**Τ.Ε.Ι Πάτρας**
**Σχολή Οικονομίας και Διοίκησης**
**Τμήμα Επιχειρηματικού Σχεδιασμού και Πληροφοριακών Συστημάτων**

**Πτυχιακή Εργασία**

# Βασικές Αρχές Κρυπτογράφησης και Εφαρμογές τους


**Σπουδάστριες:** **Βαλμά Καλλιόπη**
**Κανελλοπούλου Χριστίνα**
**Καρλή Μαρία**

**Εισηγήτρια:** **κ. Καλαπόδη Αλέκα**

**Πάτρα 2008**

**Και πάντα να θυμάστε:**

**«Δεν υπάρχει κωδικός φτιαγμένος από έναν άνθρωπο**
**που να είναι αδύνατον να σπάσει από έναν άλλο άνθρωπο».**

**ΠΕΡΙΕΧΟΜΕΝΑ**

# Πρόλογος

Η κρυπτογραφία δεν αποτελεί μια σύγχρονη έννοια. Από την αρχαιότητα, με την ανάπτυξη του γραπτού λόγου ως μέσου επικοινωνίας, δημιουργήθηκε η ανάγκη για διασφάλιση των γραπτών πληροφοριών ούτως ώστε να μη γίνονται αντιληπτές από οποιονδήποτε «πέσουν στα χέρια του», αλλά αποκλειστικά και μόνο από τον νόμιμο παραλήπτη.

Άλλωστε, η λέξη κρυπτογραφία (cryptography) είναι σύνθετη. Αποτελείται από:

- το πρώτο συνθετικό, το κρυπτό και
- το δεύτερο συνθετικό, το γράφω.

Ουσιαστικά κρυπτογραφία σημαίνει κρύβω αυτά που γράφω. Η κρυπτογραφία λοιπόν είναι η επιστήμη ή η τέχνη της απόκρυψης του γραπτού λόγου από ανεπιθύμητους αναγνώστες.

Οι αρχικοί αλγόριθμοι για την κρυπτογράφηση των κειμένων βασίζονταν σε απλές αντικαταστάσεις των γραμμάτων του εκάστοτε αλφαβήτου. Εδώ αξίζει να σημειωθεί πως εμπνευστής της μεθόδου αυτής, η οποία αποτέλεσε τη βάση για πολλές μεταγενέστερες, ήταν ο Ιούλιος Καίσαρας.

Στη συνέχεια, τόσο η ανάπτυξη των νέων τεχνολογιών πληροφοριών όσο και η εξέλιξη των επικοινωνιακών μέσων, δημιούργησαν την ανάγκη για επινόηση όλο και πιο σύγχρονων μεθόδων κρυπτογράφησης.

Πλέον μπορούμε να πούμε πως η κρυπτογραφία παίζει πρωταγωνιστικό ρόλο στις καθημερινές μας δραστηριότητες. Η ασφάλεια των περισσότερων συναλλαγών μας αλλά και των επικοινωνιακών δικτύων που χρησιμοποιούμε, βασίζονται σε κρυπτογραφικές εφαρμογές.

Στην εργασία αυτή, ξεκινάμε το πρώτο κεφάλαιο με μια σύντομη ιστορική αναδρομή στην εμφάνιση και την ανάπτυξη της κρυπτογραφίας. Στη συνέχεια εξετάζονται απλές πρακτικές κρυπτογράφησης, η έννοια της κρυπτανάλυσης και η εξέλιξή τους.

Στο δεύτερο κεφάλαιο περιγράφονται οι σύγχρονες μέθοδοι κρυπτογράφησης και οι αλγόριθμοι που χρησιμοποιούνται. Επίσης αναλύονται διάφορα προγράμματα κρυπτογράφησης και πρωτόκολλα ασφαλείας.

Το τρίτο κεφάλαιο παρουσιάζει τις εφαρμογές της κρυπτογραφίας στον οικονομικό τομέα. Πιο συγκεκριμένα, αναφέρονται τα «μέτρα» που λαμβάνονται για την ασφάλεια των συναλλαγών στις ηλεκτρονικές επιχειρήσεις, στις υπηρεσίες του e- banking, στα μηχανήματα αυτόματης ανάληψης και κατάθεσης χρημάτων (ATM), στη χρήση έξυπνων καρτών και τέλος στη διενέργεια μιας ηλεκτρονικής δημοπρασίας.

Το τέταρτο κεφάλαιο ασχολείται με τη χρησιμότητα της κρυπτογραφίας στα επικοινωνιακά δίκτυα. Αναλυτικότερα, δίνεται η έννοια της εφαρμογής πολιτικών ασφαλείας σε ασύρματα και ενσύρματα επικοινωνιακά δίκτυα, ενώ παράλληλα περιγράφονται τεχνικές «δικτύωσης».

Η εργασία ολοκληρώνεται με μια σύντομη αναφορά στον κρατικό έλεγχο όσον αφορά την ισχυρή κρυπτογραφία.

# Κεφάλαιο 1

# Η εξέλιξη της κρυπτογραφίας μέσα στο πέρασμα των χρόνων

(Για το κεφάλαιο που ακολουθεί χρησιμοποιήθηκαν στοιχεία από τις πηγές [7], [19], [20], [25], [39], [40]).

Η μετάβαση από τον προφορικό λόγο στο γραπτό ήταν σίγουρα ένα μεγάλο βήμα για τον ανθρώπινο πολιτισμό. Βέβαια από τα χρόνια του αρχαίου Ελληνικού πολιτισμού υπήρχε επίγνωση των αρνητικών συνεπειών που επέφερε η καταγραφή κάθε είδους πληροφορίας. Συγκεκριμένα, η κύρια αρνητική συνέπεια της γραφής ήταν ότι μπορούσε το γραπτό να πέσει σε χέρια που δεν έπρεπε. Άρα λοιπόν ή δεν έπρεπε να γράφονται πληροφορίες ζωτικής σημασίας ή έπρεπε να βρεθεί τρόπος προστασίας των γραπτών αυτών πληροφοριών ώστε να μπορούν να διαβαστούν μόνο από αυτούς που έπρεπε. Ιστορικά, η εξέλιξη της κρυπτογραφίας μπορεί να παρουσιαστεί σε τέσσερεις περιόδους:

