IDEA αναπτύχθηκε το 1991 στο Swiss Federal Institute of Technology από τους X. Lai και J.Massey. Πρόκειται επίσης για έναν αλγόριθμο Τμήματος (Block Cipher). Χχρησιμοποιεί κλειδί μήκους 128-bit και συνεπώς είναι ικανός για ανθεκτικότερη κρυπτογράφηση από τον DES. Χρησιμοποιείται στο πολύ διαδεδομένο προϊόν διασφάλισης της ηλεκτρονικής αλληλογραφίας PGP (Pretty Good Privacy) ως μία από τις εναλλακτικές επιλογές, καθώς και σε διάφορα προϊόντα του εμπορίου.
Προκειμένου να αναπτυχθεί ένας πολύπλοκος μετασχηματισμός που αναλύεται δύσκολα, οι συναρτήσεις συνδυάζονται με τρόπο ώστε να καθίσταται πολύ δύσκολη η διαδικασία κρυπτανάλυσης. Ο IDEA έχει υποβληθεί σε αξιοσημείωτη διερεύνηση και εμφανίζεται ανθεκτικός σε κρυπταναλυτικές επιθέσεις. Είναι ίσως ο πιο ενδιαφέρον και βασικός αλγόριθμος κρυπτογραφίας μετά το DES και δεν μπορεί να παραβιαστεί χρησιμοποιώντας μεγάλη υπολογιστική ισχύ, για τα σημερινά δεδομένα αλλά και για τις επόμενες δεκαετίες. Τέλος, δεν υπάρχει σήμερα γνωστός αλγόριθμος ή συσκευή που να μπορεί να παραβιάσει το IDEA.

Αλγόριθμοι RC2, RC4 και RC5

Οι κρυπτογραφικοί αλγόριθμοι RC2, RC4 και RC5 αναπτύχθηκαν από τον Ron Rivest της εταιρίας RSA Security. Βασικό χαρακτηριστικό τους είναι ότι υποστηρίζουν κλειδιά μμεταβλητού μμεγέθους (από 40 έως 128 bits) και χρησιμοποιούνται σε διάφορα e-mail προγράμματα.. Αν το μέγεθος του κλειδιού είναι μμεγαλύτερο από 56 bit είναι ανθεκτικότεροι από τον κρυπτογραφικό αλγόριθμο DES.
Ο RC2 είναι ένας αλγόριθμος Τμήματος (Block Cipher) με κλειδί μεταβλητού μήκους και η ασφάλειά του είναι ανάλογη με το μήκος αυτό. Επίσης, είναι έως και τρεις φορές ταχύτερος από τον DES. Χρησιμοποιείται σε διάφορα e-mail προγράμματα.
Ο RC4 είναι ένας αλγόριθμος Ροής (Stream Cipher) με κλειδί ,επίσης, μεταβλητού μήκους και λειτουργεί στο επίπεδο του byte. Χρησιμοποιείται όπως και ο RC2 σε e-mail προγράμματα.
Ο RC5 είναι ένας αλγόριθμος Τμήματος (Block Cipher). Έχει μεταβλητό μήκος κλειδιού, μεταβλητό μέγεθος τμήματος (block) το οποίο συνήθως είναι 32 (πειραματικές εφαρμογές), 64 bits (για αντικατάσταση του DES) και 128 bits και μεταβλητό αριθμό επαναλήψεων. Ο αριθμός των επαναλήψεων μπορεί να είναι από 0 έως και 255. Ο RC5 είναι εύκολος στην ανάλυση του καθώς είναι πολύ απλός στην λειτουργία του. Η χαμηλή απαίτηση μνήμης τον καθιστά κατάλληλο για αξιοποίηση σε έξυπνες κάρτες και άλλες συσκευές περιορισμένης μνήμης. Προορίζεται για να παρέχει υψηλή ασφάλεια με τον προσδιορισμό των κατάλληλων παραμέτρων.

Αλγόριθμος Blowfish

Ο Blowfish είναι ένας αλγόριθμος Τμήματος (Block Cipher) που κατασκευάστηκε από τον από τον Bruce Schneier το 1993 και καθιερώθηκε ως μία από τις δημοφιλέστερες εναλλακτικές λύσεις του DES. Το μέγεθος τμήματος είναι 64 bits και χαρακτηριστικό γνώρισμα του Blowfish αποτελεί το μήκος κλειδιού, το οποίο είναι μεταβλητό, μπορεί να λάβει τιμές έως 448-bit, αν και πρακτικά χρησιμοποιούνται κλειδιά των 128-bit. Πρόκειται για έναν γρήγορο αλγόριθμο, έχει σχεδιασθεί για 32-bit μηχανές και είναι αρκετά ταχύτερο από τον DES. Δεν έχουν παρατηρηθεί σοβαρές αδυναμίες και θεωρείται αρκετά ασφαλής.

Αλγόριθμος CAST

Το CAST αποτελεί μία διαδικασία σχεδίασης συμμετρικών αλγορίθμων κρυπτογράφησης, η οποία αναπτύχθηκε το 1997 από τους C. Adams και S. Tavares της εταιρίας Entrust Technologies. Ένας συγκεκριμένος αλγόριθμος που αναπτύχθηκε ως τμήμα του προγράμματος CAST είναι ο CAST-128. Στον αλγόριθμο αυτό χρησιμοποιείται μέγεθος κλειδιού με τιμές μεταξύ 40 και 128 bits, με βήματα των 8 bits. Το CAST είναι το αποτέλεσμα μιας μακράς χρονικά διαδικασίας έρευνας και ανάπτυξης και έχει ενσωματώσει σειρά σχολίων από κρυπταναλυτές. Σε πρώτη φάση είχε χρησιμοποιηθεί σε διάφορα προϊόντα, συμπεριλαμβανομένου και του PGP.

Αλγόριθμος Safer

Πρόκειται για ακόμα έναν αλγόριθμο Τμήματος (Block Cipher).Ο αλγόριθμος SAFER K-64, συγκεκριμένα, έχει αρχικό μήνυμα 64 bit και blocks κρυπτογραφημάτων. Αποτελείται από r

όμοιους γύρους, ακολουθούμενους από μια έξοδο μετασχηματισμού. Ο SAFER αποτελείται ολοκληρωτικά από απλές λειτουργίες byte, εκτός από τις περιστροφές byte στο πρόγραμμα κλειδιού. Επομένως, είναι κατάλληλος για επεξεργαστές με μικρό μέγεθος λέξεων όπως είναι οι chipcards.

Αλγόριθμος Twofish

Ο συγκεκριμένος αλγόριθμος σχεδιάστηκε στηριζόμενος στον κρυπτογραφικό αλγόριθμο AES. Είναι ένας αλγόριθμος Τμήματος (Block Cipher) με μέγεθος τμήματος 128 bits. Το κλειδί που χρησιμοποιεί μπορεί να έχει μέγεθος 128 bits, 192 bits και 256 bits. Η χρήση του υποστηρίζεται από πληθώρα λογισμικών προγραμμάτων, από διαφορετικά λειτουργικά συστήματα, καθώς και από διάφορα είδη τεχνολογίας επεξεργαστών. Σε περίπτωση που ο χρήστης που επιλέγει το μέγεθος του κλειδιού επιλέξει κάποιον άλλον αριθμό, τότε ο αλγόριθμος μόνος του το προσαρμόζει στο κοντινότερο δυνατό μέγεθος. Δεν χρησιμοποιούνται ποτέ αδύναμα κλειδιά. Ο Twofish, είναι ιδιαίτερα ανθεκτικός στις επιθέσεις και το επίπεδο ασφάλειας που παρέχει είναι πολύ υψηλό.

3.2.2 Σύγκριση βασικών Block Ciphers αλγορίθμων

Από τους πολλούς αλγόριθμους που χρησιμοποιούνται στις μέρες μας οι διαφορά τους έγκειται στην πολυπλοκότητα τους, και στην ικανότητα τους να «σπάσουν». Ενώ το κομμάτι της κρυπτογράφησης διαφέρει σε κάθε αλγόριθμο, όλοι τους έχουν κοινό στόχο να διατηρήσουν την πληροφορία όσο πιο κρυφή γίνεται.

DES: Χρησιμοποιώντας απλές επιθέσεις (simple brute force attacks) ο DES παραβιάστηκε σε λιγότερες από εικοσιτέσσερις ώρες. Για αυτό θεωρείται ξεπερασμένος και εύκολα παραβιάσιμος αλγόριθμος.

TRIPLE DES: Έλυσε το πρόβλημα του μικρού μήκους κλειδιού (56 bit) , κάτι που αποτελεί προφύλαξη από επιθέσεις. Ενώ θεωρητικά φαίνεται πως είναι εύκολο να παραβιαστεί, πρακτικά δεν γίνεται. Θεωρείται ασφαλής και χρησιμοποιείται κυρίως σε οικονομικές συναλλαγές.

RC4: Παρότι είναι αρκετά ασφαλής για τις εφαρμογές που χρησιμοποιείται (SSL,WEP), είναι ευάλωτος σε επιθέσεις επειδή δεν είναι αρκετά «τυχαίος» όσο είναι απαραίτητο για την κρυπτογράφηση. Για αυτό δεν προτείνεται για νέες εφαρμογές που χρειάζονται υψηλά επίπεδα ασφάλειας.

Blowfish: Είναι ένας από τους πιο γρήγορους αλγόριθμους παρόλα αυτά μειώνεται σημαντικά η ταχύτητα του σε περιπτώσεις αλλαγής κλειδιών. Αυτό τον κράτησε μακριά από κάποιες εφαρμογές. Δημιουργήθηκε για να επιτρέπει στον καθένα να χρησιμοποιεί την κρυπτογραφία χωρίς πρότυπα και πνευματικά δικαιώματα.

Rijndael: Χρησιμοποιείται για απόρρητες και μη κυβερνητικές πληροφορίες και θεωρείται πρακτικά ασφαλής από επιθέσεις, παρότι θεωρητικά φαίνεται πιθανό να παραβιαστεί. Επιθέσεις τύπου brute force attack εναντίον του αποδείχτηκαν μη αποδοτικές. Επιθέσεις τύπου side channel attacks , όπου επιτίθενται στις εφαρμογές και όχι στον ίδιο τον

αλγόριθμο, έχουν αποδείξει πως είναι πιθανή η παραβίαση του αλγορίθμου, αλλά όχι πρακτικά εκτός αν τρέχουν στον ίδιο εξυπηρετητή με την εφαρμογή.

Στις παρακάτω Εικόνες 11 και 12 βλέπουμε συνοπτικά και συγκριτικά τα βασικά στοιχεία των παραπάνω αλγορίθμων.

Αλγόριθμος	Δημιουργοί	Μέγεθος Κλειδιού	Μέγεθος Τμήματος	Δομή Αλγορίθμου	Κύκλοι	Έχει σπάσει	Υπάρχουσες επιθέσεις
Rijndael	Joan Daemen & Vincent Rijmen το 1998	128 bits, 192 bits, 256 bits	128 Bits	Δίκτυο μεταθέσεων - αντικαταστάσεων	10, 12 ή 14	Όχι	Επιθέσεις πλευρικού καναλιού
Blowfish	Bruce Schneier το 1993	32-448 bit σε βήματα των 8 bits. 128 bits προεπιλογή	64 bits	Δίκτυο Feistel	16	Όχι	Δεύτερης τάξης διαφορική επίθεση
RC4	Ron Rivest το 1987	Ποικίλουν	Ποικίλουν	Ροής	άγνωστο	Ναι	Διάκριση με βάση το χρονοδιάγραμμα αδύναμου κλειδιού
TripleDES	IBM το1978	112 bits ή 168 bits	64 bits	Δίκτυο Feistel	48	Όχι	Πιθανώς σε θεωρητικό επίπεδο
DES	IBM το 1975	56 bits	64 bits	Δίκτυο Feistel	16	Ναι	Επίθεση ωμής βίας (Brute force attack), διαφορική κρυπτανάλυση, γραμμική κρυπτανάλυση επίθεση Davies'

Εικόνα 11: Συγκριτικά στοιχεία αλγορίθμων

Αλγόριθμοι	Μήκος Κλειδιού	Ισχύς	Παρατηρήσεις
DES	64	Αδύναμος	Αποτέλεσε το Αμερικανικό πρότυπο ασύμμετρης κρυπτογράφησης δεδομένων το 1981 χρησιμοποιούμενο από το 1976. Κρυπτογραφεί ανά τμήματα 64 bits, χρησιμοποιώντας κλειδί 56 bits (ή 64 με τα 8 bits ισοτιμίας).
Triple DES	(161), 112, 168	Ισχυρός	Κρυπτογραφεί το κείμενο τρεις φορές, χρησιμοποιώντας διαφορετικό κλειδί κάθε φορά.
AES	28,192,256	Ισχυρός	Πρόκειται για επέκταση του DES
IDEA	64,128	Ισχυρός	Θεωρείται από τους ασφαλέστερους. Είναι δομημένος όπως ο DES και κρυπτογραφεί τμήματα των 64 bits.
BLOWFISH	32,448	Αδύναμος	Κρυπτογραφεί τμήματα των 64 bits και έχει μεταβλητό μήκος κλειδιού με μέγιστο τα 448 bits.Είναι ταχύτερος από

			τον DES.
RC5	32,64,128	Αδύναμος	Αποτελεί παραλλαγή του RC4 και RC6. Έχει μεταβλητό μήκος κλειδιού, λειτουργεί σε επίπεδο byte, θεωρείται εξαιρετικά ασφαλής και ταχύς και είναι ευρύτερα χρησιμοποιούμενος.

Εικόνα 12: Συγκριτικά στοιχεία αλγορίθμων

3.2.3 Κρυπτογραφικοί αλγόριθμοι Ροής (Stream Ciphers)

Οι κρυπτογραφικοί αλγόριθμοι Ροής (Stream Ciphers) κρυπτογραφούν μια ροή μηνύματος χωρίς να την διαχωρίζουν σε τμήματα και λειτουργούν κρυπτογραφώντας το μήνυμα bit προς bit ή byte προς byte κάθε φορά με μια απλή κρυπτογραφική συνάρτηση. Η κρυπτογράφηση για μια ροή (stream) γίνεται με ένα σταθερό εναλλασσόμενο κλειδί. Με άλλα λόγια, οι stream ciphers τυπικά λειτουργούν με μικρότερες μονάδες απλού κειμένου, συνήθως με bits και κρυπτογραφούν μεμονωμένους χαρακτήρες (συνήθως δυαδικά ψηφία) ενός αρχικού μηνύματος, χρησιμοποιώντας ένα μετασχηματισμό κρυπτογράφησης που ποικίλλει με το χρόνο. Είναι εξαιρετικά γρήγοροι αλγόριθμοι, κατά πολύ γρηγορότεροι από τους block ciphers και έχουν λιγότερο πολύπλοκα στοιχεία κυκλώματος.

Οι κρυπτογραφικοί αλγόριθμοι ροής χωρίζονται σε δυο υποκατηγορίες ανάλογα με το αν έχουν τη δυνατότητα να συνεχίσουν τη διαδικασία της κρυπτογράφησης - αποκρυπτογράφησης σε περίπτωση λανθασμένης μεταβίβασης δεδομένων. Πρόκειται για τους «συγχρονους» και τους «ασυγχρονους».

1) Στους σύγχρονους αλγορίθμους ροής, η επόμενη κατάσταση που θα βρίσκεται το σύστημα είναι ανεξάρτητη τόσο από το κείμενο που κρυπτογραφείται, όσο και από το κρυπτογραφημένο κείμενο. Σε ένα τέτοιο αλγόριθμο, αν μεταβιβαστεί ένα bit λανθασμένα, τότε δεν θα επηρεαστεί η αποκρυπτογράφηση των επόμενων bits.

2) Στους ασύγχρονους αλγορίθμους ροής, η κατάσταση στην οποία βρίσκεται το σύστημα, είναι άμεσα εξαρτημένη από την το κείμενο που έχει προηγουμένως αποκρυπτογραφηθεί. Αυτό έχει σαν αποτέλεσμα αν μεταβιβαστεί ένα bit λανθασμένα, τα επόμενα bits να μη μπορούν να αποκρυπτογραφηθούν σωστά. Για αυτό το λόγο, οι αλγόριθμοι αυτοί ανά τακτά διαστήματα στέλνουν ειδικά μηνύματα επανασυγχρονισμού. Έτσι αν η τρέχουσα κατάσταση εξαρτάται από n προηγούμενες καταστάσεις, τότε σε n αποκρυπτογραφήσεις το πολύ, το λάθος θα γίνει αντιληπτό και θα γίνει επανασυγχρονισμός. Για το λόγο αυτό, οι αλγόριθμοι αυτοί ονομάζονται και «αυτοσυγχρονιζόμενοι». Η ιδιότητα των ασύγχρονων αλγορίθμων ροής να εξαρτώνται από n προηγούμενες καταστάσεις, μπορεί να θεωρηθεί ως μειονέκτημα, αφού κάποιος ο οποίος θέλει να κρυπταναλύσει τον αλγόριθμο χωρίς να γνωρίζει το κλειδί, ίσως να έχει αρκετά δεδομένα. Παρόλα αυτά, υπάρχουν πολύ λίγες αναφορές τέτοιων αλγορίθμων.

3.3 Πλεονεκτήματα και μειονεκτήματα συμμετρικής κρυπτογράφησης

Α) Πλεονεκτήματα συμμετρικής κρυπτογράφησης

1) Οι κρυπτογραφήσεις συμμετρικού κλειδιού σχεδιάζονται για να έχουν υψηλούς ρυθμούς αποτελεσμάτων δεδομένων. Μερικές εφαρμογές hardware πετυχαίνουν κρυπτογράφηση που κυμαίνεται σε εκατοντάδες megabytes το δευτερόλεπτο ενώ εφαρμογές λογισμικού ίσως επιτυγχάνουν ρυθμούς στα megabytes ανά δευτερόλεπτο.

2) Τα κλειδιά για την κρυπτογραφία συμμετρικού κλειδιού είναι σχετικά μικρά.

3) Οι κρυπτογραφήσεις συμμετρικού κλειδιού μπορούν να χρησιμοποιηθούν για την κατασκευή κρυπτογραφικών μηχανισμών, συμπεριλαμβανομένων μηχανών παραγωγής ψευδοτυχαίων αριθμών, συναρτήσεις κατακερματισμού και υπολογιστικά, επαρκή σχήματα ψηφιακών υπογραφών.

4) Η κρυπτογραφία συμμετρικού κλειδιού μπορεί να δημιουργήσει ισχυρότερες κρυπτογραφήσεις (ciphers). Απλοί μετασχηματισμοί, που είναι εύκολο να αναλυθούν, μπορούν να χρησιμοποιηθούν για τη δημιουργία ισχυρών προϊόντων κρυπτογράφησης.

5) Η κρυπτογράφηση συμμετρικού κλειδιού θεωρείται ότι έχει μεγάλη ιστορία, αν και πρέπει να αναγνωριστεί ότι παρά την ανακάλυψη των μηχανών rotor νωρίτερα, η περισσότερη γνώση σε αυτόν τον τομέα αποκτήθηκε με τη μεταγενέστερη ανακάλυψη του ψηφιακού υπολογιστή.

Β) Μειονεκτήματα συμμετρικής κρυπτογράφησης

1) Σε μια επικοινωνία που συμμετέχουν δύο, το κλειδί πρέπει να διατηρείται μυστικό και από τους δύο.

2) Σε ένα μεγάλο δίκτυο, υπάρχουν πολλά ζευγάρια κλειδιών για να χειριστούμε. Επομένως, η αποτελεσματική διαχείριση κλειδιού απαιτεί τη χρήση ενός έμπιστου TTP.

3) Στην επικοινωνία ανάμεσα στις οντότητες Α και Β, υγιής κρυπτογραφική πρακτική υπαγορεύει ότι το κλειδί αλλάζει συχνά και ίσως για κάθε τμήμα της επικοινωνίας.

4) Μηχανισμοί ψηφιακών υπογραφών που προκύπτουν από την κρυπτογραφία συμμετρικού κλειδιού, απαιτούν συνήθως είτε μεγάλα κλειδιά για την επιβεβαίωση της δημόσιας λειτουργίας είτε τη χρήση ενός TTP.

ΚΕΦΑΛΑΙΟ 4

ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

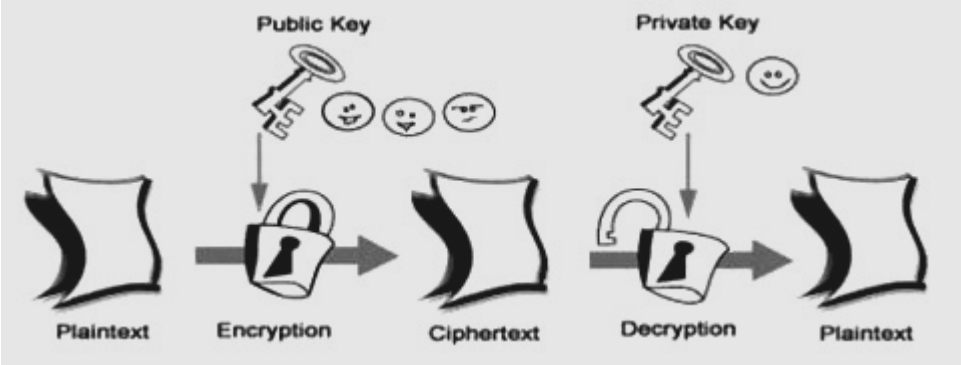
Στο κεφάλαιο αυτό γίνεται ανάλυση του τρόπου λειτουργίας της Ασύμμετρης Κρυπτογράφησης και των αντίστοιχων κρυπτογραφικών αλγορίθμων που περιλαμβάνει. Επίσης, παρουσιάζεται η διαδικασία της Ψηφιακής ή Ηλεκτρονικής Υπογραφής, η Υβριδική Κρυπτογραφία Ψηφιακού Φακέλου και τα Προσωπικά ψηφιακά πιστοποιητικά.

Για το κεφάλαιο αυτό χρησιμοποιήθηκαν στοιχεία από τις πηγές [1], [4], [5], [6], [7], [9],[15].

4.1 Ασύμμετρη Κρυπτογράφηση ή Κρυπτογράφηση δημόσιου κλειδιού (Asymmetric Cryptography ή Public key Cryptography)

Η κρυπτογράφηση δημοσίου κλειδιού (Εικόνα 13) αναπτύχθηκε κατά τη διάρκεια της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman οι οποίοι πρότειναν μια νέα τεχνική για τον περιορισμό των προβλημάτων της συμμετρικής κρυπτογράφησης. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί (ή συμμετρικό, ή ιδιωτικό) όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης τα οποία έχουν δημιουργηθεί από μια γεννήτρια κλειδιών. Το ένα ονομάζεται ιδιωτικό κλειδί (private key) και το άλλο δημόσιο κλειδί (public key). Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί θα πρέπει να το ανακοινώνει σε όλη την διαδικτυακή κοινότητα. Υπάρχουν δε και ειδικοί εξυπηρετητές δημοσίων κλειδιών (public key servers) στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό. Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού.



Εικόνα 13: Διαδικασία Ασύμμετρης Κρυπτογράφησης

Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού καθώς είναι υπολογιστικά αδύνατη. Θεωρητικά, βέβαια, το ιδιωτικό κλειδί μπορεί πάντα να υπολογιστεί αλλά το κόστος σε χρόνο, μνήμη και υπολογιστική ισχύ για κάτι τέτοιο είναι τόσο μεγάλο που καθίσταται πρακτικά αδύνατο.

4.2 Περιγραφή της διαδικασίας Ασύμμετρης Κρυπτογράφησης

Για κάθε χρήστη παράγεται ένα ζεύγος κλειδιών, το οποίο θα χρησιμοποιηθεί για την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων. Κάθε χρήστης τοποθετεί το δημόσιο κλειδί σε μία βάση δεδομένων στο φορέα ή σε κάποιο άλλο προσβάσιμο αρχείο. Το άλλο κλειδί, το ιδιωτικό, διαφυλάσσεται διατηρώντας τη μυστικότητά του. Για επίτευξη στοιχειώδους λειτουργικότητας, απαιτείται κάθε χρήστης να είναι σε θέση με ευκολία να ανακτήσει τα δημόσια κλειδιά των άλλων. Στη συνέχεια, ο αποστολέας κρυπτογραφεί το μήνυμα που επιθυμεί να στείλει χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη. Ο παραλήπτης με τη σειρά του λαμβάνει το μήνυμα και το αποκρυπτογραφεί με το ιδιωτικό του κλειδι. Κανένας άλλος δεν μπορεί να αποκρυπτογραφήσει το μήνυμα, αφού μόνο ο παραλήπτης γνωρίζει το ιδιωτικό του κλειδί, που σχετίζεται μοναδικά με το αντίστοιχο δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση. Τέλος, όλοι οι συμμετέχοντες θα πρέπει να έχουν πρόσβαση στα δημόσια κλειδιά, ενώ τα ιδιωτικά κλειδιά να παράγονται τοπικά για τον κάθε συμμετέχοντα ώστε να διασφαλίζεται αυστηρά η μυστικότητα τους. Οποιαδήποτε στιγμή, ο χρήστης μπορεί να τροποποιήσει το ιδιωτικό του κλειδί και ταυτοχρόνως να δημοσιεύσει το αντίστοιχο νέο δημόσιο κλειδί, έτσι ώστε να αντικατασταθεί το προηγούμενο μη ισχύον πλέον δημόσιο κλειδί.

4.3 Κρυπτογραφικοί αλγόριθμοι ασύμμετρης κρυπτογράφησης και περιγραφή τους

Οι βασικοί κρυπτογραφικοί αλγόριθμοι που έχουν αναπτυχθεί στην ασύμμετρη κρυπτογράφηση είναι οι εξής: RSA, Diffie – Hellman (ανταλλαγή κλειδιών), ECC (Κρυπτογράφηση ελλειπτικών καμπυλών), DSA, Paillier, El Gamal, Rabin. Άλλοι αλγόριθμοι οι οποίοι αφορούν στην ψηφιακή υπογραφή η οποία σχετίζεται άμεσα με την ασύμμετρη κρυπτογράφηση είναι οι GOST, Ong – Schnorr – Shamir και ESIGN.

Αλγόριθμος RSA

Ο αλγόριθμος RSA αναπτύχθηκε στα τέλη της δεκαετίας του 1970 από τους Rivest, Shamir και Adleman. Η ασφάλεια του συστήματος αυτού βασίζεται στη δυσκολία εύρεσης παραγόντων πολύ μεγάλων αριθμών ώστε να αποκτήσει ο χρήστης ένα ζεύγος κλειδιών. Ο RSA είναι σημαντικός γιατί επιτρέπει ψηφιακές υπογραφές που χρησιμοποιούνται για να πιστοποιήσουν ηλεκτρονικά έγγραφα με τον ίδιο ακριβώς τρόπο που οι ιδιόχειρες υπογραφές χρησιμοποιούνται για να πιστοποιήσουν έντυπα έγγραφα. Είναι ενσωματωμένος σε διάφορους φυλλομετρητές (browsers) παγκοσμίου ιστού όπως ο NetScape και τον χρησιμοποιούν τα περισσότερα προϊόντα και πρότυπα που χρησιμοποιούν ασύμμετρα κρυπτοσυστήματα για κρυπτογράφηση και ψηφιακή υπογραφή. Η παραβίαση του αλγορίθμου RSA προσανατολίζεται σε δύο τρόπους. Ο πρώτος είναι της εξαντλητικής αναζήτησης όπου δοκιμάζονται όλα τα πιθανά ιδιωτικά κλειδιά. Όσο μεγαλύτερο πλήθος bits χρησιμοποιείται, τόσο πιο ασφαλής είναι ο αλγόριθμος. Παρόλα αυτά, επειδή απαιτούνται

πολύπλοκοι υπολογισμοί τόσο κατά την δημιουργία των κλειδιών όσο και κατά την κρυπτογράφηση και την αποκρυπτογράφηση, όσο μεγαλύτερο είναι το μέγεθος των κλειδιών τόσο βραδύτερος θα είναι και ο ρυθμός λειτουργίας του συστήματος. Ο δεύτερος τρόπος επικεντρώνεται στη διαδικασία ανεύρεσης δύο πρώτων αριθμών που είναι παράγοντες του n. Για έναν μεγάλο αριθμό n, η διαδικασία αποτελεί δύσκολο πρόβλημα αλλά όχι σε μεγάλο βαθμό όσο ήταν τα προηγούμενα χρόνια.
Οι σχεδιαστές του RSA, τον Ιανουάριο του 1997, προσέφεραν αμοιβή 100 δολαρίων σε όποιον αποκρυπτογραφούσε ένα κρυπτογραφημένο κείμενο που είχαν δημοσιεύσει στο περιοδικό Scientific American. Εκτιμούσαν ότι κάτι τέτοιο ήταν αδύνατο να συμβεί στα επόμενα 40τετράκις εκατομμύρια χρόνια. Όμως τον Απρίλιο του 1994 μια ερευνητική ομάδα κέρδισε το βραβείο μετά από 8 μήνες προσπάθειας αξιοποιώντας την υπολογιστική ισχύ 1600 υπολογιστών στο Internet. Χρησιμοποιήθηκε δημόσιο κλειδί μεγέθους 129 δεκαδικών ψηφίων, δηλαδή περίπου 428 bits. Επιπλέον, το 1996 αναλύθηκε σε γινόμενο πρώτων παραγόντων ένας αριθμός 130 ψηφίων με 10 φορές λιγότερες πράξεις από όσες είχαν απαιτηθεί κατά την ανάλυση του αριθμού με 129 ψηφία. Τα αποτελέσματα αυτά, βεβαίως, με κανένα τρόπο δε μειώνουν τις δυνατότητες του RSA. Απλώς σημαίνουν ότι πρέπει να χρησιμοποιούνται μεγαλύτερα μεγέθη κλειδιών. Ένα κλειδί μεγέθους 2048 bits θεωρείται ισχυρό για όλες τις σημερινές τυπικές εφαρμογές. Η ισχύς του RSA είναι τόσο μεγάλη που η κυβέρνηση των ΗΠΑ έχει περιορίσει σημαντικά την εξαγωγή του αλγορίθμου σε ξένες χώρες.
Μερικά από τα πλεονεκτήματα που παρέχει ο RSA, τα οποία βοήθησαν στην υλοποίηση πιο ασφαλών και ευκολότερα διαχειρίσιμων συναλλαγών, είναι η απλοποίηση του προβλήματος της διαχείρισης κλειδιών καθώς σε ένα κρυπτοσύστημα δημοσίου κλειδιού η σχέση που συνδέει τον αριθμό των χρηστών με τον αριθμό των κλειδιών είναι γραμμική και για αυτό το λόγο εύκολα διαχειρίσιμη ακόμα και όταν ο αριθμός των χρηστών είναι πολύ μεγάλος. Επίσης, είναι η ενισχυμένη ασφάλεια των συναλλαγών, καθώς, κάθε χρήστης παράγει μόνος του και για δική του χρήση ένα ζεύγος κλειδιών. Το ιδιωτικό κλειδί θα πρέπει να μένει μυστικό και κρυφό από οποιαδήποτε μη εξουσιοδοτημένη οντότητα εξαλείφοντας έτσι όχι μόνο το πρόβλημα της μεταφοράς του αλλά και την απαίτηση για την εγκατάσταση ενός ασφαλούς διαύλου επικοινωνίας. Το δημόσιο κλειδί από την άλλη είναι ευρέως διαθέσιμο και άρα μπορεί να μεταφερθεί με οποιαδήποτε βολική μέθοδο σε ένα δίκτυο χωρίς να τίθεται θέμα για την διατήρηση της μυστικότητάς του.

Αλγόριθμος Diffie - Hellman και Ανταλλαγή κλειδιών

Η τεχνική - πρωτόκολλο Diffie-Hellman παρουσιάστηκε το 1976 από τους Whitfield Diffie και Martin Hellman. Πριν από τη δημιουργία αυτού κάθε κρυπτογραφική τεχνική βασιζόταν σε κάποιο προσυμφωνημένο κλειδί. Το συγκεκριμένο πρωτόκολλο είναι το πρώτο που προτάθηκε ώστε να επιτρέπει σε δυο οντότητες, χωρίς προηγούμενη επικοινωνία, να ανταλλάξουν ένα κοινό κλειδί μέσω ενός μη ασφαλούς διαύλου επικοινωνίας. Ένας σημαντικός αριθμός προϊόντων υιοθέτησε αυτή την τεχνική.
Σκοπός του αλγορίθμου είναι να καταστήσει εφικτή και ασφαλή μεταξύ δύο χρηστών την ανταλλαγή ενός μυστικού κλειδιού, το οποίο ακολούθως θα χρησιμοποιηθεί για κρυπτογράφηση μηνυμάτων. Ο αλγόριθμος περιορίζεται ακριβώς στην ανταλλαγή των κλειδιών. Η αποτελεσματικότητα του βασίζεται στη δυσκολία υπολογισμού διακριτών λογαρίθμων και για μεγάλους πρώτους αριθμούς το πρόβλημα θεωρείται ανέφικτο να επιλυθεί.