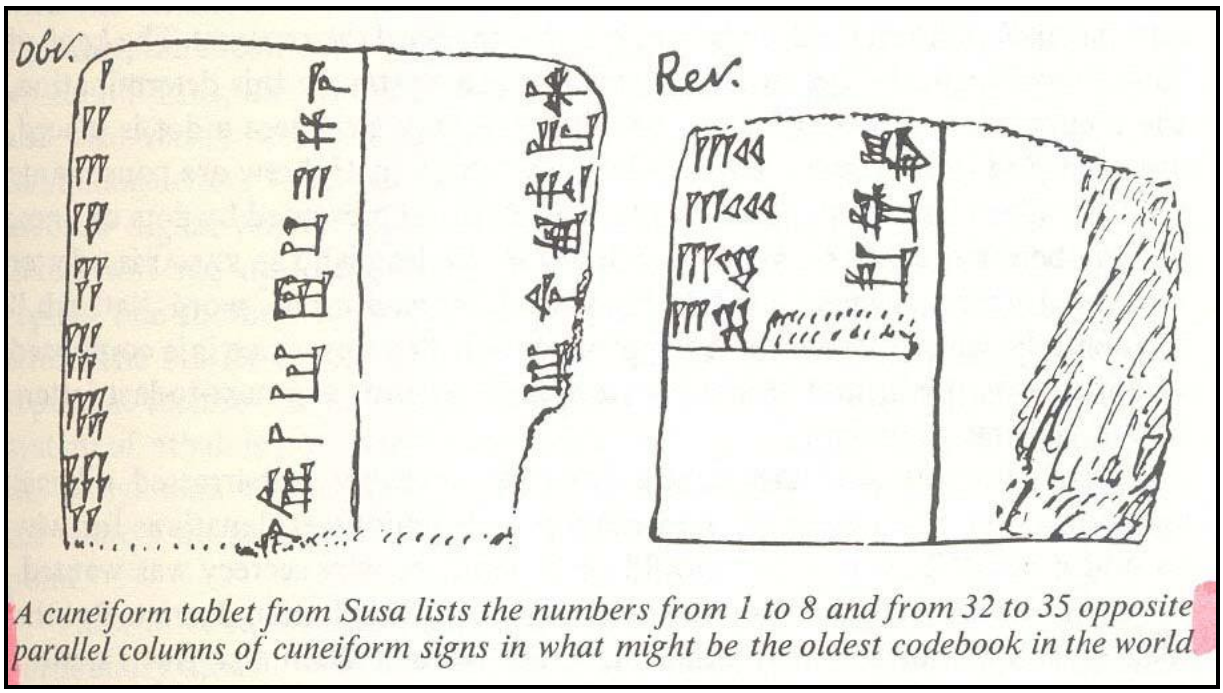
- η πρώτη περίοδος περιλαμβάνει τα απλά κρυπτογραφικά συστήματα που αναπτύχθηκαν την προχριστιανική εποχή και βασίζονταν σε απλές αντικαταστάσεις
- η δεύτερη περίοδος εκτείνεται από την αρχαιότητα μέχρι το 1900 μ. Χ. και περιλαμβάνει διάφορα συστήματα κρυπτογράφησης, μεγαλύτερης πολυπλοκότητας από εκείνα της πρώτης περιόδου, τα οποία ουσιαστικά μελετήθηκαν μετά τον $14^{ο}$ αιώνα μ. Χ.
- η τρίτη περίοδος εκτείνεται από το 1900 μ.Χ. έως το 1950 μ.Χ., όπου εμφανίζονται τα πρώτα μηχανικά συστήματα κρυπτογράφησης

- η τέταρτη περίοδος ξεκινά το 1950 μ.Χ. και φτάνει ως σήμερα, όπου η κρυπτογραφία αποκτά θεωρητική επιστημονική βάση και αναπτύσσονται αλγοριθμικά συστήματα κρυπτογράφησης.

## 1.1 Πρώτη Περίοδος Κρυπτογραφίας.

Κατά την διάρκεια αυτής της περιόδου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, που βασιζόταν 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 κρυπταναλυθεί και έχει αποδειχθεί ότι εάν μας 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 στην 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.



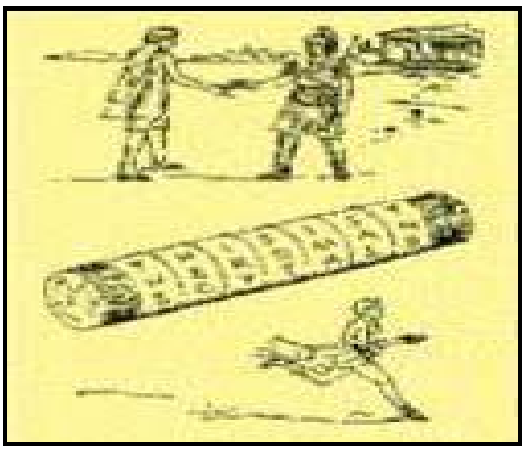

**Εικόνα 1:** Σφηνοειδής επιγραφή, που ανακαλύφθηκε στα Σούσα της Περσίας.

Επίσης, το αρχαιότερο βιβλίο κρυπτοκωδικών στον κόσμο θεωρείται μία σφηνοειδής επιγραφή στα Σούσα της Περσίας. Η επιγραφή αυτή 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 (Εικόνα 1).

**Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες.** Γύρω στον 5ο π.Χ. αιώνα εφεύραν την πρώτη κρυπτογραφική συσκευή, τη «σκυτάλη», στην οποία χρησιμοποιήθηκε η μέθοδος της αντικατάστασης.

Polybius Square

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | a | b | c | d | e |
| 2 | f | g | h | i/j | k |
| 3 | l | m | n | o | p |
| 4 | q | r | s | t | u |
| 5 | v | w | x | y | z |



Σκυτάλη (Σπάρτη)

**Εικόνα 2:** Η πρώτη κρυπτογραφική συσκευή «Σπαρτιατική Σκυτάλη».

Όπως αναφέρει ο Πλούταρχος, η «Σπαρτιατική Σκυτάλη» (Εικόνα 2), 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 ξετύλιγαν τη λωρίδα το κείμενο ήταν ακατάληπτο εξαιτίας της ανάμειξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης!

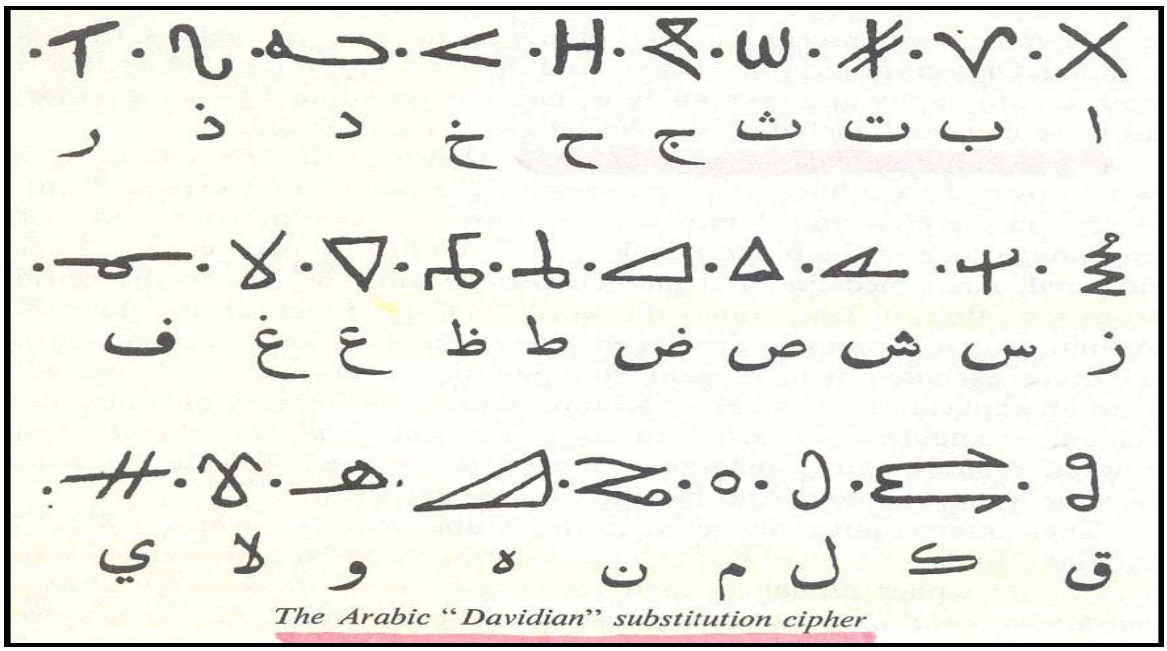
Γενικά, στην αρχαιότητα χρησιμοποιήθηκαν κυρίως συστήματα τα οποία βασίζονταν στην στεγανογραφία και όχι τόσο στην κρυπτογραφία. Οι Έλληνες συγγραφείς δεν αναφέρουν αν και πότε χρησιμοποιήθηκαν συστήματα γραπτής αντικατάστασης γραμμάτων, αλλά τα βρίσκουμε στους Ρωμαίους κυρίως την εποχή του Ιουλίου Καίσαρα.

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 ακόμα και 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 βιβλίο αυτό δυστυχώς δεν διασώθηκε αλλά, αν και χαμένο, θεωρείται **το πρώτο βιβλίο κρυπτολογίας**. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες.

## 1.2 Δεύτερη Περίοδος Κρυπτογραφίας

Στην διάρκεια του Μεσαίωνα η κρυπτολογία ήταν κάτι το απαγορευμένο και αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας, κάτι που συντέλεσε στην καθυστέρηση της ανάπτυξής της. Παρόλα αυτά, 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 (Εικόνα 3).