Κρυπτογράφηση ελλειπτικών καμπυλών - ECC (Elliptic Curve Cryptography)

Όπως προαναφέρθηκε, τα περισσότερα προϊόντα και πρότυπα που χρησιμοποιούν ασύμμετρα κρυπτοσυστήματα για κρυπτογράφηση και ψηφιακή υπογραφή χρησιμοποιούν τον αλγόριθμο RSA. Το πλήθος των bits που χρησιμοποιείται για ασφαλή χρήση του RSA έχει αυξηθεί σημαντικά τα τελευταία χρόνια και το γεγονός αυτό έχει επιβαρύνει τις αντίστοιχες εφαρμογές με σημαντικό επεξεργαστικό φόρτο. Το πρόβλημα εντείνεται σε περιβάλλον ιστοσελίδων εφαρμογών ηλεκτρονικού εμπορίου, όπου πραγματοποιούνται πολλές ασφαλείς δοσοληψίες. Τα τελευταία χρόνια έχει αρχίσει να αναπτύσσεται ένα ανταγωνιστικό σύστημα του RSA. Πρόκειται για την Κρυπτογράφηση Ελλειπτικής Καμπύλης (ECC). Ήδη, το ECC κινείται στα πλαίσια προτυποποίησής του, αφού έχει συμπεριλάβει το πρότυπο για ασύμμετρα κρυπτοσυστήματα IEEE P1363.
Ο κύριος λόγος που καθιστά ελκυστικό το ECC συγκρινόμενο με το RSA, είναι ότι προσφέρει το ίδιο επίπεδο ασφαλείας για μικρότερο πλήθος bits, μειώνοντας κατ' αυτόν τον τρόπο τον απαιτούμενο υπολογιστικό χρόνο και φόρτο εργασίας. Σύμφωνα με σχετικά πρόσφατες επιστημονικές ανακοινώσεις, έγινε κατορθωτό να κρυπταναλυθεί το ECC με μέγεθος κλειδιού 109 bits αξιοποιώντας αδιάκοπα την επεξεργαστική ισχύ 10.000 υπολογιστών επί 549 ημέρες. Στην παρούσα φάση ο αλγόριθμος θεωρείται ασφαλής αν το μέγεθος του κλειδιού διατηρεί μήκος τουλάχιστον 163 bits. Από την άλλη πλευρά, αν και η θεωρία του ECC ήταν γνωστή για αρκετό καιρό, μόλις πρόσφατα έχουν ξεκινήσει να εμφανίζονται προϊόντα που τον χρησιμοποιούν. Το γεγονός αυτό δικαιολογεί το χαμηλό επίπεδο εμπιστοσύνης προς το ECC, σχετικά με το RSA.
Το ECC σε θεωρητική βάση είναι πιο δύσκολο να εξηγηθεί, συγκριτικά με τους αλγορίθμους RSA και Diffie-Hellman. Η αξιοποιηθείσα τεχνική βασίζεται στη χρήση ενός μαθηματικού μοντέλου, γνωστού ως ελλειπτική καμπύλη.

Αλγόριθμος DSA (Digital Secure Algorithm)

Το DSA είναι ένας αλγόριθμος ο οποίος χρησιμοποιείται αποκλειστικά για ψηφιακές υπογραφές και την πιστοποίησή τους. Προτάθηκε τον Αύγουστο του 1991 από το NIST (National Institute of Standards and Technology) της Αμερικής. Έχει προτυποποιηθεί ως FIPS 186 (Federal Information Processing Standard) και το πρότυπο αυτό έχει ονομαστεί DSS (Digital Signature Standard) και είναι ο πρώτος αλγόριθμος ψηφιακής υπογραφής που αναγνωρίστηκε παγκόσμια. Ο DSA αποτελεί μια παραλλαγή του αλγορίθμου ElGamal για ψηφιακές υπογραφές και σχεδιάστηκε αποκλειστικά για τη δημιουργία και επαλήθευση ψηφιακών υπογραφών και κατά συνέπεια και για τον έλεγχο της ακεραιότητας των δεδομένων. Η λογική του αλγορίθμου βασίζεται σε αυτήν της ασύμμετρης κρυπτογραφίας, αφού και σε αυτήν την περίπτωση κάθε οντότητα δημιουργεί ένα ζεύγος δημοσίου και ιδιωτικού κλειδιού. Ως αλγόριθμος είναι πιο αργός από το RSA. Η ασφάλειά του βασίζεται στη δυσκολία του υπολογισμού διακριτών λογαρίθμων μέσα σε ένα πεπερασμένο σώμα. Έρευνες πάνω στον αλγόριθμο έχουν δείξει την ύπαρξη πρώτων αριθμών οι οποίοι θα μπορούσαν να οδηγήσουν στη δημιουργία κλειδιών ευάλωτων σε επιθέσεις. Όμως, αυτοί οι αριθμοί είναι ελάχιστοι και μπορούν εύκολα να αποφευχθούν σε μία σωστή διαδικασία δημιουργίας ζεύγους κλειδιών. Από το 1996 προτείνεται το μέγεθος του δημόσιου κλειδιού p να είναι τουλάχιστον 768 bits. Το πρότυπο FIPS 186 δεν επιτρέπει πρώτους αριθμούς p που το μέγεθός τους ξεπερνά τα 1024 bits. Ένα σημαντικό πλεονέκτημα του DSA είναι ότι, η εκθετοποίηση ως διαδικασία μπορεί να προηγείται της δημιουργίας της ψηφιακής υπογραφής, κάτι που δεν είναι εφικτό με τον RSA.

4.4 Ψηφιακή ή ηλεκτρονική υπογραφή (Digital signature)

Η αναφορά στον όρο ψηφιακή υπογραφή προσδίδει συνειρμικά και λογικά την παραδοσιακή ιδιόχειρη υπογραφή στα έντυπα έγγραφα με την οποία υποδηλώνεται η ταυτότητα, η βούληση, η συμφωνία και η εγγύηση του υπογράφοντα να δεσμευτεί νομικά ως προς το περιεχόμενο του υπογεγραμμένου εγγράφου, προκειμένου να μην μπορεί να υπάρξει αποκήρυξη της υπογραφής σε μελλοντική περίπτωση. Όταν αναφερόμαστε σε ηλεκτρονικές υπογραφές εννοούμε τις ψηφιακές υπογραφές που προκύπτουν από κρυπτογραφικούς μηχανισμούς και όχι ιδιόχειρη υπογραφή που προκύπτει μέσω μεταφοράς από ηλεκτρονικά μέσα όπως για παράδειγμα από έναν σαρωτή.

Ο όρος ψηφιακή υπογραφή λοιπόν εννοεί το σύνολο από bits που προσθέτει ο αποστολέας ενός εγγράφου σε αυτό ή είναι συνημμένα ή συσχετίζεται λογικά με αυτό. Πρωταρχικός λόγος χρησιμοποίησής είναι να επιβεβαιωθεί ότι τα δεδομένα που στάλθηκαν δεν έχουν τροποποιηθεί, να διασφαλιστεί η μη αποποίηση της αποστολής ενός μηνύματος και να επαληθευτεί ο αποστολέας των δεδομένων.

Κατόπιν σχετικής οδηγίας (1999/93/ΕΚ) του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου, στον ελλαδικό χώρο, εκδόθηκε το προεδρικό διάταγμα 150/2001 που καθιστά ισότιμες και εξομοιώνει πλήρως την ψηφιακή υπογραφή με την ιδιόχειρη υπογραφή.

Αναφέρθηκε προηγουμένως ότι η ψηφιακή υπογραφή είναι παράγωγο της ασύμμετρης κρυπτογράφησης. Πρέπει να σημειωθεί όμως ότι κατά την δημιουργία μιας ψηφιακής υπογραφής δεν κρυπτογραφούνται τα προς υπογραφή δεδομένα , αλλά μια μικρή μαθηματική σύνοψη (digest).

4.4.1 Συνάρτηση κατακερματισμού ή κατατεμαχισμού ή κατάτμησης (Hash Function)

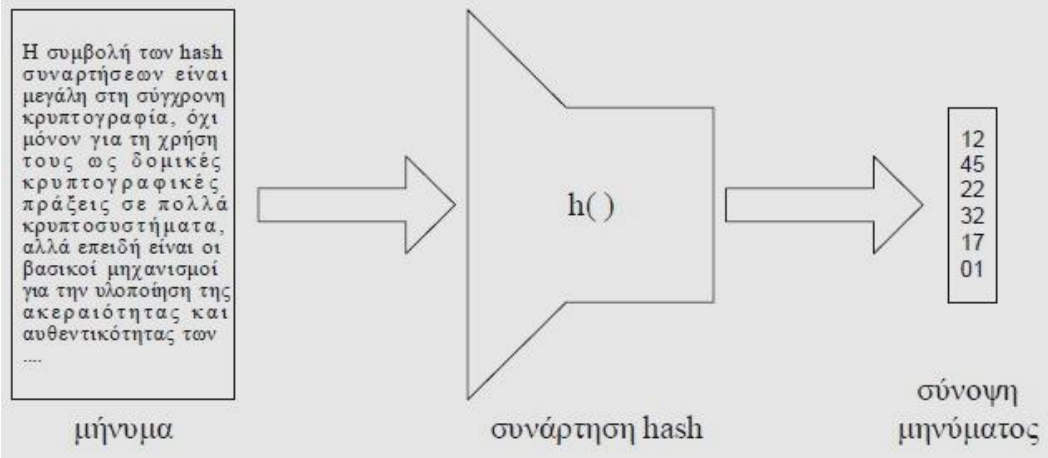
Μια πολύ πρακτική μέθοδος κρυπτογράφησης είναι η συνάρτηση κατακερματισμού ή κατατεμαχισμού ή κατάτμησης (hash function, σύμφωνα με την οποία από κάθε μήνυμα και ανεξαρτήτως του μεγέθους του δημιουργείται μια σύνοψή του, που είναι μια σειρά από bits με συγκεκριμένο πλήθος, για παράδειγμα 128 bits. Η σύνοψη του μηνύματος, που είναι γνωστή με τον όρο fingerprint ή message digest, αποτελεί ψηφιακή αναπαράσταση του μηνύματος και είναι μοναδική για το μήνυμα που αντιπροσωπεύει.

Αν αλλάξουμε έστω και μια τελεία στο μήνυμα, θα αλλάξει και η σύνοψή του, ενώ είναι πρακτικά αδύνατο δύο διαφορετικά μηνύματα να δώσουν την ίδια σύνοψη. Η μεγάλη αυτή ευαισθησία στα δεδομένα εισόδου αποτελεί μια από τις πολυτιμότερες ιδιότητες (δυνατότητες) των συναρτήσεων hash. Είναι επίσης πρακτικά αδύνατο να ανακτηθεί το αρχικό μήνυμα αν είναι γνωστή η σύνοψή του. Ο αποστολέας δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να αποστείλει, χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού και δημιουργείται έτσι μια σειρά από bits με συγκεκριμένο μήκος.

Οι hash συναρτήσεις αποτελούν δομικές κρυπτογραφικές πράξεις σε πολλά κρυπτοσυστήματα αλλά κατεξοχήν αποτελούν βασικούς μηχανισμούς για την υλοποίηση της ακεραιότητας και αυθεντικοποίησης των δεδομένων.

Η συνάρτηση δέχεται ένα συγκριτικά μεγάλο μήνυμα και παράγει μια σύνοψη όπως φαίνεται στην Εικόνα 14. Οι κρυπτογραφικές hash συναρτήσεις δεν ακολουθούν απαραιτήτως όλες τις

ιδιότητές τους. Στην πράξη υπάρχει περίπτωση, ανάλογα με την εφαρμογή, να απαιτούνται μόνο ορισμένες από αυτές. Έτσι, ορίζονται οικογένειες κρυπτογραφικών hash συναρτήσεων οι οποίες χωρίζονται σε μονόδρομες (one way hash functions) και ανθεκτικές σε συγκρούσεις (collision resistance hash functions). Επίσης, οι οικογένειες των κρυπτογραφικών hash συναρτήσεων που χρησιμοποιούνται στην αυθεντικοποίηση και στην ακεραιότητα κατατάσσονται στις κατηγορίες των κωδικών αυθεντικοποίησης (Message Authentication Code, MAC) και των κωδικών ανίχνευσης τροποποίησης (Modification Detection Code, MDC). Η επιλογή του MAC και του MDC εξαρτάται από τις συγκεκριμένες συνθήκες της εφαρμογής καθώς και την υπόθεση της επίθεσης του αντιπάλου.



Εικόνα 14: Δημιουργία σύνοψης μηνύματος

4.4.2 Βήματα διαδικασία υπογραφής, αποστολής και παραλαβής ενός μηνύματος

Τα βήματα που ακολουθούν, περιγράφουν αναλυτικά την διαδικασία υπογραφής, αποστολής και παραλαβής ενός μηνύματος και απεικονίζονται την Εικόνα 15.

α) Ο αποστολέας υπολογίζει την τιμή κατάτμησης του μηνύματος.

β) Στην συνέχεια κρυπτογραφεί την τιμή κατάτμησης με το μυστικό του κλειδί (η τιμή αυτή αποτελεί την ψηφιακή υπογραφή του μηνύματος).

γ) Ο αποστολέας επισυνάπτει την κρυπτογραφημένη τιμή κατάτμησης στο κείμενο.

δ) Ο αποστολέας κρυπτογραφεί το υπογεγραμμένο κείμενο (κείμενο και υπογραφή) με το δημόσιο κλειδί του παραλήπτη.

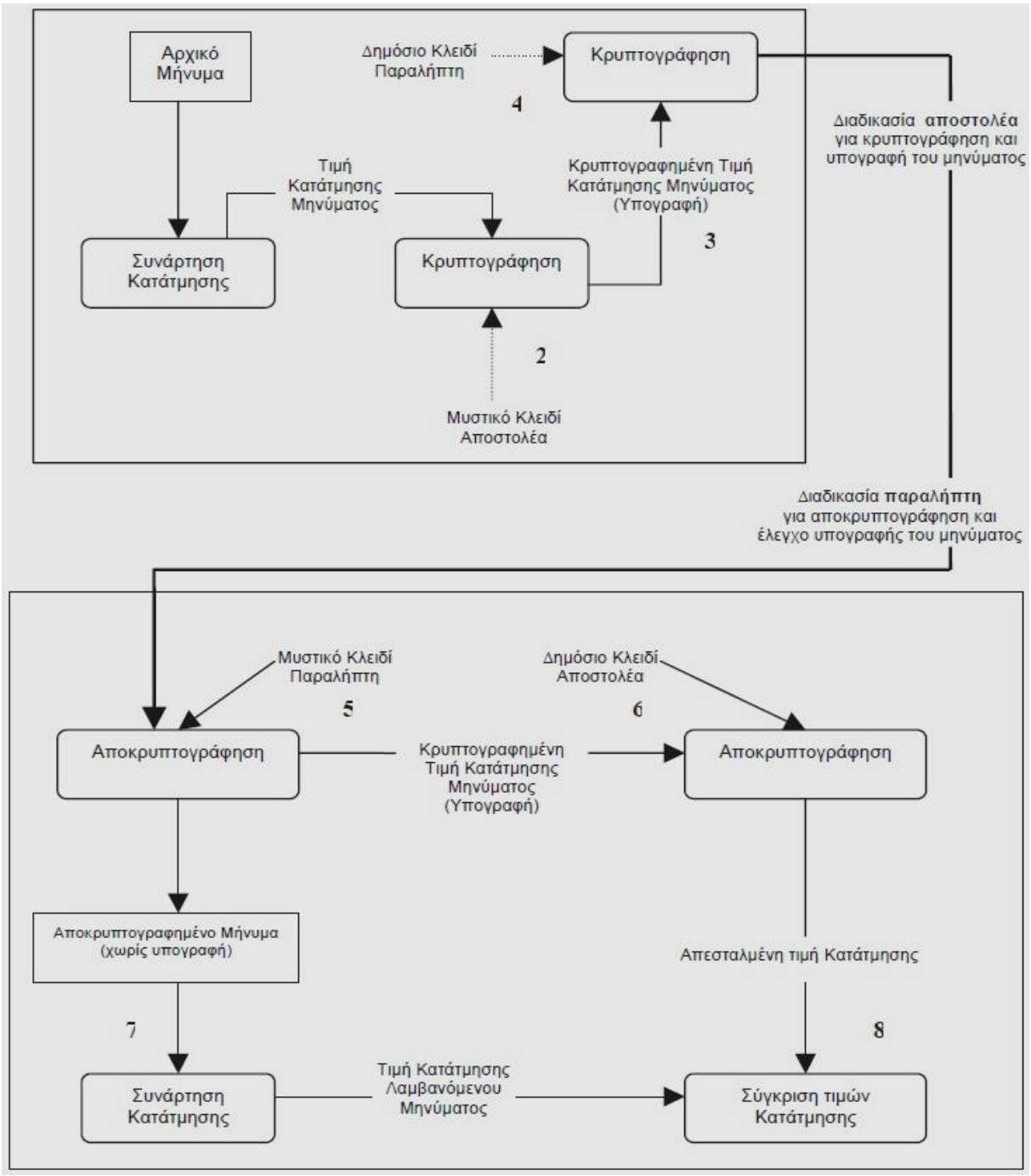
ε) Ο παραλήπτης παραλαμβάνει το υπογεγραμμένο κείμενο και χρησιμοποιεί το προσωπικό του μυστικό κλειδί για να το αποκρυπτογραφήσει.