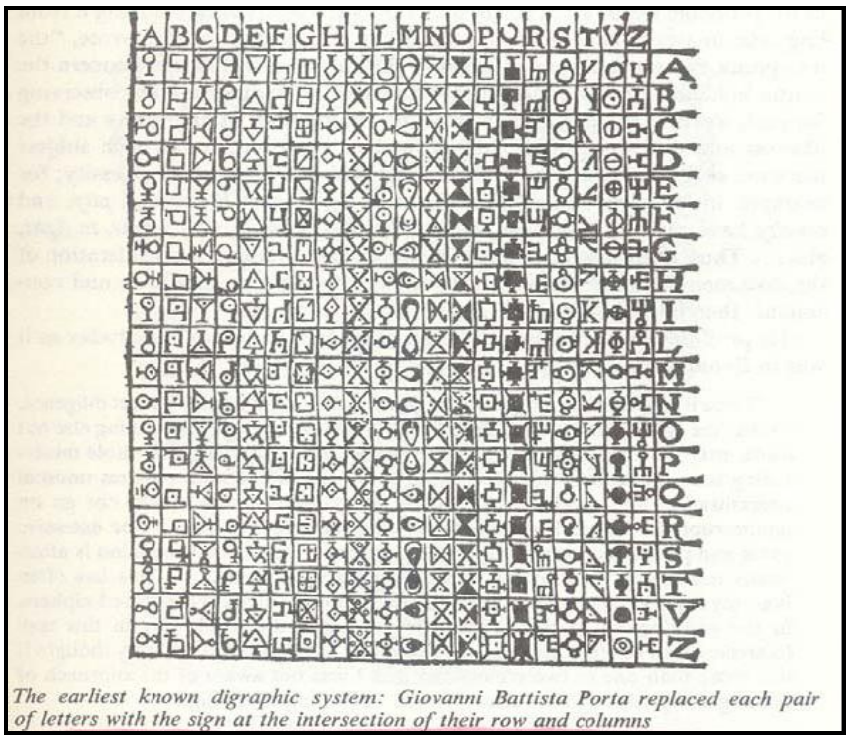



**Εικόνα 3:** Το αλφάβητο «Dawoudi».

Οι Άραβες είναι οι πρώτοι που ανακάλυψαν και χρησιμοποίησαν μεθόδους κρυπτανάλυσης. Γύρω στον 14$^{ο}$ αιώνα ανακάλυψαν πως το κυριότερο εργαλείο στην κρυπτανάλυση, ήταν η χρησιμοποίηση των συχνοτήτων των γραμμάτων κειμένου σε συνδυασμό με τις συχνότητες εμφάνισης στα κείμενα των γραμμάτων της γλώσσας.

Η κρυπτογραφία λόγω κυρίως των στρατιωτικών εξελίξεων, σημείωσε σημαντική ανάπτυξη στους επόμενους αιώνες. Οι σημαντικότεροι σταθμοί στην ανάπτυξη αυτή είναι οι ακόλουθοι:

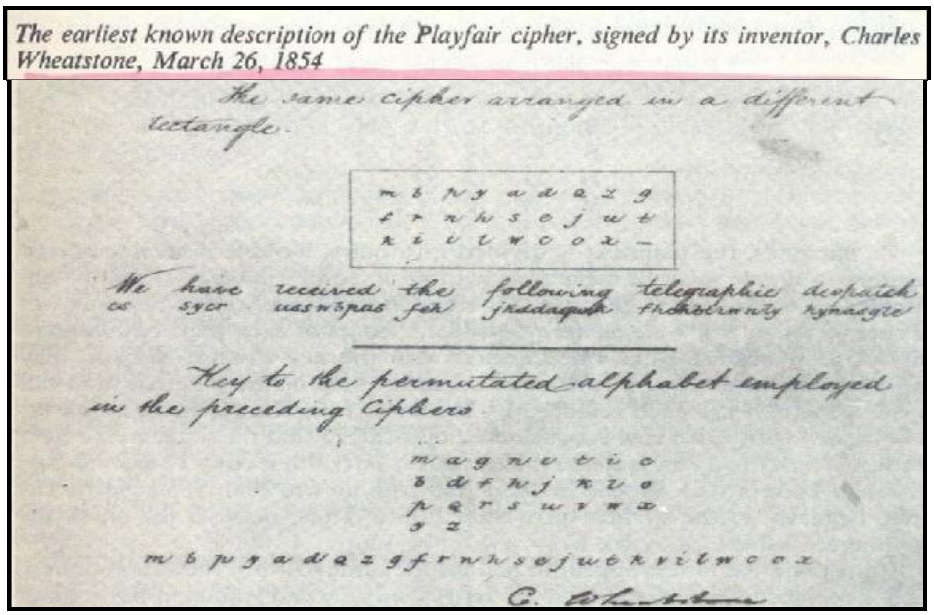
**1.** Ο Ιταλός **Giovanni Batista Porta**, το 1563, δημοσίευσε το περίφημο για την κρυπτολογία βιβλίο «De furtivis literarum notis», με το οποίο έγιναν γνωστά τα πολυαλφαβητικά συστήματα κρυπτογράφησης και τα διγραφικά κρυπτογραφήματα στα οποία δύο γράμματα αντικαθίστανται από ένα (Εικόνα 4).




**Εικόνα 4**: Βιβλίο κρυπτολογίας «De furtivis literarum notis».

**2.** Σημαντικός εκπρόσωπος εκείνης της εποχής είναι και ο Γάλος **Vigenere,** του οποίου ο πίνακας πολυαλφαβητικής αντικατάστασης χρησιμοποιείται ακόμη και σήμερα.

**3.** Ο **C.Wheatstone**, γνωστός από τις μελέτες του στον ηλεκτρισμό, παρουσίασε την πρώτη μηχανική κρυπτοσυσκευή, η οποία αποτέλεσε τη βάση για την ανάπτυξη των κρυπτομηχανών της δεύτερης ιστορικής περιόδου της κρυπτογραφίας (Εικόνα 5).




**Εικόνα 5:** Πρώτη μηχανική κρυπτοσυσκευή.

**4**. Η <u>σημαντκότερη αποκρυπτογράφηση</u> 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 στο 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.

Το 17ο αιώνα αναθερμάνθηκε το ενδιαφέρον για την αποκρυπτογράφηση των ιερογλυφικών. Έτσι το 1652 ο Γερμανός ιερέας **Α. Κίρχερ** εξέδωσε ένα λεξικό ερμηνείας τους με τίτλο «Oedipous Aegyptiakus». Με βάση αυτό προσπάθησε να ερμηνεύσει τις αιγυπτιακές γραφές αλλά η προσπάθεια του ήταν κατά γενική ομολογία αποτυχημένη. Για παράδειγμα, το όνομα του Φαραώ Απρίλη το ερμήνευσε σαν «τα ευεργετήματα του θεϊκού Όσιρι εξασφαλίζονται

μέσω των ιερών τελετών της αλυσίδας των πνευμάτων, ώστε να επιδαψιλευθούν τα δώρα του Νείλου».

**5.** Παρόλα αυτά, η προσπάθειά του άνοιξε τον δρόμο προς την σωστή ερμηνεία των ιερογλυφικών**.** Σημείο σταθμό αποτέλεσε η ανακάλυψη της στήλης της Ροζέτας (εικόνα 6) η οποία αποκρυπτογραφήθηκε, τελικά, από τον **Γιάνγκ** και τον **Σαμπολιόν**.

**Εικόνα 6:** Η στήλη της Ροζέτας .

Όπως βλέπουμε και στην εικόνα 6, η στήλη της ροζέτας ήταν μια πέτρινη στήλη που βρήκαν τα στρατεύματα του Ναπολέοντα στην Αίγυπτο και είχε χαραγμένο πάνω της το ίδιο κείμενο, τρεις φορές: α) Μια στα ιερογλυφικά, β) μια στα ελληνικά και γ) μια στα ιερατικά.