στ) Έπειτα χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για να εξάγει την τιμή κατάτμησης από την υπογραφή.

ζ) Ο παραλήπτης, χρησιμοποιεί την ίδια συνάρτηση κατάτμησης για να υπολογίσει την τιμή κατάτμησης του παραληφθέντος κειμένου. Δηλαδή, εφαρμόζει στο κανονικό κείμενο τον ίδιο αλγόριθμο κατακερματισμού, ώστε να δημιουργήσει μια δική του σύνοψη.

η) Τέλος, ο παραλήπτης συγκρίνει τις δύο τιμές κατάτμησης. Αν προκύψει ασυμφωνία, τότε είτε το περιεχόμενο του κειμένου έχει αλλοιωθεί κατά τη διάρκεια της μεταφοράς, είτε ο αποστολέας δεν είναι πράγματι αυτός ο οποίος ισχυρίζεται ότι είναι.

Οι πιο ευρέως διαδεδομένοι αλγόριθμοι που χρησιμοποιούνται για τη δημιουργία και επαλήθευση των ψηφιακών υπογραφών είναι οι DSA και RSA.



Εικόνα 15: Βήματα διαδικασία υπογραφής, αποστολής και παραλαβής ενός μηνύματος

4.5 Υβριδική Κρυπτογραφία Ψηφιακού Φακέλου

Ιδιαίτερο ενδιαφέρον για την επίτευξη ασφαλούς επικοινωνίας μεταξύ δύο μερών παρουσιάζει η υβριδική κρυπτογραφία που είναι γνωστή και ως ψηφιακός φάκελος (digital envelope) και αξιοποιεί ταυτόχρονα τις τεχνικές συμμετρικής και ασύμμετρης κρυπτογραφίας. Η υβριδική αυτή κρυπτογραφία μπορεί να χρησιμοποιηθεί για πολλούς παραλήπτες ταυτόχρονα. Τα βήματα που ακολουθούνται για τη δημιουργία ενός ψηφιακού φακέλου είναι τα εξής:

α) Δημιουργείται ένα συμμετρικό κλειδί με χρήση ενός αλγορίθμου συμμετρικής κρυπτογραφίας (π.χ. του DES).

β) Η αρχική πληροφορία κρυπτογραφείται με το συμμετρικό κλειδί που έχει δημιουργηθεί.

γ) Το συμμετρικό κλειδί κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη.

δ) Τα δύο κρυπτογραφημένα κείμενα αποτελούν τον ψηφιακό φάκελο του παραλήπτη.

Ο παραλήπτης ανοίγει τον ψηφιακό του φάκελο αποκρυπτογραφώντας με το ιδιωτικό κλειδί του το κρυπτογραφημένο συμμετρικό κλειδί. Με χρήση του συμμετρικού κλειδιού ο παραλήπτης αποκρυπτογραφεί το αρχικό κείμενο. Μετά την επίτευξη μιας ασφαλούς επικοινωνίας μεταξύ αποστολέα και παραλήπτη το συμμετρικό κλειδί καταστρέφεται. Η χρήση της υβριδικής κρυπτογραφίας βοήθα στο να ξεπεραστούν κάποιες σημαντικές αδυναμίες της κρυπτογραφίας δημοσίου κλειδιού. Συγκεκριμένα η κρυπτογραφία δημοσίου κλειδιού είναι αρκετά αργή σε σύγκριση με την συμμετρική κρυπτογραφία, ειδικά όταν πρόκειται να κρυπτογραφηθούν μεγάλα μηνύματα.

Ακόμα όμως και στην περίπτωση που ο όγκος των προς κρυπτογράφηση δεδομένων είναι μικρός, έχει καθιερωθεί να χρησιμοποιείται η κρυπτογραφία ψηφιακού φακέλου. Με αυτόν τον τρόπο αποφεύγεται οποιαδήποτε σύγχυση ως προς το αν το αποτέλεσμα της αποκρυπτογράφησης είναι δεδομένα ή συμμετρικό κλειδί.

4.6 Προσωπικά ψηφιακά πιστοποιητικά (Digital certificates)

Τα προσωπικά ψηφιακά πιστοποιητικά πιστοποιούν την ταυτότητα του κατόχου του σε τρίτους και παρέχουν σε αυτούς τα μέσα ελέγχου της εγκυρότητας αυτής της ταυτότητας. Η έκδοσή τους βασίζεται στις αρχές της επιστήμης της Κρυπτογραφίας.

Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται από τους τελικούς χρήστες κατά κύριο λόγο στην επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου. Το κοινό ηλεκτρονικό ταχυδρομείο δεν εξασφαλίζει την ταυτότητα του αποστολέα ούτε την ακεραιότητα του περιεχομένου του μηνύματος, σε αντίθεση με το ασφαλές ηλεκτρονικό. Το τελευταίο, βασίζεται στο πρωτόκολλο S/MIME (Secure Multipurpose Internet Mail Extensions), που υποστηρίζεται από τις τελευταίες εκδόσεις λογισμικού διαχείρισης ηλεκτρονικού ταχυδρομείου (π.χ. Outlook Express, Mozilla Thunderbird). Κατά κύριο λόγο χρησιμεύουν για την ασφαλή πρόσβαση σε ιστοσελίδες δικτυακών τόπων που έχουν πιστοποιηθεί με βάση το ψηφιακό αυτό πιστοποιητικό για την ακρίβεια των στοιχείων του εξυπηρετητή που στεγάζει τις ιστοσελίδες (π.χ. οι ιστοσελίδες της υπηρεσίας webmail και άλλα).

4.7 Πλεονεκτήματα και μειονεκτήματα ασύμμετρης κρυπτογράφησης

Α) Πλεονεκτήματα ασύμμετρης κρυπτογράφησης

1) Μόνο το ιδιωτικό κλειδί πρέπει να διατηρείται μυστικό

2) Η διοίκηση των κλειδιών σε ένα δίκτυο απαιτεί την παρουσία μόνο ενός λειτουργικού έμπιστου ΤΤΡ ενώ αντιτίθεται σε ένα άνευ όρων έμπιστο ΤΤΡ.

3) Ανάλογα με τον τρόπο χρήσης, ένα ζευγάρι ιδιωτικού / δημόσιου κλειδιού μπορεί να μην αλλάξει για δεδομένες χρονικές περιόδους, για παράδειγμα πολλές εποχές (ακόμα και μερικά χρόνια).

4) Πολλά σχήματα δημόσιων κλειδιών αποφέρουν σχετικούς μηχανισμούς ψηφιακών υπογραφών. Το κλειδί που χρησιμοποιείται για να περιγράψει τη λειτουργία δημόσιας επιβεβαίωσης είναι συνήθως πολύ μικρότερο από αυτό που μετρά το συμμετρικό κλειδί.

5) Σε ένα μεγάλο δίκτυο, ο αριθμός των απαραίτητων κλειδιών μπορεί να είναι θεωρητικά μικρότερο από ότι σε ένα σενάριο συμμετρικού κλειδιού.

Β) Μειονεκτήματα ασύμμετρης κρυπτογράφησης

1) Το μέγεθος των κλειδιών είναι μεγαλύτερο από αυτό που απαιτείται στην κρυπτογραφία συμμετρικού κλειδιού.

2) Κανένα σχήμα δημόσιου κλειδιού δεν αποδείχθηκε ασφαλές. Τα αποτελεσματικότερα συστήματα δημόσιας κρυπτογράφησης φαίνεται ότι βασίζουν την ασφάλειά τους στη δυσκολία μικρών θεωρητικών - αριθμητικών προβλημάτων.

3) Η κρυπτογραφία δημόσιου κλειδιού δεν έχει τόσο μεγάλη ιστορία όπως η συμμετρική κρυπτογραφία αφού ανακαλύφθηκε μόλις στα μέσα της δεκαετίας του 1970.

ΚΕΦΑΛΑΙΟ 5

ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Στο κεφάλαιο αυτό παρουσιάζονται οι βασικοί τομείς στους οποίους βρίσκει εφαρμογή η κρυπτογράφηση στην καθημερινή μας ζωή και αναλύονται ενδεικτικά κάποιες από αυτές.
Για το κεφάλαιο αυτό χρησιμοποιήθηκαν στοιχεία από τις πηγές [10], [11], [13], [14], [16], [17].

5.1 Εφαρμογές της κρυπτογραφίας

Η εξέλιξη της χρήσης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη την μεταφορά της πληροφορίας. Έτσι, η επιστήμη της κρυπτογραφίας βρίσκει εφαρμογή σε πάρα πολλούς τομείς του ψηφιακού και δικτυακού κόσμου. Αρκετούς από αυτούς βλέπουμε στην παρακάτω Εικόνα 16:

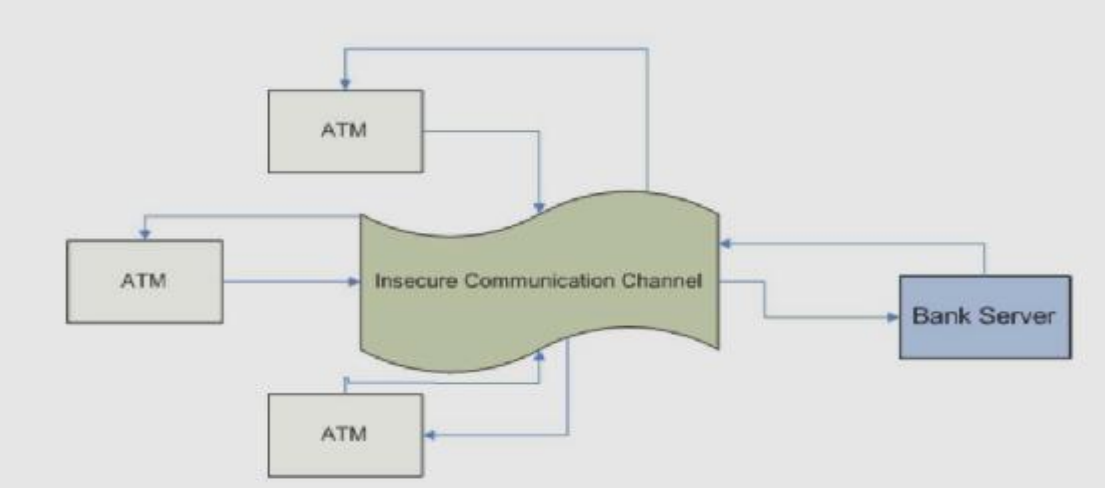
Ασφάλεια συναλλαγών σε τράπεζες δίκτυα - ATM	Συστήματα συναγερμών
Κινητή τηλεφωνία - μυστικότητα	Συστήματα βιομετρικής αναγνώρισης
Σταθερή τηλεφωνία (cryptophones)	Έξυπνες κάρτες
Διασφάλιση Εταιρικών πληροφοριών	Ιδιωτικά δίκτυα (VPN)
Στρατιωτικά δίκτυα	Word Wide Web
Διπλωματικά δίκτυα (Τηλεγραφήματα)	Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)	Ασύρματα δίκτυα (Hipperlan, Bluetooth, 802.11x)
Ηλεκτρονική ψηφοφορία	Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
Ηλεκτρονική δημοπρασία	Τηλεσυνδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP)
Ηλεκτρονικό γραμματοκιβώτιο	Συστήματα συναγερμών

Εικόνα 16: Τομείς εφαρμογής της κρυπτογραφίας

5.2 Η κρυπτογραφία στις τραπεζικές συναλλαγές μέσω ATM

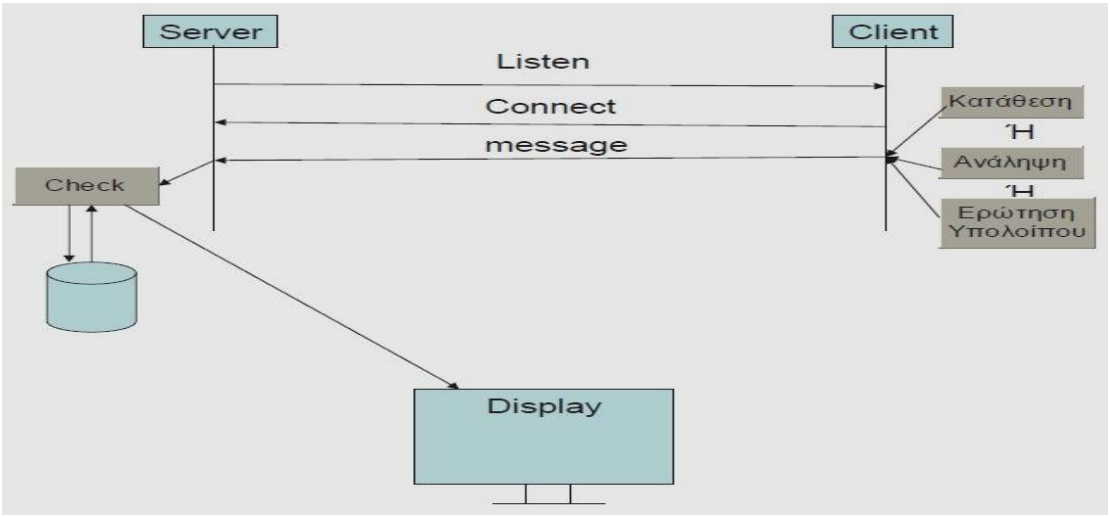
Η σύγχρονη έρευνα πάνω στο θέμα της κρυπτογράφησης και της ασφάλειας των τηλεπικοινωνιακών δικτύων από ανεπιθύμητους έχει εφεύρει ήδη κάποιους αλγόριθμους κρυπτογράφησης ικανούς να αποθαρρύνουν τους επίδοξους υποκλοπείς που είναι εύκολα υλοποιήσιμοι σε υλικό (firmware). Η έρευνα πάνω στο τομέα αυτό πρέπει να λάβει υπ’ όψη τις ταχύτητες μεταφοράς του ATM και άρα να προσανατολιστεί προς αλγόριθμους με ικανοποιητικά αποτελέσματα αλλά και μικρό βαθμό πολυπλοκότητας, έτσι ώστε να μην υπάρχει μεγάλη επιβάρυνση (overhead) στα τελικά σημεία της σύνδεσης.
Στα σημερινά δημόσια δίκτυα τηλεφωνίας η παρακολούθηση μιας σύνδεσης είναι σχετικά απλή υπόθεση, μιας και η διαδρομή ενός κυκλώματος είναι σε γενικές γραμμές προβλέψιμη

και παραμένει σταθερή καθ' όλη τη διάρκεια της συνομιλίας. Κατ' αντιστοιχία, στα περισσότερα δίκτυα υπολογιστών μικρής και μεσαίας απόστασης (π.χ. Ethernet και FDDI) τα δεδομένα ταξιδεύουν πάνω στο κοινό μέσο (καλώδιο ή οπτική ίνα) και είναι απροστάτευτα από εκείνους που θέλουν να υποκλέψουν τα δεδομένα. Σ' αυτές τις περιπτώσεις, ο μόνος αναγκαίος εξοπλισμός είναι ένας προσαρμογέας δικτύου σε «αδιάκριτη» κατάσταση (promiscuous mode) και κάποιο εργαλείο ανάλυσης δικτύου που μπορεί και περνάει από φίλτρο όλα τα πακέτα που περνάνε από το μέσο για να κρατήσει αυτά που έχουν «ενδιαφέρον»: κωδικοί εισόδου (passwords), αριθμοί πιστωτικών καρτών κ.ο.κ. Όλα αυτά μπορεί να απασχολήσουν πολύ σοβαρά κάποιον οργανισμό που στοχεύει να στηρίξει την οργανωτική του υποδομή πάνω σε ένα δίκτυο δεδομένων και να διακινεί σημαντικά και απόρρητα δεδομένα πάνω σε αυτό.
Το ATM μπορεί και παρέχει ασφάλεια στις συνδέσεις ακριβώς επειδή το «κύκλωμα» που εγκαθίσταται με μία σύνδεση είναι εικονικό (virtual circuit) και αποσυντίθεται αμέσως μετά το τέλος της σύνδεσης. Αυτό συνδυαζόμενο με το γεγονός της μη προκαθορισμένης διαδρομής των πακέτων καθιστά σχεδόν αδύνατη την πλήρη παρακολούθηση μίας σύνδεσης ATM.
Παρακάτω εξετάζεται η τρέχουσα τεχνολογία συναλλαγής μεταξύ ενός κεντρικού υπολογιστή (Server) μιας τράπεζας και ενός ATM (Client) (Εικόνα 17) όσων αφορά θέματα ασφάλειας. Η ασφάλεια αφορά την πιστοποίηση της ταυτότητας του συναλλασσόμενου, την ασφαλή μεταφορά δεδομένων καθώς και την ασφαλή καταχώρηση στοιχείων τα οποία θα ήταν δυνατό να χρησιμοποιηθούν σε μελλοντικές διενέξεις.