**6.** Οι προϊστορικοί πληθυσμοί χρησιμοποίησαν κυρίως 3 γραφές, μέχρι να επινοήσουν αλφάβητο, γύρω στο 850 π.Χ.

<u>Χρονολογικά, οι γραφές αυτές κατατάσσονται ως εξής:</u>

3000 1600 π.Χ. : Εικονογραφική (Ιερογλυφική) γραφή

1850 1450 π.Χ.: Γραμμική γραφή Α

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. Η ιερογλυφική γραφή συνυπήρχε με την γραμμική γραφή Α, τόσο χρονικά όσο και τοπικά, όπως προκύπτει από τις ανασκαφές στο ανάκτορο Μαλίων της Κρήτης. Εμφανίζεται στο **Δίσκο της Φαιστού** (Εικόνα 7) που ανακαλύφθηκε το 1908, στην νότια Κρήτη.

**Εικόνα 7:** Ο Δίσκος της Φαιστού.

Πρόκειται για μια κυκλική πινακίδα, που χρονολογείται γύρω στο 1700 π.Χ. και φέρει γραφή με την μορφή δύο σπειρών. Τα σύμβολα δεν είναι χειροποίητα αλλά έχουν χαραχθεί με την βοήθεια μίας ποικιλίας σφραγίδων καθιστώντας τον Δίσκο ως το αρχαιότερο δείγμα στοιχειοθεσίας. Δεν υπάρχει άλλο ανάλογο εύρημα, έτσι η αποκρυπτογράφηση στηρίζεται σε πολύ περιορισμένες πληροφορίες. Μέχρι σήμερα δεν έχει αποκρυπτογραφηθεί και παραμένει η πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή.

Οι πρώτες επιγραφές με Γραμμική γραφή ανακαλύφθηκαν από τον **Sir Arthur Evans**, το μεγάλο Άγγλο αρχαιολόγο, που άνεσκαψε 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 στην σφηνοειδή γραφή ή εικόνες όντων, όπως στην αιγυπτιακή ιερατική. Ειδικότερα:

I. *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 δεν έχουν βρεθεί μόνο στην Κνωσό και Φαιστό της Κρήτης, αλλά και στη Μήλο και τη Θήρα. Παρά την πρόοδο που έχει σημειωθεί, η γραμμική γραφή Α δεν έχει αποκρυπτογραφηθεί ακόμη. Ωστόσο πλάκες με επιγραφές σε γραμμική Α, εκτίθενται στο Μουσείο Ηρακλείου.

II. Ο Evans έδωσε και την ονομασία στην *Γραμμική γραφή Β*, επειδή αναγνώρισε ότι πρόκειται για συγγενική γραφή με την γραμμική Α, αλλά πιο πρόσφατη επομένως και πιο εξελιγμένη. Με βάση όσα γνωρίζουμε σήμερα, η γραφή αυτή υιοθετήθηκε αποκλειστικά για λογιστικούς σκοπούς. Πινακίδες χαραγμένες με την 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. Οι γραφείς 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, χρησιμοποιούνταν «ομάδες» ή «πολύπτυχα» πινακίδων, οι οποίες εμφανίζουν κοινά χαρακτηριστικά 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.

**7.** Συστηματικά με την Γραμμική Β, 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 άποψή του αυτή δεν έγινε δεκτή αρχικά από τους ειδικούς. Στην συνέχεια όμως αρκετοί προσχώρησαν στην άποψή του.

**8.** 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 συμπεράσματα 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».

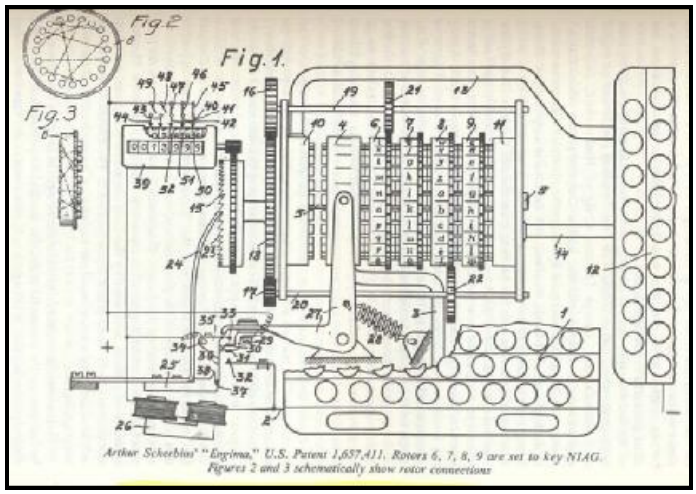
## 1.3 Τρίτη Περίοδος Κρυπτογραφίας

Η τρίτη περίοδος της κρυπτογραφίας 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 την 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 για μεγάλο χρονικό διάστημα. Ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ.

Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά την διάρκεια αυτής της περιόδου, η κρυπτανάλυση τους είναι συνήθως επιτυχημένη. Οι Γερμανοί έκαναν εκτενή χρήση (σε διάφορες παραλλαγές) ενός συστήματος γνωστού ως Enigma (Εικόνες 8-9).

**Εικόνα 8:** Κρυπτομηχανή Enigma.




**Εικόνα 9 :** Οι καλωδιώσεις της μηχανής Enigma.

<u>Παρόλο που το σύστημα κρυπτογράφησης enigma θεωρούνταν απαραβίαστο:</u>

Ο Marian Rejewski, στην Πολωνία, επιτέθηκε και παραβίασε την πρώτη μορφή του χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ήταν η πιο εντυπωσιακή ανακάλυψη στην κρυπτολογική ανάλυση της χιλιετίας. Οι Πολωνοί συνέχισαν να παραβιάζουν τα μηνύματα που βασίζονταν στην κρυπτογράφηση με την μηχανή Enigma μέχρι το 1939.

Τότε, ο γερμανικός στρατός έκανε κάποιες αλλαγές και οι Πολωνοί δεν μπόρεσαν να ακολουθήσουν γιατί η παραβίαση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν.

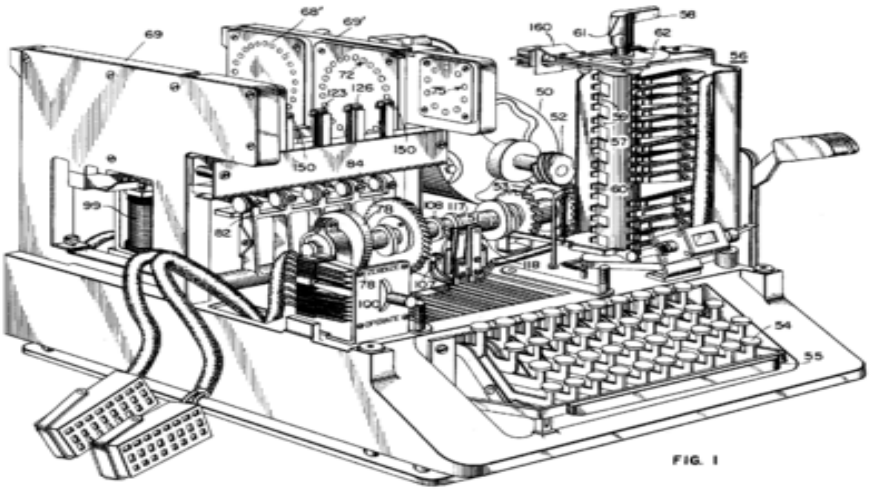
Έτσι, εκείνο το καλοκαίρι μεταβίβασαν τη γνώση τους μαζί με μερικές μηχανές που είχαν κατασκευάσει στους Βρετανούς και τους Γάλλους. Ακόμη και ο Rejewski, καθώς και όλοι οι μαθηματικοί και κρυπτογράφοι της ομάδας του κατέληξαν να συνεργάζονται με τους Βρετανούς και τους Γάλλους μετά από αυτή την εξέλιξη.