Εικόνα 17: Σύνδεση Bank server με τα ATM

Οι αυτόματες ταμειακές μηχανές (ATM) αποτελούν στοιχεία ενός κατανεμημένου συστήματος που σκοπός του είναι να παρέχει ένα σύνολο τραπεζικών υπηρεσιών στους πελάτες μίας τράπεζας, για παράδειγμα ερωτήσεις υπόλοιπου λογαριασμού, καταθέσεις, αναλήψεις μετρητών κλπ.
Ο κεντρικός υπολογιστής της τράπεζας (Bank Server) ανήκει σε ένα κατανεμημένο σύστημα στο οποίο πολλαπλά ATM μπορούν να συνδεθούν μαζί του με σκοπό την εκτέλεση εντολών που επιθυμεί ο εκάστοτε πελάτης. Στο παρακάτω διάγραμμα (Εικόνα 18) βλέπουμε την διαδικασία συναλλαγής:

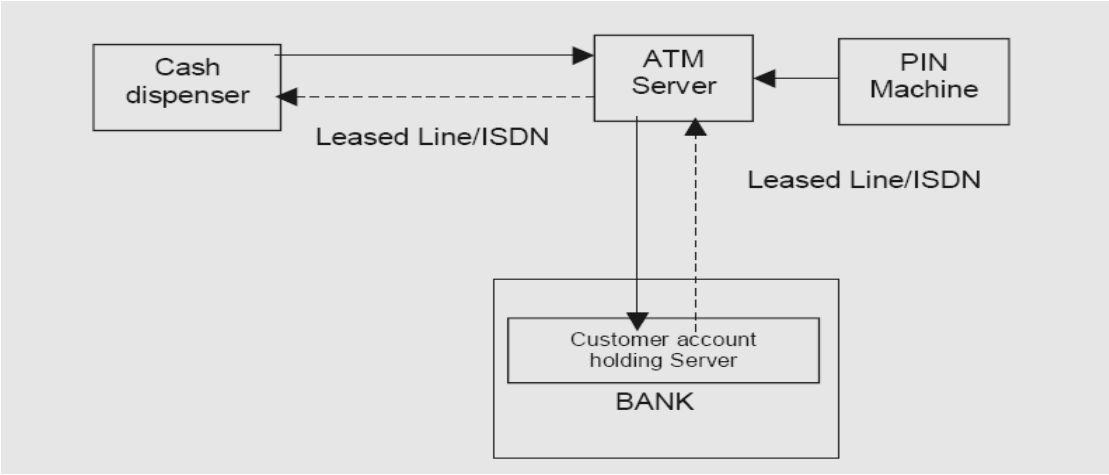


Εικόνα 18: Διαδικασία συναλλαγής

Αναλυτικότερα η διαδικασία έχει ως εξής:

Ο Server «ακούει» για τυχόν αίτημα σύνδεσης (διεργασία Listen).
Ο Client κάνει αίτημα σύνδεσης στον Server. Μόλις γίνει η σύνδεση ο Server στέλνει το Public Key του στον Client (στο σχήμα διεργασία «Connect»).
Το μήνυμα αυτό περιλαμβάνει το PIN, το Account Number, το ποσό και το είδος της συναλλαγής. Όλα αυτά γίνονται ένα αλφαριθμητικό (message) και κωδικοποιούνται με το Public Key του Server. Ο Server μόλις το λάβει το αποκωδικοποιεί με το Private Key του και στη συνέχεια ξεχωρίζονται τα στοιχεία αυτά. Το μήνυμα (message) αυτό στη συνέχεια υπογράφεται ψηφιακά από τον αποστολέα με σκοπό να ελεγχθεί η ακεραιότητα του μηνύματος από τον παραλήπτη (στο σχήμα διεργασία «message»).
Αφού ο Server ξεχωρίσει τα στοιχεία του πελάτη, ελέγχει στην βάση δεδομένων για τον πελάτη σύμφωνα με το PIN και το Account Number και την ενημερώνει ανάλογα με το είδος της συναλλαγής που επιθυμεί ο πελάτης. Τα αποτελέσματα που παίρνει μας τα εμφανίζει στην οθόνη (στο σχήμα διεργασία «Check»).
Οι αυτόματες μηχανές ανάληψης (ATM) εμφανίζονται παντού και μας επιτρέπουν να κάνουμε ανάληψη από την τράπεζα 24 ώρες το 24ωρο , 7 μέρες την εβδομάδα ,365 μέρες το χρόνο με την χρήση της κάρτας ανάληψης. Η κάρτα ανάληψης αποτελείται από δυο συστατικά, τον αριθμό της κάρτας και τον προσωπικό αριθμό αναγνώρισης (PIN). Κάθε τράπεζα εκδίδει έναν αριθμό κάρτας ο οποίος είναι μοναδικός για κάθε πελάτη. Εάν είναι μια χρεωστική κάρτα ο αριθμός αυτός θα είναι επίσης μοναδικός παγκοσμίως. Το PIN είναι ένας κωδικός που ελέγχει την αυθεντικότητα του πελάτη. Τα ATM ελέγχουν και τον αριθμό της κάρτας και το PIN. Στο σημείο αυτό θα εξετάσουμε τον σχεδιασμό ασφάλειας πίσω από το PIN καθώς θα παρουσιάσουμε ακόμα και το πώς αποθηκεύονται και διαχειρίζονται τα στοιχεία αυτά με ασφάλεια.

Τα συστήματα ATM έχουν 3 κύρια συστατικά: τον Cash dispenser, τον ATM Server και το PIN machine (Εικόνα 19).



Εικόνα 19: Τα κύρια συστατικά ενός συστήματος ATM.

Ο Cash dispenser διαβάζει τον αριθμό της κάρτας και το PIN το οποίο εισάγεται από τον πελάτη με αποτέλεσμα στη συνέχεια αυτά τα δυο να στέλνονται κεντρικό ATM Server. Ο ATM Server έχει μια βάση δεδομένων η οποία αποθηκεύει τον αριθμό της κάρτας ATM καθώς και λεπτομέρειες του PIN. Το τρίτο συστατικό το PIN machine χρησιμοποιείται για να επικυρώσει τον αριθμό ATM PIN του πελάτη. Συνδέεται άμεσα με τον ATM Server και είναι μια συσκευή απόδειξης πλαστογραφήσεων που αποθηκεύει ένα μοναδικό μυστικό κλειδί. Ο πελάτης αφού πρώτα εισάγει την κάρτα του στο ATM και πληκτρολογεί το PIN του ο Cash dispenser θα διαβάσει τον αριθμό της κάρτας από την μαγνητική ταινία καθώς και το PIN που έχει πληκτρολογηθεί και θα τα στείλει στον ATM Server. Ο ATM Server ελέγχει το PIN σε σχέση με τον αριθμό της κάρτας με την βοήθεια του PIN machine και στέλνει μια θετική ή αρνητική επιβεβαίωση στον Cash dispenser. Σε αυτό το σημείο ο πελάτης έχει επικυρωθεί και μπορεί να χρησιμοποιήσει τον λογαριασμό του.

Η ασφάλεια του ATM PIN είναι ένα κρίσιμο σημείο στην όλη διαδικασία. Είναι η πιο μυστική πληροφορία του πελάτη. Για αυτό το λόγο η ασφάλεια ATM PIN είναι πολύ αυστηρή σε όλα τα δίκτυα ATM. Υπάρχουν δυο τρόποι όπου ένας επιτιθέμενος θα προσπαθούσε να πάρει τον αριθμό ATM PIN. Θα μπορούσε να εισχωρήσει στο δίκτυο όταν ένας Cash dispenser μεταδίδει το PIN στον ATM Server ή θα μπορούσε να αναγκάσει έναν ATM Server και ένα Pin machine να «παραχωρήσουν» το PIN του χρήστη. Ευτυχώς αυτές οι απειλές έχουν εξαλειφθεί στα σημερινά συστήματα ATM
και θα πρέπει να δούμε το πώς.
Για να αποτρέψουμε την εισχώρηση και την κλοπή του PIN κατά τη διαδικασία της μετάδοσης, το PIN κρυπτογραφείται με την χρήση του DES και του Triple DES κρυπτογραφικού αλγορίθμου και στη συνέχεια αυτό μεταδίδεται από τον Cash dispenser στον ATM Server. Το κοινό μυστικό κλειδί αποθηκεύεται στον Cash dispenser καθώς και στον ATM Server. Αυτή η εφαρμογή αποθηκεύει το διαμοιραζόμενο κλειδί DES σε μια κρυπτογραφημένη μορφή χρησιμοποιώντας τον ιδιόκτητο αλγόριθμο του προμηθευτή (π.χ. ACI ATM software) και κατά συνέπεια έχει αποτραπεί η κλοπή του κλειδιού από την μηχανή.
Η επίλυση του δεύτερου προβλήματος είναι ενδιαφέρουσα. Το σύστημα διαχωρίζει το PIN του πελάτη σε δυο μέρη και τα αποθηκεύει σε δυο διαφορετικά σημεία. Έτσι ακόμα και όταν ένα μηχάνημα μείνει έκθετο το PIN συνεχίζει να παραμένει ασφαλές. Τώρα το πρόβλημα είναι το πώς θα διαχωρίσουμε το PIN με ασφάλεια σε δυο μέρη. Επίσης πρέπει να έχουμε στο

νου μας ότι ο πελάτης μπορεί πάντα οποιαδήποτε στιγμή να αλλάξει το PIN του. Για αυτό το λόγο έχει σχεδιαστεί ένας αλγόριθμος ο οποίος επιτρέπει στο PIN του πελάτη να διαχωριστεί καθώς επίσης δίνεται η δυνατότητα στον πελάτη να αλλάξει το PIN του.

Ο μηχανισμός επικύρωσης του ATM PIN είναι πολύ απλός. Όταν ο πελάτης εισάγει την κάρτα του και πληκτρολογήσει το PIN, ο αριθμός της κάρτας και το PIN στέλνονται στον ATM Server κωδικοποιημένα. Ο ATM Server αποκωδικοποιεί τον αριθμό της κάρτας και το PIN. Πρώτα επικυρώνει τον αριθμό της κάρτας σύμφωνα με τη βάση δεδομένων. Ο έγκυρος αριθμός κάρτας, το PIN Offset β της κάρτας και το PIN που πληκτρολογήθηκε από τον πελάτη στέλνονται στο PIN machine. Τώρα το PIN machine δημιουργεί το Natural PIN γ από τον αριθμό της κάρτας, τοποθετείται με το PIN Offset β και δημιουργείται το πραγματικό PIN α του πελάτη. Στη συνέχεια συγκρίνει το ακριβές PIN α του πελάτη με το PIN που προμηθεύεται ο πελάτης. Αν αυτά τα δυο ταιριάζουν τότε στέλνεται θετική επιβεβαίωση στον ATM Server με αποτέλεσμα την επικύρωση του πελάτη. Σημειώστε ότι σε αυτή την διαδικασία, το Natural PIN δεν αφήνει ποτέ το tamper proof του PIN machine, και το PIN machine δεν είναι αναγκαίο να αποθηκεύσει ατομικά PIN όλων των πελατών. Αποθηκεύει με ασφάλεια το κλειδί DES για δημιουργία του Natural PIN από τον αριθμό κάρτας του κάθε πελάτη.

Παραγωγή και διανομή του ATM PIN

Το σύστημα ATM διαπραγματεύεται με κρίσιμες πληροφορίες του πελάτη είναι πιο ασφαλές εξ' αρχής, αλλά υπάρχουν ακόμα ρίσκα ασφαλείας κατά την διαδικασία παραγωγής και διανομής μιας νέας κάρτας και ενός PIN. Ο αριθμός κάρτας παράγεται από τον ATM Server και το PIN παράγεται από το PIN machine και από τον αριθμό της κάρτας, αλλά για πρώτη φορά το PIN Offset του καινούριου PIN παράγεται τυχαία από το PIN machine. Υπάρχουν δύο τρόποι να εμφανίσεις το PIN mailer. Στην πρώτη μέθοδο, ο διαχειριστής θα παράγει ένα νέο PIN χρησιμοποιώντας το PIN machine, παίρνουμε το PIN και παράγουμε την τυπωμένη αναφορά του PIN mailer. Στην δεύτερη μέθοδο ο διαχειριστής ζητάει από το PIN machine να παράγει το PIN και κατευθείαν να το τυπώσει σε έναν συνδεδεμένο εκτυπωτή και να σφραγίσει τον print mailer πριν περάσει στον διαχειριστή. Η δεύτερη μέθοδος είναι ξεκάθαρα πιο ασφαλής από την πρώτη καθώς ο διαχειριστής ποτέ δεν είναι σε θέση να γνωρίζει το μυστικό PIN.

5.3 Έξυπνες κάρτες (Smart Cards)

Η ιστορική προέλευση των έξυπνων καρτών μας οδηγεί στη δεκαετία του 70. Ύστερα από αρκετές διεργασίες η πρώτη έξυπνη κάρτα κατασκευάστηκε τελικά το 1977 από την Motorola και την Bull ενώ συγχρόνως 3 εμπορικοί κατασκευαστές, η Bull, η SGS Thomson και η Schlumberger ξεκίνησαν να αναπτύσσουν εφαρμογές πάνω στη νέα τεχνολογία. Η πρώτη αυτή κάρτα περιείχε δύο μικροτσίπ, δηλαδή ένα μικροελεγκτή και μία ξεχωριστή συσκευή μνήμης. Το 1980 η Motorola παρουσίασε την πρώτη ασφαλή έξυπνη κάρτα με ένα μικροτσίπ, για χρήση στο Γαλλικό τραπεζικό χώρο. Το 1982 έγινε στη Γαλλία το πρώτο εκτεταμένο και πραγματικό τεστ έξυπνων καρτών και συγκεκριμένα τηλεφωνικών καρτών σειριακής μνήμης. Ακολούθως το 1984 έγιναν τα πρώτα τεστ στην παραγωγή των έξυπνων καρτών αυτόματης ανάληψης.

Με την πάροδο των χρόνων, οι έξυπνες κάρτες εξελίσσονταν συνεχώς, και καινούριες εφαρμογές αναπτύσσονταν, κυρίως στην Ευρώπη. Η Γαλλία έχει πρωτοπορήσει όλα αυτά τα

χρόνια στο σχεδιασμό και τη χρήση εφαρμογών έξυπνων καρτών και μαζί με τη Γερμανία αποτελούν τις κορυφαίες χώρες σε εισαγωγή ποικίλων εφαρμογών σε έξυπνες κάρτες. Το 1987 εφαρμόστηκε το πρώτο μεγάλης κλίμακας έργο με έξυπνες κάρτες στην Αμερική ενώ το 1993 οι πρώτες εφαρμογές με κάρτες πολλαπλών διεργασιών δοκιμάστηκαν στην Γαλλία. Το ίδιο έτος ολοκληρώθηκε σχεδόν στη Γαλλία η αντικατάσταση των υπάρχουσων τραπεζικών καρτών με έξυπνες κάρτες και η τάση αυτή εξαπλώθηκε σε άλλες Ευρωπαϊκές και Ασιατικές χώρες.

Έκτοτε η βιομηχανία των έξυπνων καρτών εξαπλώνεται με πολύ μεγάλο ρυθμό και έχει φτάσει σε βαθμό παραγωγής και αποστολής καρτών σχεδόν ίσο με 1.000.000.000 το χρόνο ενώ πλέον οι έξυπνες κάρτες χρησιμοποιούνται σε διάφορες εφαρμογές σε περισσότερες από 90 χώρες παγκοσμίως. Το μεγαλύτερο μερίδιο της αγοράς των έξυπνων καρτών κατέχουν οι εφαρμογές τηλεφωνίας, οι τραπεζικές εφαρμογές, έργα που αφορούν το τομέα της Υγείας καθώς και άλλα ποικίλα σχέδια που θα αναπτύξουμε παρακάτω.
Τα συστήματα που χρησιμοποιούν έξυπνες κάρτες, βασίζονται στην κατοχή, από την πλευρά του χρήστη, ενός αντικειμένου. Ένα τέτοιο σύστημα, για παράδειγμα, χρησιμοποιεί ένα μηχανισμό password, ζητώντας από το χρήστη να πληκτρολογήσει μια λέξη, την οποία ο χρήστης θα δει στο Smart Card του. Δηλαδή, ο host θα δώσει στο χρήστη κάποιου είδους πληροφορία, την οποία ο χρήστης θα πληκτρολογήσει στο πληκτρολόγιο του Smart Card του, και το Smart Card θα δώσει μια απάντηση στο χρήστη, η οποία θα πρέπει να πληκτρολογηθεί στο πληκτρολόγιο του host, προτού επιτευχθεί η πλήρης σύνδεση. Υπάρχουν και άλλα συστήματα αυθεντικοποίησης όπως ανιχνευτές δακτυλικών αποτυπωμάτων, που όμως είναι πολυδάπανες.