Η εργασία αυτή συνεχίστηκε από τον Alan Turing, τον Gordon Welchman και από πολλούς άλλους στο Bletchley Park και οδήγησε σε συνεχείς παραβιάσεις των διαφόρων παραλλαγών της μηχανής Enigma.

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 στην μάχη του Midway.

Το Ιαπωνικό υπουργείο εξωτερικών χρησιμοποίησε ένα τοπικά αναπτυγμένο κρυπτογραφικό σύστημα, (που καλείται Purple), και διάφορες παρόμοιες μηχανές για τις συνδέσεις μερικών ιαπωνικών πρεσβειών. Μία από αυτές αποκαλέστηκε ως "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 Purple πριν καν ακόμη αρχίσει ο δεύτερος 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 10) Οι δύο αυτές κρυπτομηχανές ήταν ηλεκτρομηχανικά σχέδια παρόμοια στο πνεύμα με το Enigma, αλλά με σημαντικές βελτιώσεις.




**Εικόνα 10** : Κρυπτομηχανή SIGABA.

Κανένα δεν έγινε γνωστό ότι παραβιάστηκε κατά τη διάρκεια του πολέμου. Τα στρατεύματα στο πεδίο μάχης χρησιμοποίησαν το M-209 και τη λιγότερη ασφαλή οικογένεια κρυπτομηχανών M-94. Οι Βρετανοί πράκτορες SOE χρησιμοποίησαν αρχικά ένα τύπο κρυπτογραφίας που βασιζόταν σε ποιήματα (τα απομνημονευμένα ποιήματα ήταν τα κλειδιά).

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 πήρε ακριβώς μερικές ώρες για να την σπάσει και έτσι αναγκάστηκαν να την αλλάξουν βιαστικά. Τα μηνύματα που εστάλησαν με Lacida δεν ήταν συγκρίσιμα με αυτά της μηχανής enigma, αλλά η παρεμπόδιση θα μπορούσε να έχει σημάνει το τέλος της κρίσιμης κρυπταναλυτικής Πολωνικής προσπάθειας.

## 1.4 Τέταρτη Περίοδος 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**, που είναι αναμφισβήτητα ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας. Το 1949 δημοσίευσε την εργασία «Θεωρία επικοινωνίας των συστημάτων μυστικότητας» (Communication Theory of Secrecy Systems), στο τεχνικό περιοδικό Bell System και λίγο αργότερα στο βιβλίο του «Μαθηματική Θεωρία της Επικοινωνίας» (Mathematical Theory of Communication) μαζί με τον Warren Weaver. Εκτός από τις άλλες εργασίες του επάνω στη θεωρία δεδομένων και επικοινωνίας, καθιέρωσε μια στερεά θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση. Εκείνη την εποχή η κρυπτογραφία επίσημα εξαφανίζεται και ερευνάται μόνο από τις μυστικές υπηρεσίες κυβερνητικών επικοινωνιών όπως η NSA. Πολύ λίγες εξελίξεις δημοσιοποιήθηκαν ξανά μέχρι τα μέσα της δεκαετίας του '70.

**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 και άλλες μεγάλες οικονομικές οργανώσεις. Μετά από τις συμβουλές και την τροποποίηση από την NSA, αυτό το πρότυπο

υιοθετήθηκε και δημοσιεύθηκε ως ένα ομοσπονδιακό τυποποιημένο πρότυπο επεξεργασίας πληροφοριών το 1977 (αυτήν την περίοδο αναφέρεται σαν FIPS 46-3). Ο DES ήταν ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης που εγκρίνεται από μια εθνική υπηρεσία όπως η NSA. Η απελευθέρωση της προδιαγραφής της από την NBS υποκίνησε μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας.

ü 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 ενσωματωμένοι σε πολλά εθνικά και οργανωτικά πρότυπα.

Εντούτοις, το βασικό μέγεθος των 56-bit που χρησιμοποιούσε ο DES 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 πια αναμφίβολα επισφαλής για χρήση στα νέα σχέδια των κρυπτογραφικών συστημάτων. Επίσης μηνύματα που προστατεύονται από τα παλαιότερα κρυπτογραφικά συστήματα που χρησιμοποιούν DES και όλα τα μηνύματα που έχουν αποσταλεί από το 1976 με την χρήση DES διατρέχουν επίσης σοβαρό κίνδυνο αποκρυπτογράφησης.

Ανεξάρτητα από την έμφυτη ποιότητά του, το βασικό μέγεθος του DES (56-bit), πιθανώς ήταν πάρα πολύ μικρό ακόμη και το 1976, πράγμα που είχε επισημάνει ο Whitfield Diffie. Υπήρχε επίσης η υποψία, ότι κυβερνητικές

οργανώσεις είχαν ακόμα και τότε ικανοποιητική υπολογιστική δύναμη ώστε να σπάσουν μηνύματα που είχαν κρυπτογραφηθεί με τον DES.

## 1.5 Η εξέλιξη των πρώτων μεθόδων κρυπτογράφησης

Η κρυπτογραφία στην πράξη: Λύσεις στο πρόβλημα της ασφαλούς επικοινωνίας .Η επίτευξη ασφαλούς επικοινωνίας μεταξύ δύο ανθρώπων έχει ως βασική απαίτηση τη δυνατότητα αποστολής ενός μηνύματος (συχνά κείμενο γραμμένο σε κάποια φυσική γλώσσα) με τέτοιο τρόπο ώστε να είναι δυνατόν να διαβαστεί μόνο από τον παραλήπτη στον οποίο απευθύνεται.

Με ποιους τρόπους θα ήταν δυνατή η εκπλήρωση αυτής της απαίτησης;

- Μια πρώτη ιδέα που έρχεται κατά νου είναι να στείλουμε το μήνυμά μας με κάποιο μέσο που θα καθιστά αδύνατη την υποκλοπή του από κάποιον. Το πρόβλημα με αυτή την προσέγγιση είναι ότι μέχρι τώρα τα συμβατικά μέσα μετάδοσης μηνυμάτων (π.χ. ραδιοκύματα, οπτικές ίνες), αλλά και πιο μοντέρνα (π.χ. κβαντικά κανάλια) δεν αποκλείουν τη λήψη ενός μηνύματος από οποιονδήποτε έχει τον κατάλληλο εξοπλισμό.
- Αποδεχόμενοι το γεγονός ότι υπάρχει πάντα η δυνατότητα παρακολούθησης ενός καναλιού επικοινωνίας και υποκλοπής του μηνύματός μας οδηγούμαστε σε μια δεύτερη ιδέα που αποτελεί και το βασικό στόχο της σύγχρονης κρυπτογραφίας: εφόσον δεν είναι δυνατό να εξασφαλίσουμε ασφαλή κανάλια επικοινωνίας, ας μεταμορφώσουμε το μήνυμά μας με τέτοιο τρόπο ώστε, ακόμη και αν υποκλαπεί, να είναι «αδύνατη» η κατανόησή του από μη εξουσιοδοτημένα πρόσωπα. Τη λέξη «αδύνατη», τη βάζουμε σε εισαγωγικά, διότι, όπως θα δούμε, κανένα από τα σχήματα κρυπτογραφίας που έχουν προταθεί μέχρι τώρα (και μάλλον αυτό ισχύει και για όσα θα προταθούν και στο μέλλον) δεν απαγορεύει την αποκρυπτογράφηση του μηνύματος. Εκεί που η

κρυπτογραφία αποκτά υπόσταση και εφαρμογή είναι το ότι μπορεί να προσφέρει ισχυρές ενδείξεις ή εγγυήσεις ότι ο επίδοξος υποκλοπέας του μηνύματος θα συναντήσει τόσο μεγάλες δυσκολίες στην αποκρυπτογράφηση, που, στην πράξη, η αποκρυπτογράφηση μπορεί να θεωρηθεί αδύνατη.