Η έξυπνη κάρτα στην πραγματικότητα ορίζεται ως μία πλαστική κάρτα, συνήθως σε μέγεθος και σχήμα πιστωτικής κάρτας, η οποία όμως περιέχει μνήμη ή / και μικροεπεξεργαστή που της δίνουν τη δυνατότητα αποθήκευσης και επεξεργασίας μεγάλου όγκου δεδομένων και η οποία συμμορφώνεται με διεθνή πρότυπα. Με απλούς όρους, η έξυπνη κάρτα είναι ένας μικροσκοπικός υπολογιστής με πολύ σημαντικές δυνατότητες και αποτελεί την πιο πρόσφατη εξέλιξη στο χώρο των πλαστικών καρτών, έχοντας ήδη ανοίξει το δρόμο σε σημαντικές και εκτεταμένες εφαρμογές παγκοσμίως. Ο μικροσκοπικός αυτός υπολογιστής, αλλιώς καλούμενος μικροτσίπ, είναι ένα ολοκληρωμένο κύκλωμα με ηλεκτρικές επαφές ή με δυνατότητες ασύρματης επικοινωνίας που συνδυαζόμενος με την κατάλληλη συσκευή υποδοχής καρτών έχει τη δυνατότητα αποθήκευσης και μεταφοράς χιλιάδων bit πληροφορίας καθώς και μεγάλη δύναμη επεξεργασίας αυτών των δεδομένων για την εξυπηρέτηση ποικίλων εφαρμογών. Κύρια χαρακτηριστικά των έξυπνων καρτών είναι ότι παρέχουν ασφάλεια δεδομένων και συνδιαλλαγών, ταχύτητα και ευκολία χρήσης καθώς επίσης αντοχή στην καταπόνηση και κακή χρήση και μεγάλο διάστημα “ζωής”. Σε αντίθεση με τις γνωστές κάρτες με μαγνητική ταινία, οι έξυπνες κάρτες κατέχουν βασικές και απαραίτητες διεργασίες και πληροφορίες αποθηκευμένες στο σώμα τους προσφέροντας έτσι περισσότερη ασφάλεια καθώς και τη δυνατότητα μεταφοράς σημαντικών δεδομένων χωρίς την ανάγκη σύνδεσης με κεντρικές βάσεις δεδομένων για την άντληση ουσιωδών πληροφοριών. Για αυτό το λόγο η τάση στις σύγχρονες αγορές κυρίως της Ευρώπης, είναι η αντικατάσταση των καρτών μαγνητικής ταινίας από τις έξυπνες κάρτες (Εικόνα 20) και η ανάπτυξη όλο και πιο πολύπλοκων εφαρμογών, όλο και πιο αυτοματοποιημένων διαδικασιών.

Υπάρχουν διάφορες κατηγορίες στις οποίες χωρίζονται οι έξυπνες κάρτες, ανάλογα με τον τύπο της διεπαφής τους (interface) με τον έξω κόσμο ή ανάλογα με το τύπο του μικροτσίπ. Ονομαστικά υπάρχουν οι εξής: Contact Cards, Contactless Cards, Combi – Hybrid Cards,

Memory Cards (*Straight Memory Cards, Protected / Segmented Memory Cards, Stored Value Memory Cards*), Microprocessor Cards.

Εικόνα 20: Έξυπνη κάρτα και Κάρτα μαγνητικής ταινίας

Οι δύο παραπάνω μορφές πλαστικών καρτών παρουσιάζουν σημαντικές διαφορές σε τομείς όπως:

• Αποθήκευση Δεδομένων:
σε σχέση με τη περιορισμένη δυνατότητα αποθήκευσης πληροφοριών των καρτών μαγνητικής ταινίας (ως 140 byte πληροφορίας), οι έξυπνες κάρτες έχουν μεγάλη χωρητικότητα, με δυνατότητα αποθήκευσης ως και 80 φορές περισσότερων ηλεκτρονικών δεδομένων (από 1Kbyte ως 32Kbytes πληροφορίας).

• Ασφάλεια:
ενώ στις κάρτες μαγνητικής ταινίας οι εκάστοτε πληροφορίες μπορούν εύκολα να αλλοιωθούν ή να αναπαραχθούν από μη έγκυρους χρήστες, οι έξυπνες κάρτες παρέχουν αυξημένη ασφάλεια δεδομένων και συναλλαγών, με τη χρήση διαδικασιών όπως κρυπτογράφηση και κωδικοποίηση.

• Αντοχή / Διάρκεια:
σε αντίθεση με την ευαισθησία των καρτών μαγνητικής ταινίας που συνίσταται στη πιθανότητα απομαγνητισμού της ταινίας λόγω χρήσης ή λόγω εξωτερικών μαγνητικών πεδίων, οι έξυπνες κάρτες παρουσιάζουν μεγάλη ανθεκτικότητα και έχουν μεγάλη συγκριτικά διάρκεια ζωής και αντοχή σε αλλεπάλληλες εισαγωγές σε μηχανήματα υποδοχής καρτών 100.000 φορές και πάνω.

• Χρήση:
η σχεδίαση των καρτών μαγνητικής ταινίας γίνεται για μία εφαρμογή και η χρήση τους περιορίζεται σε απλά και επαναλαμβανόμενα καθήκοντα, ενώ οι έξυπνες κάρτες υποστηρίζουν πολλαπλές και πολύπλοκες εφαρμογές.

• Ευελιξία:
τα δεδομένα μίας κάρτας μαγνητικής ταινίας είναι μόνο αναγνώσιμα με αποτέλεσμα οποιαδήποτε σημαντική αλλαγή στοιχείων να καθιστά αναγκαία την έκδοση νέας κάρτας, ενώ σε μία έξυπνη κάρτα διαδικασίες ανάγνωσης, εγγραφής και ανανέωσης δεδομένων γίνονται εύκολα και γρήγορα.

• Σύνδεση:
η χρήση καρτών μαγνητικής ταινίας καθιστά αναγκαία την online σύνδεση με κεντρική βάση δεδομένων για κάθε συναλλαγή, γεγονός που συνεπάγεται συνήθως την ύπαρξη μισθωμένης γραμμής. Το κόστος που αντιστοιχεί στη μίσθωση γραμμής είναι ένα επιπλέον κόστος που δεν υπάρχει στην περίπτωση των έξυπνων καρτών, οι οποίες μπορούν να κάνουν offline ασφαλείς και έγκυρες συναλλαγές τα στοιχεία των οποίων θα περνάνε αν χρειάζεται σε κεντρικό σύστημα σε δεδομένη χρονική στιγμή, ανεξάρτητη της στιγμής συναλλαγής.

Το κόστος κατασκευής έξυπνων καρτών είναι μεγαλύτερο από το αντίστοιχο των καρτών μαγνητικής ταινίας, λόγω όμως της ανθεκτικότητάς τους, της χρησιμοποίησής τους σε ποικίλες εφαρμογές, τη μείωση των οικονομικών απατών και τη μείωση του κόστους τηλ/κής σύνδεσης, οι έξυπνες κάρτες είναι τελικά πιο αποδοτικές ως προς το κόστος. Αν και οι παράγοντες που ευνοούν τη χρήση των έξυπνων καρτών στη θέση των καρτών μαγνητικής ταινίας είναι σημαντικοί, δεν έχουν το ίδιο βάρος σε όλες τις σύγχρονες αγορές με αποτέλεσμα να μην έχουν την ίδια απήχηση παγκοσμίως. Έτσι χρησιμοποιούνται ήδη ευρέως στις αγορές της Ευρώπης, της Ασίας και της Αφρικής, έχοντας γίνει ένα προϊόν εμπορικά επιτυχημένο. Οι εφαρμογές που στηρίζονται σε έξυπνες κάρτες καλύπτουν τομείς όπως η πρόσβαση και η αναγνώριση ταυτότητας σε διάφορους χώρους, οι ηλεκτρονικές αγορές μέσω του Διαδικτύου και οι τουριστικές επιχειρήσεις, δίνοντας εξελιγμένες δυνατότητες. Υπάρχουν όμως αγορές στις οποίες οι έξυπνες κάρτες, παρότι παρουσιάστηκαν επιτυχώς και ελπιδοφόρα, δεν έχουν καταφέρει ακόμα να καθιερωθούν ως κοινό μέσο συναλλαγών και εφαρμογών.

Εφαρμογές Έξυπνων Καρτών

Οι έξυπνες κάρτες βοηθούν τις επιχειρήσεις να εξελιχθούν και να διευρύνουν τα προϊόντα και τις υπηρεσίες τους σε μία συνεχώς μεταβαλλόμενη παγκόσμια αγορά. Λόγω της επεξεργαστικής δυνατότητας που έχουν μέσω του ενσωματωμένου μικροτσίπ, χρησιμοποιούνται παγκοσμίως για ένα μεγάλο εύρος καθημερινών εργασιών αλλά και προηγμένων εφαρμογών, την πλειονότητα των οποίων θα αναπτύξουμε παρακάτω. Οι εκάστοτε εταιρίες, σχεδιάζοντας εφαρμογές και προγράμματα, μπορούν να δουν και να χρησιμοποιήσουν τις έξυπνες κάρτες ως:

• Μέσα Πληρωμής:
οι έξυπνες κάρτες εξασφαλίζουν ασφαλείς χρεωστικές και πιστωτικές συναλλαγές, με μηχανισμούς που να προστατεύουν από κακόβουλες επιθέσεις. Συγχρόνως, αποτελούν για τις εταιρίες μία νέα καθαρή πηγή εσόδων αφού τις απαλλάσσουν από το πάγιο κόστος συναλλαγής το οποίο συνόδευε κάθε συναλλαγή με τις γνωστές τραπεζικές κάρτες (credit / debit cards) όπως και από τις πιθανές απώλειες εσόδων λόγω χαμένων / κλεμμένων καρτών.

• Εργαλεία Πρόσβασης:
οι έξυπνες κάρτες υποστηρίζουν λειτουργίες κρυπτογράφησης, πιστοποίησης, εξουσιοδότησης, επεξεργασίας και αποθήκευσης πληροφοριών οι οποίες καθιστούν δυνατή την ασφαλή διεξαγωγή οικονομικών συναλλαγών και ανταλλαγή πληροφορίας σε on-line / off-line περιβάλλοντα. Έτσι γίνονται ιδανικές για τον έλεγχο πρόσβασης στο Διαδίκτυο και για εφαρμογές όπως το home banking.

• Διαχειριστές Πληροφοριών:
λόγω της επεξεργαστικής και αποθηκευτικής τους δύναμης όσο αφορά πληροφορίες, οι έξυπνες κάρτες μπορούν να χρησιμοποιηθούν ως ένα κινητό ηλεκτρονικό αρχείο που μπορεί να μεταφέρει δεδομένα όπως χρήσιμα τηλέφωνα, στοιχεία του λογαριασμού του κατόχου, πόντους προγραμμάτων εμπιστοσύνης λιανικής πώλησης ή ακόμα και τον ιατρικό φάκελο του χρήστη.

• Εργαλεία Προώθησης:
οι έξυπνες κάρτες μπορούν να λειτουργήσουν ως προϊόντα προώθησης μίας εταιρίας αφού υπηρεσίες όπως εκπτωτικές προσφορές, προγράμματα εμπιστοσύνης, ηλεκτρονικά κουπόνια

και δωροεπιταγές μπορούν κάλλιστα να αποθηκεύουν και να επεξεργάζονται με ασφάλεια τα εκάστοτε στοιχεία τους στις έξυπνες κάρτες.

• Συστήματα Προσωποποιημένων Υπηρεσιών:
με τις δυνατότητες αποθήκευσης, επεξεργασίας και κωδικοποίησης δεδομένων που υποστηρίζουν οι έξυπνες κάρτες, μπορούν να κρατούν σημαντικά στοιχεία για το κάτοχό τους και να χρησιμεύουν για την παροχή προσωποποιημένων υπηρεσιών από διάφορες εταιρίες.

Με μία ή περισσότερες από τις μορφές που αναφέρθηκαν παραπάνω, οι έξυπνες κάρτες έχουν χρησιμοποιηθεί σε ποικίλες εφαρμογές τις οποίες θα παραθέσουμε ακολούθως πιο διεξοδικά.

Τηλεφωνικές Κάρτες

Οι τηλεφωνικές κάρτες προπληρωμένης αξίας αποτελούν μία από τις πρώτες εφαρμογές έξυπνων καρτών. Διαδεδομένη χρήση τους ξεκίνησε το 1986 από τη Γαλλία και έκτοτε επεκτάθηκε ραγδαία και σε άλλες χώρες. Σε περισσότερες από 100 χώρες παγκοσμίως οι τηλεφωνικοί κερματοδέκτες σε δημόσιους και κοινόχρηστους χώρους, έχουν αντικατασταθεί από καρτοτηλέφωνα και τα κέρματα, ως μέσο πληρωμής των τηλεφωνικών υπηρεσιών, από τις τηλεφωνικές έξυπνες κάρτες. Αγοράζονται από τους καταναλωτές έναντι συγκεκριμένου αντιτίμου (3€, 6€ και 18€ για την Ελληνική αγορά) και περιέχουν συγκεκριμένο αριθμό μονάδων (ανάλογα με το ποσό αγοράς τους), οι οποίες μειώνονται με κάθε κλήση. Οι τηλεκάρτες είναι έξυπνες κάρτες που ανήκουν στην κατηγορία των καρτών μνήμης (memory cards). Μεγάλης κλίμακας προγράμματα εφαρμόζονται σε χώρες όπως η Γερμανία, η Γαλλία, η Αγγλία, η Βραζιλία, το Μεξικό και η Κίνα, ενώ στην Ελλάδα το δίκτυο καρτοτηλεφωνίας περιλαμβάνει 70.000 καρτοτηλέφωνα σε όλη τη χώρα.

Κινητή Τηλεφωνία (GSM)

Οι έξυπνες κάρτες χρησιμοποιούνται ευρέως ως κάρτες SIM (Security Identity Module) στην κινητή τηλεφωνία GSM (Global System for Mobile communications). Η κάρτα SIM περιέχει πληροφορίες ασφαλείας και συνδρομητικά στοιχεία. Μπορεί είτε να εισάγεται στη συσκευή είτε να βρίσκεται ενσωματωμένη σε αυτή και με την ενεργοποίησή της το τηλέφωνο προσωποποιείται ως προς το χρήστη και φορτώνει στοιχεία όπως το νούμερό του στο δίκτυο, πληροφορίες κοστολόγησης και πρόσφατα κληθέντες αριθμούς. Η κάρτα μπορεί να μεταφέρεται από συσκευή σε συσκευή αφού περιέχει τα στοιχεία του συνδρομητή τα οποία προστατεύονται από ειδικό κωδικό (PIN). Οι παροχείς κινητής τηλεφωνίας κερδίζουν από τη μείωση των περιπτώσεων απάτης και μη έγκυρης χρήσης λόγω της αυξημένης ασφάλειας που προσφέρουν οι έξυπνες κάρτες. Με την έλευση προηγμένων υπηρεσιών κινητής τηλεφωνίας όπως η πρόσβαση στο Διαδίκτυο (web browsing), το ηλεκτρονικό ταχυδρομείο και άλλες υπηρεσίες πληροφοριών, οι παροχείς βασίζονται στις έξυπνες κάρτες να δράσουν ως μηχανισμοί ασφαλείας για τις υπηρεσίες αυτές. Στη παγκόσμια αγορά, το 1994 πωλήθηκαν περισσότερες από 9.000.000 έξυπνες κάρτες κινητής τηλεφωνίας ενώ πλέον τα κινητά τηλέφωνα που χρησιμοποιούν τις έξυπνες κάρτες ως κάρτες SIM ξεπερνούν τα 300.000.000.

Συνδρομητική Τηλεόραση

Σχεδόν κάθε μικρό πιάτο δορυφορικής τηλεόρασης στις Ηνωμένες Πολιτείες χρησιμοποιεί μία έξυπνη κάρτα ως αφαιρέσιμο στοιχείο ασφαλείας και πληροφοριών για το συνδρομητή. Οι έξυπνες κάρτες λειτουργούν ως μία προπληρωμένη εφαρμογή, όπως και οι τηλεκάρτες που αναφέρθηκαν παραπάνω, και περιέχουν πληροφορίες εξουσιοδότησης και κοστολόγησης που αντιστοιχούν στον συνδρομητή-κάτοχο. Κυρίως περιέχουν ειδικά "κλειδιά" (keys) τα οποία χρειάζονται για να μπορεί ο συνδρομητής να δει την κωδικοποιημένη μετάδοση. Η κάρτα συνδρομητικής τηλεόρασης μπορεί να χρησιμοποιηθεί σε οποιοδήποτε χώρο έχει την κατάλληλη υποδομή και δε συνδέεται αποκλειστικά με τη συσκευή αλλά με το συνδρομητή. Έτσι ένας συνδρομητής μπορεί με την κάρτα του να παρακολουθήσει το πρόγραμμα της συνδρομητικής τηλεόρασης στο σπίτι του αλλά και σε ένα ξενοδοχείο. Ένα μεγάλο προτέρημα της χρήσης έξυπνων καρτών σε αυτή την εφαρμογή είναι τα στοιχεία προσωποποίησης που περιέχουν και προσδιορίζουν-φιλτράρουν το μέρος της μετάδοσης που θα λαμβάνει ο συνδρομητής. Έτσι οι γονείς μπορούν να παρέχουν στα παιδιά κάρτες συνδρομητικής τηλεόρασης που αποκλείουν την πρόσβαση των παιδιών σε προγράμματα ακατάλληλα. Στην Αμερική, πάνω από 4.000.000 κάρτες συνδρομητικής τηλεόρασης χρησιμοποιούνται και εκατομμύρια ακόμα διατίθενται στην Ευρώπη και την Ασία.