**Με βάση τα παραπάνω, ένα κρυπτογραφικό σχήμα μπορεί να παρασταθεί ως εξής:** υπάρχουν δύο πρόσωπα, ο Α και ο Β. Ο Α επιθυμεί να στείλει ένα μήνυμα Μ μέσα από ένα μη ασφαλές κανάλι (π.χ. μια δικτυακή σύνδεση μεταξύ υπολογιστών). Ο Α, γνωρίζοντας ότι το κανάλι δεν παρέχει καμία ασφάλεια, μετασχηματίζει το μήνυμά του με κάποια διαδικασία Ε (μέθοδο κρυπτογράφησης), παράγοντας το μετασχηματισμένο μήνυμα Ε(Μ) το οποίο και αποστέλλει στον Β μέσα από το κανάλι επικοινωνίας. Το μήνυμα Μ και Ε(Μ), αν και το δεύτερο δεν είναι παρά ένας μετασχηματισμός του πρώτου, θα φαίνονται ότι δεν έχουν καμία ομοιότητα. Το επιθυμητό βέβαια είναι για έναν υποκλοπέα, έστω Γ, που θα αποκτήσει το κωδικοποιημένο μήνυμα Ε(Μ), η κατανόηση του μηνύματος (δηλαδή η ανάκτηση και το διάβασμα του Μ) να είναι πρακτικά αδύνατη (σύμφωνα με τις εγγυήσεις της κρυπτογραφίας!).

Όμως κάτι φαίνεται να μην είναι σωστό στο πιο πάνω βασικό σχήμα. Αφού είναι δύσκολο για τον υποκλοπέα Γ να αποκωδικοποιήσει το μήνυμα Ε(Μ), δεν θα είναι εξίσου δύσκολο και για τον νόμιμο παραλήπτη;

Πώς μπορούμε όμως να εξασφαλίζουμε τους «φαινομενικά» αντικρουόμενους στόχους, δηλαδή το μήνυμα να διαβάζεται από τον Β αλλά όχι από τον Γ; Η απάντηση σε αυτό είναι ότι ο Β είναι εφοδιασμένος από πριν με ένα κλειδί κ, το οποίο καθιστά εύκολη την επαναφορά του Ε(Μ) στο Μ με μια αντίστροφη απεικόνιση αποκωδικοποίησης Α(Ε(Μ), κ)=Μ.

### 1.5.1 Ένα απλό κρυπτογραφικό σχήμα – Το «σχήμα του Καίσαρα».

Η κρυπτογράφηση δεν είναι νέα υπόθεση. Ακόμη και στην αρχαιότητα χρησιμοποιούνταν διάφορες μέθοδοι κρυπτογράφησης, με χαρακτηριστικότερη αυτή του Ιουλίου Καίσαρα, ο οποίος επινόησε έναν απλό αλγόριθμο (το λεγόμενο «σχήμα του Καίσαρα») για να επικοινωνεί με τους επιτελείς του, με μηνύματα που δε θα ήταν δυνατό να τα διαβάσουν οι εχθροί του.

Σύμφωνα με το σχήμα αυτό, καθορίζεται ένας ακέραιος αριθμός κ από το 1 μέχρι τον αριθμό των γραμμάτων του αλφάβητου της γλώσσας του κειμένου, μειωμένο κατά ένα, και κάθε γράμμα του κειμένου προς κωδικοποίηση αντιστοιχίζεται στο γράμμα που βρίσκεται μετά από κ θέσεις στη λίστα των γραμμάτων. Εάν εξαντληθούν τα γράμματα πριν να έχουμε μετρήσει κ θέσεις, απλώς συνεχίζουμε τη μέτρηση από το πρώτο γράμμα. Στη συνέχεια το μήνυμά μας ξαναγράφεται χρησιμοποιώντας την αντιστοιχία των γραμμάτων που μόλις κατασκευάσαμε.

**Ας δούμε ένα συγκεκριμένο παράδειγμα.** Στην ελληνική γλώσσα έχουμε 24 γράμματα, άρα η παράμετρος κ θα πρέπει να βρίσκεται μεταξύ του 1 και του 24- 1= 23. Έστω ότι επιλέγουμε κ= 4. Τότε η αντιστοιχία των γραμμάτων του Ελληνικού αλφάβητου θα είναι αυτή που φαίνεται στην εικόνα 11, όπου στην πρώτη γραμμή είναι το αλφάβητο, ενώ στην δεύτερη γραμμή βρίσκεται η αντιστοιχία των γραμμάτων. Για παράδειγμα, το γράμμα α αντιστοιχίζεται στο ε, ενώ το φ στο γράμμα α (προσέξτε πως για το φ «αναδιπλώθηκε» η μέτρηση).

| α | β | γ | δ | ε | ζ | η | θ | ι | κ | λ | μ | ν | ξ | ο | π | ρ | σ | τ | υ | φ | χ | ψ | ω |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ε | ζ | η | θ | ι | κ | λ | μ | ν | ξ | ο | π | ρ | σ | τ | υ | φ | χ | ψ | ω | α | β | γ | δ |

**Εικόνα 11** : Αντιστοιχίες μεταξύ γραμμάτων του Ελληνικού αλφάβητου.

Ας δούμε όμως πώς εφαρμόζεται το σχήμα αυτό. Ας υποθέσουμε ότι θέλουμε να στείλουμε το παρακάτω μήνυμα Μ:

Μ = Η ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΕΙΝΑΙ ΕΤΟΙΜΗ

Ε(Μ)= Λ ΥΨΩΒΝΕΞΛ ΙΦΗΕΧΝΕ ΙΝΡΕΝ ΙΨΤΝΠΛ

Όπως βλέπουμε, το κωδικοποιημένο μήνυμα δεν είναι κατανοητό από κάποιον που δεν γνωρίζει τον τρόπο κωδικοποίησης. Ο παραλήπτης τώρα του μηνύματος, προκειμένου να τα διαβάσει, ξέροντας φυσικά το κ= 4, που αποτελεί και το κλειδί, εφαρμόζει την αντίστροφη απεικόνιση Α(Ε(Μ),4) π.χ. το πρώτο γράμμα, το λ ,γίνεται η, το υ γίνεται π κ.λ.π ) λαμβάνοντας το αρχικό μήνυμα. Όμως τα πράγματα δεν είναι τόσο ρόδινα!

Το παραπάνω σχήμα, αν και φαίνεται ικανοποιητικό, καθώς επιτέλεσε το σκοπό του μεταμορφώνοντας το αρχικό μήνυμα έτσι ώστε να φαίνεται ακατανόητο, εν τούτοις έχει τόσο πολλές αδυναμίες που το «σπάσιμό» του ακόμα και από έναν αρχάριο κρυπταναλυτή να είναι ιδιαίτερα εύκολο!

**Κρυπτανάλυση του «σχήματος του Καίσαρα».**

Στην ενότητα αυτή θα προσπαθήσουμε ως επίδοξοι κρυπταναλυτές να επιτεθούμε στο «σχήμα του Καίσαρα», με σκοπό μέσα από την ανακάλυψη των αδυναμιών του να διαφανούν στο τέλος τα χαρακτηριστικά που είναι επιθυμητό να έχει ένα καλό σχήμα κρυπτογραφίας.

Η μεγαλύτερη αδυναμία του σχήματος αυτού, την οποία οι σύγχρονες μέθοδοι κρυπτογράφησης κάνουν το παν για να αποφύγουν, είναι ο περιορισμένος αριθμός πιθανών κλειδιών.

Εάν γνωρίζουμε ότι ένα μήνυμα είναι γραμμένο στην Ελληνική γλώσσα και είναι κρυπτογραφημένο με το σχήμα του Καίσαρα, τότε αρκεί να δοκιμάσουμε 23 πιθανές μεταθέσεις των γραμμάτων (23 κλειδιά) κοιτώντας εάν το αποκωδικοποιημένο κείμενο έχει νόημα στην Ελληνική γλώσσα.