Συγκοινωνίες

Οι έξυπνες κάρτες χρησιμοποιούνται σε μεγάλο βαθμό ως "εισιτήρια", στα μέσα μαζικής μεταφοράς, στα πάρκινγκ και τα διόδια. Συνήθως χρησιμοποιούνται contactless (χωρίς επαφή) κάρτες, που διευκολύνουν και επιταχύνουν τη διαδικασία. Πωλούνται ως κάρτες προπληρωμένης αξίας, όπως και οι τηλεφωνικές. Σχεδιάζονται για χρήση σε μέσα μαζικής μεταφοράς όπως λεωφορεία και τρένα, όπως επίσης και στα διόδια, κάνοντας τη διαδικασία έκδοσης εισιτηρίων πολύ πιο γρήγορη και εύκολη. Η αξία του εισιτηρίου, ανάλογα με το πεδίο εφαρμογής, αφαιρείται από το ποσό που είναι αποθηκευμένο στη κάρτα κάθε φορά που ο κάτοχος περνάει από την ειδική συσκευή ανάγνωσης / γραφής και μπορεί να επαναφορτώνεται στο κατάλληλο σημείο πώλησης. Αυτός ο τρόπος παρέχει ευκολία στους καταναλωτές και με τη χρήση ειδικών "επιβραβευτικών" προγραμμάτων στις συγκοινωνίες, αυξάνει τη χρήση των μέσων μαζικής μεταφοράς, προσελκύοντας περισσότερους καταναλωτές. Ειδικά στην περίπτωση των διοδίων, η χρήση των έξυπνων καρτών συμβάλει πολύ στην εξυπηρέτηση του κοινού αφού επιτρέπει την συλλογή διοδίων χωρίς τη παρεμπόδιση της κυκλοφορίας. Στις περιοχές συλλογής των διοδίων υπάρχουν ειδικές συσκευές ανάγνωσης και πάνω στα διερχόμενα οχήματα υπάρχουν ειδικές συσκευές για τις έξυπνες κάρτες ούτως ώστε με τη διέλευση του οχήματος από το σημείο συλλογής, η χρέωση να γίνεται αυτόματα χωρίς να χρειάζεται να δημιουργούνται ουρές.

Banking / E-purse

Ο οικονομικός και τραπεζικός χώρος ήταν από τους πρώτους που υιοθέτησαν την τεχνολογία των έξυπνων καρτών σε πολλές χώρες παγκοσμίως. Κάθε Γαλλική χρεωστική κάρτα VISA έχει πλέον μικροτσίπ. Χώρες όπως η Πορτογαλία και η Σιγκαπούρη έχουν εισάγει προγράμματα ηλεκτρονικού πορτοφολιού στα εθνικά τραπεζικά δίκτυά τους. Οι έξυπνες κάρτες χρησιμοποιούνται από τις τράπεζες είτε ως πιστωτικές είτε ως χρεωστικές, εις αντικατάσταση των υπάρχουσων καρτών μαγνητικής ταινίας. Οι πιστωτικές κάρτες δίνουν πληροφορίες για το πιστωτικό λογαριασμό του κατόχου ο οποίος θα χρεωθεί μετά από μία

αγορά και είναι ένας τρόπος να δοθεί μία “πίστωση χρόνου” στον κάτοχό της για την πληρωμή, ένας τρόπος άτοκου (μέχρι ενός ορισμένου χρονικού διαστήματος) δανεισμού. Οι χρεωστικές κάρτες δίνουν πληροφορίες για τον καταθετικό λογαριασμό του κατόχου της κάρτας και η οποιαδήποτε αγορά χρεώνεται κατευθείαν στο λογαριασμό, είναι δηλαδή μία άμεση πληρωμή χωρίς μετρητά. Η πιστοποίηση της ταυτότητας του κατόχου μίας κλασικής πιστωτικής κάρτας γίνεται με παρατήρηση της υπογραφής του και της ταυτότητας του, ενώ στην περίπτωση των συνηθισμένων χρεωστικών καρτών (debit cards) υπάρχει ένας κωδικός (PIN) που επαληθεύεται όμως μόνο on-line. Οι έξυπνες κάρτες έρχονται να αλλάξουν αυτό το τοπίο αφού ο κωδικός του κατόχου είναι αποθηκευμένος στην ίδια την κάρτα και προστατεύεται όπως και επαληθεύεται με ασφαλείς διαδικασίες που παρέχει η κάρτα. Έτσι οι κάρτες αυτές γίνονται πιο ασφαλείς και για τις καινούριες τραπεζικές υπηρεσίες που παρέχονται στους πελάτες, όπως το web-banking, αυξάνοντας την ποιότητα εξυπηρέτησης των πελατών. Συγχρόνως, μειώνεται το λειτουργικό κόστος των πιστωτικών ιδρυμάτων αφού εργασίες που θα απαιτούσαν καθημερινή ανθρώπινη εργασία γίνονται με ηλεκτρονικό τρόπο. Η τεχνολογία των έξυπνων καρτών ευνοεί και τους πωλητές λιανικής αφού με την ασφάλεια που παρέχει μειώνει το κόστος από απώλειες λόγω απατών ή λαθών. Στην αγορά των έξυπνων τραπεζικών καρτών παγκοσμίως το μεγαλύτερο μερίδιο κατέχει σταθερά η Ευρώπη, το μέγεθος όμως του μεριδίου ελαττώνεται με την πάροδο των ετών, καθώς η τεχνολογία αυτή εξαπλώνεται στις άλλες ηπείρους. Τέλος, το ηλεκτρονικό πορτοφόλι (e-purse/e-wallet) είναι ένας ακόμα τρόπος κατοχής ηλεκτρονικού χρήματος (κάτι αντίστοιχο με τις κάρτες προπληρωμένης αξίας όπως οι τηλεφωνικές κάρτες), με τη διαφορά ότι μπορεί να γίνει και πίστωση και χρέωση στην κάρτα, δίνοντας έτσι μεγαλύτερες δυνατότητες στο κάτοχο. Το ηλεκτρονικό πορτοφόλι προσφέρει στους κατόχους ευκολία χρήσης και ασφάλεια και προτείνεται κυρίως σε εφαρμογές που έχουν σχέση με το Διαδίκτυο.

Προγράμματα Εμπιστοσύνης

Πολλές εταιρίες χρησιμοποιούν έξυπνες κάρτες σε προγράμματα εμπιστοσύνης για να εντοπίζουν και να δίνουν κίνητρα αγοράς στους τακτικούς πελάτες. Οι κάρτες αυτές είναι συνήθως κάρτες επαφής (contact cards) που μαζεύουν πόντους από αγορά προϊόντων ή υπηρεσιών από συγκεκριμένο πωλητή λιανικής. Οι πόντοι αυτοί ανταλλάσσονται με πιστώσεις, με βραβεία ή και άλλα στοιχεία. Μέσω του συστήματος αυτού, οι εταιρίες λιανικής πώλησης μπορούν για πρώτη φορά να έχουν λεπτομερή στοιχεία για τις προτιμήσεις των πελατών. Ειδικά για μεγάλες αλυσίδες πωλήσεων που διαχειρίζονται προγράμματα εμπιστοσύνης σε διαφορετικά αντικείμενα (όπως τα πολυκαταστήματα), πληροφορίες για τον πελάτη και τις προτιμήσεις του διαχειρίζονται και αποθηκεύονται κεντρικά σε μία έξυπνη κάρτα που κατέχει όλες τις πληροφορίες και δίνει την δυνατότητα στις εταιρίες λιανικής πώλησης να κάνουν σωστό σχεδιασμό της πολιτικής προσέγγισης των πελατών. Έτσι παρέχεται μεγαλύτερη ποιότητα στην εξυπηρέτηση των πελατών και σαφώς τα έσοδα για τις εταιρίες είναι μεγαλύτερα.

Έλεγχος Πρόσβασης

Σημαντική δραστηριότητα έχει παρουσιαστεί από μεγάλες εταιρίες και οργανισμούς, καθώς και από κυβερνήσεις για την εισαγωγή καινούριων συστημάτων ελέγχου πρόσβασης, τα οποία ελέγχουν την ταυτότητα και τα επίπεδα εξουσιοδότησης κάποιου πριν του δοθεί πρόσβαση φυσική (σε κάποιο κτίριο για παράδειγμα) ή λογική (π.χ. σε εμπιστευτικές πληροφορίες σε δίκτυα). Όσο περισσότερο οι ανωτέρω φορείς χρησιμοποιούν δίκτυα τοπικά

και μη, και το Διαδίκτυο για να αποθηκεύουν και να κοινοποιούν σημαντικές πληροφορίες σε αυτούς που τις χρειάζονται, τόσο περισσότερο επεκτείνεται η χρήση των έξυπνων καρτών σε αυτό το τομέα. Μεγάλες εμπορικές επιχειρήσεις όπως η Sun και η Microsoft, εφαρμόζουν συστήματα ελέγχου πρόσβασης που βασίζονται στη τεχνολογία των έξυπνων καρτών για να διαχειριστούν καθολικά την πρόσβαση εργαζομένων σε συγκεκριμένες πηγές. Σε αυτή την κατεύθυνση, οι έξυπνες κάρτες προσφέρουν ταχύτητα πρόσβασης και μειωμένα κόστη συντήρησης (ειδικά στην περίπτωση του ασύρματου ελέγχου πρόσβασης), πολλαπλά επίπεδα ταυτοποίησης και πλήθος μεθόδων κρυπτογράφησης και πιστοποίησης, καθώς και ευελιξία στη χρησιμοποίηση διαφορετικών καρτών λόγω σταθερών προτύπων που ακολουθούνται.

Υγεία

Οι ιατρικές έξυπνες κάρτες χρησιμοποιούνται κατά κόρον σε πολλές χώρες παγκοσμίως. Η τάση των τελευταίων ετών είναι η μεταφορά από συστήματα πληροφοριών ιατρικής φροντίδας που βασίζονται σε χαρτιά και έγγραφα σε ηλεκτρονικά συστήματα τα οποία προστατεύουν τα προσωπικά δεδομένα των κατόχων των καρτών. Οι έξυπνες ιατρικές κάρτες αποθηκεύουν πολλών ειδών ιατρικές πληροφορίες που αφορούν τον κάτοχο, όπως λεπτομέρειες για αλλεργίες και χρόνιες ασθένειες. Μπορούν να έχουν αποθηκευμένες παλιές, επαναλαμβανόμενες ή και νέες συνταγές ιατρών καθώς και διάφορες θεραπείες στις οποίες ο κάτοχος έχει υποβληθεί. Για τους ασθενείς, αυτός ο τρόπος αυξάνει την ποιότητα της παρεχόμενης ιατρικής φροντίδας, ενώ για τους παροχείς της ιατρικής βοήθειας, μειώνονται τα λειτουργικά κόστη και αυξάνεται η αποτελεσματικότητα της δράσης τους. Το κυριότερο είναι ότι με αυτή τη μέθοδο, σώζονται πραγματικά ζωές, αφού το ηλεκτρονικό ιατρικό ιστορικό του ασθενή είναι εύκολα προσβάσιμο και μπορεί να μεταφέρεται. Πολλές χώρες με εθνικά προγράμματα ιατρικής φροντίδας χρησιμοποιούν συστήματα έξυπνων καρτών, το μεγαλύτερο των οποίων λειτουργεί στη Γερμανία όπου πάνω από 80.000.000 κάρτες έχουν μοιραστεί σε κάθε άτομο στη Γερμανία και την Αυστρία.

Πανεπιστημιακοί χώροι

Πανεπιστήμια και σχολές σε πολλές χώρες χρειάζονται ένα τρόπο αναγνώρισης της ταυτότητας των εργαζομένων και των φοιτητών και χρησιμοποιούν τη τεχνολογία των έξυπνων καρτών για αυτό το σκοπό. Οι περισσότεροι από τους κατόχους αυτών των καρτών έχουν πρόσβαση σε συγκεκριμένες πληροφορίες, εξοπλισμό και τμήματα, ανάλογα με τις συνθήκες και τα χαρακτηριστικά της θέσης τους. Έξυπνες κάρτες πολλαπλών διεργασιών περιέχουν τα στοιχεία ταυτότητας με χαρακτηριστικά πρόσβασης ενώ επίσης μπορούν να αποθηκεύουν αξία (χρήματα) για χρήση σε διάφορους χώρους εντός των πανεπιστημίων, όπως τα κυλικεία ή κάποια καταστήματα. Γίνονται έτσι ένα εύκολο εργαλείο για τον εργαζόμενο και τον φοιτητή ο οποίος με μία κάρτα μπορεί να κινηθεί όπου επιθυμεί και να καλύψει τις ανάγκες του στο συγκεκριμένο χώρο. Για παράδειγμα, το Πανεπιστήμια της Florida, έχει εκδώσει 40.000 κάρτες οι οποίες εξυπηρετούν λειτουργίες προσωπικής ταυτοποίησης, τραπεζικών συναλλαγών και πρόσβασης σε σπουδαστικούς χώρους για τους φοιτητές ενώ ταυτόχρονα λειτουργούν ως κάρτες προπληρωμένης αξίας για υπηρεσίες σίτισης, τηλεφωνίας και μετακίνησης μέσα στο Πανεπιστήμιο.

5.4 Ηλεκτρονική δημοπρασία

Με τον όρο ηλεκτρονική δημοπρασία (e-auction) εννοούμε την δημιουργία δικτυακών τόπων κατάλληλων για τη διεξαγωγή δημοπρασιών, χωρίς φυσική παρουσία των συμμετεχόντων και με την αξιοποίηση του διαδικτύου, ιδιωτικών ή ιδεατά ιδιωτικών δικτύων. Στις πιο σύγχρονες υλοποιήσεις του μοντέλου η ηλεκτρονική δημοπρασία μπορεί να είναι μια υπηρεσία που επιτρέπει στους χρήστες της να εκθέτουν τα προϊόντα που επιθυμούν προς δημοπράτηση μέσω του Διαδικτύου. Στις περισσότερο διαδεδομένες από αυτές τις υλοποιήσεις, ο διαπιστευμένος χρήστης της υπηρεσίας μπορεί, με πάρα πολύ απλό τρόπο, να προσθέσει στη Web σελίδα του μια υπηρεσία η οποία αναλαμβάνει να εμφανίζει στους επισκέπτες της σελίδας τα προϊόντα του, να δέχεται προσφορές για αυτά και να κρατάει στατιστικά στοιχεία για την κίνηση των προϊόντων και για τους υποψήφιους αγοραστές.

Το μοντέλο αυτό απευθύνεται σε οποιονδήποτε επιθυμεί να βρει αγοραστές για τα προϊόντα του μέσω του Διαδικτύου. Το μόνο που απαιτείται από πλευράς χρήστη είναι να έχει μια Web σελίδα η οποία θα φιλοξενεί την κατάλληλη υπηρεσία. Κατά τα άλλα η χρήση της υπηρεσίας δεν απαιτεί καθόλου ιδιαίτερες γνώσεις καθώς όλα γίνονται μέσω φιλικών προς τον χρήστη οδηγών (wizards). Αυτό είναι και το μεγάλο πλεονέκτημα της αφού επιτρέπει σε χρήστες χωρίς προγραμματιστικές γνώσεις να απευθυνθούν στο «ηλεκτρονικό» καταναλωτικό κοινό.
Ανεξάρτητα με το αν μιλάμε για το απλοϊκό ή το εξελιγμένο μοντέλο ηλεκτρονικής δημοπρασίας, οι σημαντικότερες και ταυτόχρονα αναγκαίες ενότητες για τη δημιουργία ενός συστήματος για τη διεξαγωγή ηλεκτρονικών δημοπρασιών είναι: ο κατάλογος δημοπρατούμενων προϊόντων, η εγγραφή μέλους, η πιστοποίηση (verification), η υποστήριξη, η επικοινωνία με το σύστημα δημοπρασίας, το περιβάλλον διεπαφής, η παραγγελία και πληρωμή, η παρουσίαση πληροφοριών δημοπρασίας, η παροχή λίστας συχνών ερωτήσεων (FAQ), η επικοινωνία μεταξύ των πελατών μέσα από Chat rooms, η παροχή δυνατότητας αυτόματης προσφοράς και η διανομή των προϊόντων. Οι ενότητες αυτές αναλύονται στη συνέχεια. Κατάλογος δημοπρατούμενων προϊόντων Η επιχείρηση έχει τη δυνατότητα να παρουσιάσει στον καταναλωτή μια λίστα με τα προϊόντα ή τις υπηρεσίες που προσφέρει, διευκολύνοντάς τον και παρέχοντάς του άμεσα την πληροφορία για τα προϊόντα της, χωρίς να τον αναγκάσει να χρησιμοποιήσει κάποια μηχανή αναζήτησης. Τα προϊόντα ωφέλιμο είναι να είναι σωστά κατηγοριοποιημένα, να συνοδεύονται από τιμές, ακριβή χαρακτηριστικά, σύντομη αλλά και εκτενή περιγραφή καθώς και σχόλια και κριτικές από άλλους πελάτες που έχουν αγοράσει το προϊόν ή έχουν χρησιμοποιήσει την υπηρεσία. Οι πληροφορίες για τα προσφερόμενα αγαθά αναγκαίο είναι να χαρακτηρίζονται από επάρκεια, έτσι ώστε ο καταναλωτής να παίρνει πλήρη εικόνα γι' αυτά και άρα η απόφαση του να είναι σίγουρη.