Για κάποιο από αυτά τα 23 κλειδιά είναι σίγουρο ότι θα λάβουμε το μήνυμα, άρα 23 προσπάθειες, στη χειρότερη περίπτωση, αρκούν για να σπάσουμε το σχήμα αυτό. Και σα να μην έφτανε η αδυναμία του μικρού αριθμού δυνατών κλειδιών, για κάθε κλειδί ο έλεγχος του εάν το κλειδί αυτό είναι το σωστό είναι γρήγορος ακόμα και με το «χέρι» (πόσο μάλλον με τη χρήση υπολογιστή – εμείς απλώς θα κοιτάμε την οθόνη μέχρι να σχηματιστεί ένα μήνυμα που να έχει νόημα), καθώς ένα μήνυμα αποτελείται συνήθως από ένα μικρό αριθμό λέξεων!

Ο τρόπος αυτός της κρυπτανάλυσης καλείται ανάλυση με χρήση «**ωμής βίας»**, καθώς απλώς δοκιμάζεται κάθε πιθανό κλειδί στο κωδικοποιημένο μήνυμα, μέχρι να ανακτηθεί το αρχικό μήνυμα.

Στο σημείο αυτό κάποιος μπορεί να υπερεκτιμήσει την ισχύ της «ωμής βίας» από την επιτυχία της στο σχήμα του Καίσαρα. Με τη χρήση ηλεκτρονικού υπολογιστή θα περιμέναμε μηδαμινούς χρόνους κρυπτανάλυσης και άλλων κρυπτογραφικών σχημάτων, όμως τα περισσότερα από τα μοντέρνα και συχνά χρησιμοποιούμενα σχήματα κάνουν την προσέγγιση «ωμής βίας» πρακτικά άχρηστη, καθώς ο αριθμός των πιθανών κλειδιών με τα οποία μπορεί να έχει κωδικοποιηθεί ένα μήνυμα ανέρχεται σε μεγέθη της τάξης πολλών δισεκατομμυρίων! Και εδώ δύσκολα θα είναι σε μεγάλη χρησιμότητα, ακόμα και το ταχύτερο δίκτυο παράλληλων υπερυπολογιστών όλου του κόσμου.

### 1.5.2 Μεγαλώνοντας το χώρο των πιθανών κλειδιών: Γενικευμένα σχήματα αντικατάστασης χαρακτήρων.

Θα εξετάσουμε στη συνέχεια έναν τρόπο για να αντιμετωπίσουμε το βασικό πρόβλημα του σχήματος του καίσαρα: τον μικρό αριθμό πιθανών κλειδιών. Αφού το πρόβλημά μας είναι ότι όλοι οι χαρακτήρες απεικονίζονται ομοιόμορφα προς τα δεξιά κατά 23 δυνατούς τρόπους, γιατί να μην

χρησιμοποιήσουμε μια «άτακτη» απεικόνιση κάθε χαρακτήρα, είτε προς τα δεξιά είτε προς τα αριστερά και σε οποιαδήποτε θέση (αρκεί φυσικά να μην απεικονίζονται δυο χαρακτήρες στον ίδιο χαρακτήρα). Μιλάμε πλέον για μια μετάθεση των γραμμάτων του αλφάβητου.

Για παράδειγμα, μια μετάθεση των γραμμάτων Α, Β, Γ, Δ και Ε είναι η εξής: Ε, Α, Δ, Γ και Β. αυτό μας δίνει την αντιστοιχία Α **à** Ε, Β **à** Α, Γ **à** Δ, Δ **à** Γ, Ε **à** Β. παρατηρούμε ότι δεν υπάρχει καμία κανονικότητα και τάξη, όπως αυτή που υπήρχε στο σχήμα του Καίσαρα, αλλά μια αταξία που δίνει μεγάλο αριθμό πιθανών αντιστοιχιών.

**Ποιος είναι όμως αυτός ο αριθμός; Ας εξετάσουμε τον αριθμό αυτό για τα 24 γράμματα του ελληνικού αλφάβητου.**

Το πρώτο γράμμα, το Α, μπορεί να αντιστοιχιθεί σε 24 πιθανές θέσεις (μαζί με τον εαυτό του). Για το Β απομένουν, συνεπώς, 23 πιθανές θέσεις, καθώς δεν θα πρέπει να αντιστοιχιθεί στη θέση που έχει αντιστοιχιθεί το Α. Το Γ μπορεί με τη σειρά του να αντιστοιχιθεί σε 22 πιθανές θέσεις, καθώς δεν θα πρέπει να αντιστοιχιθεί στις δύο θέσεις στις οποίες αντιστοιχίζονται το Α και το Β. Συνοψίζοντας, με αυτό τον τρόπο για όλα τα γράμματα του αλφάβητου καταλήγουμε ότι για το Ψ υπάρχουν 2 πιθανές θέσεις και για το Ω απομένει μια θέση, καθώς στις υπόλοιπες 23 έχουν ήδη αντιστοιχιθεί γράμματα. Συνεπώς, υπάρχουν 24*23*22*21*20*19….*3*2*1 δυνατές μεταθέσεις των 24 γραμμάτων ή, με τον συνήθη συμβολισμό, 24! μεταθέσεις.

Αξίζει να παρατηρήσουμε ότι ο αριθμός αυτός που είναι ίσος με τον αριθμό των πιθανών κλειδιών στο γενικευμένο σχήμα αντικατάστασης γραμμάτων, είναι μεγαλύτερος από το 623.000.000.000.000.000.000.000!

Είναι πλέον φανερό ότι ο αριθμός των δυνατών κλειδιών στο σχήμα του Καίσαρα, το 23, ωχριά μπροστά στον αριθμό κλειδιών του νέου μας σχήματος!

Συμπερασματικά, ο επίδοξος κρυπταναλυτής καλείται να ανακαλύψει το σωστό κλειδί μέσα από πολλά εκατομμύρια πιθανά κλειδιά και όχι μέσα από μόνο 23. Κατά συνέπεια η απλή επίθεση «ωμής βίας» δεν είναι πια εύκολη ακόμη και για έναν ηλεκτρονικό υπολογιστή.

### 1.5.3 Το μεγάλο σύνολο των πιθανών κλειδιών δεν είναι πανάκεια.

Βρήκαμε λοιπόν ένα πανίσχυρο σχήμα κρυπτογράφησης. Αν και η σχεδίαση του γενικευμένου σχήματος που στηρίζεται σε τυχαίες μεταθέσεις των γραμμάτων του αλφάβητου παρέχει ένα μεγάλο αριθμό πιθανών κλειδιών που φαίνεται να δυσχεραίνει την κρυπτανάλυσή του, εντούτοις αυτό δε σημαίνει ότι έχει επιτευχθεί η επιθυμητή ασφάλεια. Το γεγονός ότι δυσχεραίνεται η προφανής προσπάθεια κρυπτανάλυσης, η επίθεση ωμής βίας, δε σημαίνει και ότι δεν μπορεί να υπάρξει κάποια άλλη πιο έξυπνη και πιο γρήγορη επίθεση. Αυτή η γενική παρατήρηση ισχύει για κάθε κρυπτογραφικό σχήμα που μπορεί να συναντήσουμε.

Στη συνέχεια θα δούμε μερικά χαρακτηριστικά του γενικευμένου σχήματος αντικατάστασης και θα ανακαλύψουμε τρόπους για μια επιτυχημένη κρυπτανάλυσή του.

Έστω ότι για τις ανάγκες μας χρησιμοποιούμε το πιο κάτω κλειδί:

| Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ω | Α | Ο | Η | Π | Ι | Ε | Β | Γ | Δ | Ζ | Θ | Κ | Λ | Μ | Ν | Ξ | Ρ | Υ | Τ | Σ | Ψ | Χ | Φ |

Σύμφωνα με το κλειδί αυτό το μήνυμα :

Η ΠΑΡΟΥΣΙΑΣΗ ΤΗΣ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ ΑΝΑΒΛΗΘΗΚΕ

Κρυπτογραφείται ως εξής :

Ε ΝΩΞΜΤΡΓΩΡΕ ΥΕΡ ΝΥΤΨΓΩΔΕΡ ΠΞΟΩΡΓΩΡ ΩΚΩΑΖΕΒΕΔΠ

Προφανώς, ο νόμιμος παραλήπτης μπορεί εύκολα να αποκρυπτογραφήσει το μήνυμα με χρήση του πίνακα που περιγράφει τη μετάθεση (η μετάθεση είναι το μυστικό διαμοιραζόμενο κλειδί).