Εγγραφή μέλους

Οι πελάτες που επισκέπτονται μια ηλεκτρονική δημοπρασία στο διαδίκτυο είναι είτε περαστικοί, οι οποίοι δεν έχουν δικαίωμα να συμμετέχουν ενεργά, είτε «γνωστοί» (καταχωρημένοι). Η καταχώρηση των χρηστών γίνεται συνήθως με τη συμπλήρωση μιας ηλεκτρονικής φόρμας στην οποία ο χρήστης προσδιορίζει συγκεκριμένα υποχρεωτικά στοιχεία. Ορισμένα από αυτά είναι: το όνομα, το επώνυμο, η ηλικία και το e-mail του. Στη συνέχεια, η εταιρία που είναι υπεύθυνη για τη διεξαγωγή της ηλεκτρονικής δημοπρασίας, στέλνει στο e-mail του χρήστη την επιβεβαίωση για την εγγραφή του, γνωστοποιώντας του επίσης το usemame και το password που θα χρησιμοποιεί ο χρήστης στο εξής. Σε αρκετές περιπτώσεις ο χρήστης έχει τη δυνατότητα να διαλέξει μόνος του το usemame και το password.

Υποστήριξη

Η υποστήριξη είναι απαραίτητη προϋπόθεση για την επιτυχία ενός συστήματος ηλεκτρονικής δημοπρασίας. Πρώτον, γιατί οι πελάτες νοιώθουν ανασφάλεια από την απουσία φυσικών προσώπων, στους οποίους μπορούν να απευθύνουν τα ερωτήματά τους και δεύτερον γιατί η υποστήριξη οδηγεί σε ευχαριστημένους πελάτες με προοπτικές να επαναλάβουν τις αγορές τους. Επικοινωνία με το σύστημα δημοπρασίας Το ηλεκτρονικό ταχυδρομείο χρησιμοποιείται για να προσφέρει την αμεσότητα που λείπει από μια απρόσωπη σχέση μεταξύ πελάτη και ηλεκτρονικού συστήματος δημοπρασίας. Αυτή η μορφή επικοινωνίας σε κάποιες περιπτώσεις προϋποθέτει τη δέσμευση υπαλλήλων που εξυπηρετούν τους πελάτες όταν οι τελευταίοι ζητούν να λάβουν πληροφορίες σχετικά με κάποιο ζήτημα που τους απασχολεί. Σε κάποιες άλλες περιπτώσεις η επικοινωνία είναι στερεότυπη. Για παράδειγμα, όταν ολοκληρωθεί μια ηλεκτρονική δημοπρασία είναι σκόπιμο, κάθε πελάτης να λαμβάνει ένα ηλεκτρονικό μήνυμα με περιεχόμενο τα στοιχεία του είδους που ο ίδιος «χτύπησε» (σκοπός του μηνύματος αυτού είναι η επιβεβαίωση του αποτελέσματος της δημοπρασίας). Στην περίπτωση αυτή, το ηλεκτρονικό μήνυμα δεν πρέπει να συντάσσεται χειρωνακτικά αλλά να συντίθεται και να αποστέλλεται αυτόματα από το web server που στηρίζει το σύστημα ηλεκτρονικής δημοπρασίας.

Σχεδίαση του περιβάλλοντος διεπαφής

Κατά την υλοποίηση του περιβάλλοντος διεπαφής πρέπει να ακολουθούνται κάποιες αρχές έτσι ώστε να διευκολύνεται η πλοήγηση των χρηστών μέσα στις ιστοσελίδες της επιχείρησης e-auction αλλά και η διεκπεραίωση της δημοπρασίας τους. Πρέπει να γίνεται όσο. το δυνατόν αναλυτικότερη περιγραφή των προϊόντων και επεξήγηση τεχνικών όρων. Στα συστήματα e-auction, ακριβώς επειδή δεν υπάρχει η δυνατότητα άμεσης επικοινωνίας με το προσωπικό της επιχείρησης, στο οποίο θα μπορούσε ο πελάτης να απευθυνθεί για ερωτήσεις, είναι αναγκαίο το περιεχόμενο των σελίδων να είναι επαρκώς περιγραφικό. Πρέπει κάθε προϊόν να συνοδεύεται με ανάλογη εικόνα, ενώ οι τεχνικοί όροι θα πρέπει αν εξηγούνται πιθανόν με την παραπομπή σε ένα γλωσσάριο. Συνήθως οι δικτυακές επιχειρήσεις μοιάζουν να είναι αχανείς και ακόμα και αν συμμορφώνονται με τις σχεδιαστικέ ς αρχές, δεν είναι λίγοι αυτοί οι χρήστες που δεν μπορούν να βρουν εύκολα αυτό που θέλουν. Επιβάλλεται σε αυτές τις περιπτώσεις η ύπαρξη δυνατότητας αναζήτησης στον ιστότοπο. Επίσης οφείλει η δυνατότητα αναζήτησης να είναι εμφανής από όλες τις ιστοσελίδες της e-auction επιχείρησης και όχι μόνο από την αρχική. Επίσης τα αποτελέσματα της αναζήτησης πρέπει να είναι περιγραφικά και καθοδηγητικά ιδίως σε περιπτώσεις λάθους.

Παραγγελία και πληρωμή

Όταν ο πελάτης κερδίσει τη δημοπρασία του προϊόντος που τον ενδιαφέρει, ολοκληρώνει τη συναλλαγή συμπληρώνοντας τα προσωπικά του στοιχεία μαζί με τον τόπο προορισμού και τον τρόπο αποστολής και διάθεσης που επιθυμεί και καταβάλλει το αντίτιμο με έναν από τους υπάρχοντες-ηλεκτρονικούς τρόπους πληρωμής που διαθέτει η επιχείρηση e-auction. Οι μέθοδοι πληρωμής είναι είτε με αντικαταβολή είτε, κυρίως, με ηλεκτρονική πληρωμή. Η ηλεκτρονική πληρωμή περιλαμβάνει τις πιστωτικές κάρτες (όπου ο καταναλωτής καλείται να επιδείξει την ικανότητα του να πληρώσει, παρουσιάζοντας τον αριθμό της πιστωτικής του κάρτας στην επιχείρηση e-auction) και τις ηλεκτρονικές επιταγές που στην ουσία είναι ένα μήνυμα προς την τράπεζα του καταναλωτή να μεταφέρει κεφάλαιο από το λογαριασμό του στο λογαριασμό της eauction επιχείρησης. Το μήνυμα αυτό δεν στέλνεται απευθείας στην

τράπεζα, αλλά στο μελλοντικό αποδέκτη του κεφαλαίου, ο οποίος πρέπει να εμφανίσει την επιταγή αυτή στην τράπεζα προκειμένου να εισπράξει το ποσό του κεφαλαίου που αναγράφεται. Αφού λάβει χώρα η μεταφορά κεφαλαίου, η επικυρωμένη και εξοφλημένη επιταγή επιστρέφει στον αποστολέα, και μπορεί έτσι να χρησιμοποιηθεί ως απόδειξη της πληρωμής. Η Τρίτη μέθοδος ηλεκτρονικής πληρωμής είναι το ψηφιακό χρήμα.
Πληροφορίες δημοπρασίας
Περιλαμβάνουν όλες της απαραίτητες πληροφορίες που πρέπει να γνωρίζει ο χρήστης προκείμενου να πάρει μέρος σε μια ηλεκτρονική δημοπρασία. Έτσι λοιπόν θα πρέπει να γνωρίζει τουλάχιστον την αρχική τιμή, την τελική (επιδιωκόμενη) τιμή και τη διάρκεια της ηλεκτρονικής δημοπρασίας.

Λίστα Συχνών Ερωτήσεων (FAQ)

Τα ερωτήματα των πελατών επαναλαμβάνονται με μεγάλη συχνότητα. Οι λίστες συχνών ερωτήσεων (FAQ) αποτελούνται από έναν κατάλογο ερωτήσεων που έχουν καταγραφεί ως ερωτήσεις, οι οποίες υποβάλλονται συχνά και συνοδεύονται από κατατοπιστικές απαντήσεις.
Chat rooms
Πρόκειται για χώρους διαδικτυακής συζήτησης, όπου οι πελάτες ανταλλάσσουν απόψεις και εμπειρίες σε σχέση με προϊόντα / υπηρεσίες και διαδικασίες του e- auction.
Αυτόματη προσφορά
Μπορεί ένας πελάτης (Α) να θέσει ένα άνω όριο χρημάτων και όταν κάποιος άλλος πελάτης (Β) χτυπήσει ένα προϊόν που ενδιαφέρει τον Α, τότε αυτόματα το σύστημα να υποβάλει μία νέα πρόσφορα για λογαριασμό του Α, εφόσον η τελική τιμή δεν ξεπερνά το άνω όριο.
Διανομή
Η διανομή των προϊόντων μπορεί να γίνει είτε φυσικά, είτε με ηλεκτρονικό τρόπο. Στις ηλεκτρονικές δημοπρασίες χρησιμοποιείται κυρίως ο πρώτος τρόπος. Σε αυτήν χρησιμοποιούνται όλοι οι υπάρχοντες τρόποι όπως το ταχυδρομείο (air-mail, συστημένο, απλό), η ταχυαποστολή (courier) ακόμη κάποια υπηρεσία διανομής που μπορεί να ανήκει στην e-auction επιχείρηση (εφόσον πρόκειται για μεγάλη εταιρία).
Η διαδικασία της ηλεκτρονικής δημοπρασίας.
Στη συνέχεια παρουσιάζεται η διαδικασία διεξαγωγής ηλεκτρονικής δημοπρασίας. Στα βήματα που παραθέτουμε, ο όρος δημοπράτης αναφέρεται στον παροχέα και διαχειριστή του συστήματος ηλεκτρονικής δημοπρασίας και όχι στον εκάστοτε πωλητή. Ο δημοπράτης καλεί τους πωλητές να καταθέσουν μια πρόταση δημοπρασίας, προσδιορίζοντας όλες τις αναγκαίες παραμέτρους και τους ενημερώνει για την ημέρα και ώρα ανοίγματος (έναρξης) της δημοπρασίας.
Οι αγοραστές ενημερώνονται για τις επιμέρους παραμέτρους της δημοπρασίας. Οι παράμετροι συνήθως είναι:

1. Τιμή Ανοίγματος (Opening Price)
2. Επιδιωκόμενη Τιμή (Reserved Price)
3. Βήμα δημοπρασίας (Bid Increment)
4. Διάρκεια δημοπρασίας - παράταση
5. Νόμισμα
6. Proxy Bidding (αυτόματη υποβολή προσφορών)

Ο δημοπράτης παρέχει το κατάλληλο λογισμικό και την αντίστοιχη εκπαίδευση . Από την έναρξη και μετά, οι αγοραστές υποβάλουν τις προσφορές τους. Για να γίνουν δεκτές ελέγχεται αν αυτές τηρούν το ελάχιστο όριο διαφοράς (ή το βήμα) της μιας προσφοράς από την άλλη. Όταν παρέλθει ο χρόνος λήξης, ο δημοπράτης διακόπτει τη δημοπρασία. Η

διάρκειά της ορίζεται, συνήθως, στη μισή ή μία ώρα, με δυνατότητα ολιγόλεπτων παρατάσεων.

Ο δημοπράτης έχει τη δυνατότητα να εξετάσει τις προσφορές και να τις συγκρίνει μεταξύ τους, λαμβάνοντας υπόψη και άλλες παραμέτρους πέραν της τιμής. Ο πωλητής έχει τη δυνατότητα να ελέγξει τις προσφορές, ώστε να βεβαιωθεί για την ποιότητα, τις υπηρεσίες και τα άλλα κριτήρια αξιολόγησης της προσφοράς. Όλοι οι συμμετέχοντες ενημερώνονται για τις εξελίξεις και τα τελικά αποτελέσματα. Κατά τη διάρκεια της δημοπρασίας μόνο ο αριθμός των συμμετεχόντων στην δημοπρασία είναι ορατός στους συμμετέχοντες (αγοραστές και πωλητές), ενώ η ταυτότητά τους παραμένει άγνωστη. Στους περισσότερους δικτυακούς τόπους δημοπρασιών η συμμετοχή είναι δωρεάν για τους αγοραστές. Οι πωλητές συνήθως καταβάλλουν στο δημοπράτη, ένα ποσοστό της τελικής τιμής που πέτυχαν.

Πλεονεκτήματα ηλεκτρονικών δημοπρασιών

Οι ηλεκτρονικές δημοπρασίες μπορούν να αποφέρουν τεράστια οικονομικά οφέλη τόσο στους πωλητές όσο και στους αγοραστές.

Πλεονεκτήματα για τον αγοραστή:

1. Βελτιωμένη προσβασιμότητα.
2. Μεγαλύτερη αμεσότητα.
3. Αυτόματη διαχείριση προσφορών (ανώτατο όριο δαπάνης).
4. Παράλληλο, έναντι σειριακού, μοντέλο δημοπρασίας (οικονομία χρόνου, ποικιλία προϊόντων).
5. Ανωνυμία (εμπιστοσύνη, αποφυγή δημιουργίας προφίλ, κλπ).
6. Αυξημένες δυνατότητες προσφορών (χρονικά περιθώρια για έρευνα αγοράς).
7. Εργαλεία για τον εντοπισμό προϊόντων (φιλτράρισμα σύμφωνα με τα κριτήρια του χρήστη).

Πλεονεκτήματα για τον πωλητή:

1. Έλλειψη άγχους με το παράλληλο, έναντι του σειριακού, μοντέλου δημοπρασίας.
2. Ποσοτικοποίηση επιθυμίας καταναλωτή για αγορά με την εφαρμογή της τιμολογιακής τεχνικής "one to one pricing".
3. Συνεχής διάθεση προϊόντων.
4. Συμπίεση κόστους διαδικασίας (χαρτί, γραφειοκρατικά έξοδα).

ΒΙΒΛΙΟΓΡΑΦΙΑ

Έντυπη

1) Βουκάλης Δημήτριος, Εφαρμοσμένη Κρυπτογραφία, Σύγχρονη εκδοτική, 2007.

2) Γκρίτζαλης Δημήτριος, Γκρίτζαλης Στέφανος, Κάτσικας Σωκράτης, Ασφάλεια Δικτύων υπολογιστών, Εκδόσεις Παπασωτηριου, 2003.

3) Γρηγοριάδης Νίκος, Πατσός Δημήτριος, Σουρής Ανδρέας, Ασφάλεια της πληροφορίας, Εκδόσεις Νέων Τεχνολογιών, 2004.

4) Ζάχος Ευστάθιος, Θεωρία αριθμών και κρυπτογραφίας, Εθνικό Μετσόβιο Πολυτεχνείο, 2007.

5) Ζορκάδης Βασίλειος, Θεωρία Πληροφορίας και Κωδικοποίησης, Ελληνικό Ανοικτό Πανεπιστήμιο - Πάτρα, 2002.

6) Κάτος Βασίλειος, Στεφανίδης Γεώργιος, Τεχνικές κρυπτογραφία ς & κρυπτανάλυσης, Εκδόσεις Ζυγός, 2003.

7) Νάστου Παναγιώτης, Σπυράκης Παύλος, Σταματίου Γιάννης., Σύγχρονη κρυπτογραφία, Ελληνικά Γράμματα, 2003.

8) Πουλάκης Δημήτριος, Κρυπτογραφία - η επιστήμη της ασφαλούς επικοινωνίας, Εκδόσεις Ζήτη, 2004.

9) Singh Simon, μετάφραση Κυριαζόπουλος Νάσος, Κώδικες και μυστικά, Εκδόσεις Τραυλός, 2001.

Ηλεκτρονική

10) www.math.uoc.gr

11) el.wikipedia.org

12) www.harica.gr

13) www.islab.demokritos.gr

14) nefeli.lib.teicrete.gr

15) www.ceid.upatras.gr

16) www.smartcardbasics.com

17) www.smartcardalliance.org