Όμως τι μπορεί να κάνει ένας κρυπταναλυτής αντίπαλος; Μπορεί φυσικά να δοκιμάσει όλα τα πιθανά κλειδιά, αλλά όπως αναφέραμε, αυτό δεν είναι και τόσο καλή λύση λόγω του μεγάλου χώρου των πιθανών κλειδιών.

**Ας παρατηρήσουμε λίγο την κρυπτογραφημένη μορφή του μηνύματός μας.** Είναι προφανές πως είναι ακατανόητη και δεν φαίνεται να λέει και πολλά για το αρχικό κείμενο, από το οποίο προήλθε. Όμως, υπάρχει κάτι που προδίδεται λόγω της φύσης του σχήματος αντικατάστασης.

Ας δούμε στο αρχικό κείμενο πόσες φορές εμφανίζεται το γράμμα Α, εμφανίζεται 7 φορές. Το γράμμα Σ εμφανίζεται 6 φορές. Πόσες φορές τώρα εμφανίζεται στο κρυπτογραφημένο μήνυμα το γράμμα Ω, στο οποίο αντιστοιχίζεται το Α; Φυσικά εμφανίζεται 7 φορές, όπως και το Α στο αρχικό μήνυμα! Επίσης, ο χαρακτήρας Ρ στον οποίο αντιστοιχίζεται ο χαρακτήρας Σ εμφανίζεται και αυτός 6 φορές, όσες και ο Σ στο αρχικό μήνυμα!

Λίγη σκέψη πάνω στην φύση του σχήματος κρυπτογράφησης με αντικατάσταση μας πείθει ότι, μέσα από τη διαδικασία μετασχηματισμού του αρχικού μηνύματος, καταφέρνει να περνά εντελώς αμετάβλητη μια πληροφορία που αφορά στο αρχικό μήνυμα, η συχνότητα εμφάνισης των χαρακτήρων του μηνύματος.

Αυτή η παρατήρηση είναι πολύ σημαντική: εκεί που βρεθήκαμε χαμένοι σε ένα τεράστιο αριθμό πιθανών κλειδιών προς δοκιμή, φαίνεται ότι είναι στη διάθεσή μας και κάποια πληροφορία για το αρχικό μήνυμα που δεν έχουμε σκεφτεί να την εκμεταλλευτούμε.

Βέβαια όταν στο κρυπτογραφημένο μήνυμα βρίσκουμε ότι ο χαρακτήρας Ω εμφανίζεται 7 φορές, δεν είναι δυνατό να γνωρίζουμε σε ποιο χαρακτήρα αντιστοιχεί στο αρχικό κείμενο. Γνωρίζουμε μόνο ότι σε όποιο χαρακτήρα και να αντιστοιχεί, αυτός θα εμφανίζεται ακριβώς 7 φορές στο αρχικό μήνυμα.

Άρα**,** θα αναρωτηθεί κανείς, πως θα μπορούσε να χρησιμεύσει η ανακάλυψη που κάναμε σχετικά με την πληροφορία της εμφάνισης χαρακτήρων στο αρχικό μήνυμα και στο κρυπτογραφημένο μήνυμα;
Τι θα λέγατε εάν επιπλέον κάποιος σας έλεγε ότι σε ένα μεγάλο ελληνικό κείμενο, ο χαρακτήρας Α έχει τη μεγαλύτερη συχνότητα εμφάνισης;

Ίσως τώρα αρχίζει να διαφαίνεται η αδυναμία του σχήματος με αντικατάσταση και ο τρόπος επίθεσης που παρακάμπτει το μεγάλο πλήθος των πιθανών κλειδιών!

### 1.5.4 Κρυπταναλύοντας το γενικευμένο σχήμα αντικατάστασης:

Στη δεκαετία του 60 ο David Huffman παρουσίασε μια μέθοδο κωδικοποίησης δεδομένων η οποία μπορεί να ελαχιστοποιήσει το μέσο αριθμό των bits που απαιτούνται για να σταλεί ένα μήνυμα γραμμένο σε κάποια φυσική γλώσσα. Έτσι οι συχνότητες εμφάνισης των χαρακτήρων του αλφάβητου της γλώσσας είναι αρκετά διαφοροποιημένες.

Για παράδειγμα**,** στο πρώτο ραβδόγραμμα (εικόνα 12) φαίνεται το ποσοστό εμφάνισης των γραμμάτων του Ελληνικού αλφάβητου σε τρία διαφορετικά κείμενα, το πρώτο 70.000 χαρακτήρων περίπου και τα άλλα δύο των 8.000 χαρακτήρων. Παρατηρούμε ότι οι συχνότητες εμφάνισης δεν είναι και πολύ διαφορετικές στα τρία κείμενα. Αυτό δεν είναι καθόλου τυχαίο.

Η συχνότητα εμφάνισης των χαρακτήρων, σε κείμενα μιας γλώσσας, είναι κατά προσέγγιση η ίδια για αρκετά μεγάλα κείμενα (ώστε να εξαλειφθούν μεγάλες στατιστικές αποκλίσεις): Στα Ελληνικά κείμενα,

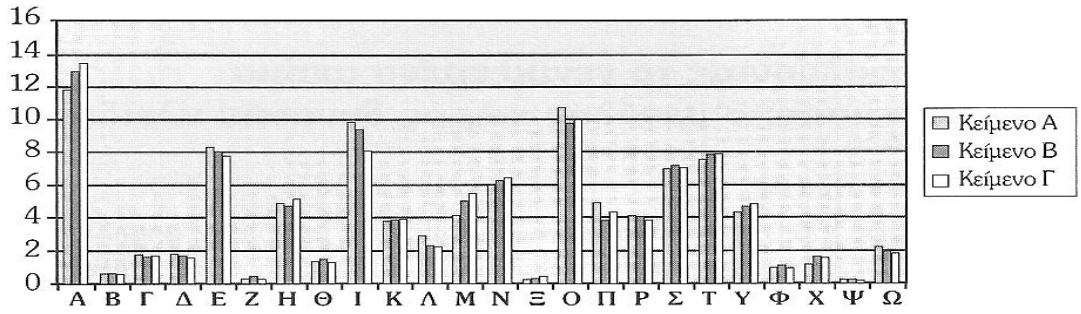
¶ το γράμμα Α αποτελεί το 12-13% των εμφανίσεων χαρακτήρων,

¶ ενώ το Ε το 8% περίπου.

Αν και η συχνότητα εμφάνισης εξαρτάται και από το είδος των κειμένων (π.χ. ενημερωτικά, επιστημονικά κ.λπ.) αλλά και από τις ιδιαιτερότητες του γράφοντα, στην πραγματικότητα αυτή η εξάρτηση υποσκελίζεται από την ισχυρότερη εξάρτηση από τους κανόνες γραμματικής και σύνταξης της γλώσσας. Συνεπώς η συχνότητα εμφάνισης μπορεί να θεωρηθεί ως αμετάβλητο στοιχείο της γλώσσας.

Αφήνοντας την ιδέα του Huffman, πριν δούμε πως μπορούμε να χρησιμοποιήσουμε τον πλεονασμό για την κρυπτανάλυση των γενικευμένων σχημάτων κρυπτογράφησης, θα αρκεστούμε να αναφέρουμε ότι :

Στην κωδικοποίηση Huffman πετυχαίνουμε αποδοτική συμπίεση κειμένων, διότι σε κάθε χαρακτήρα ανατίθεται ένας αριθμός από bits αντίστροφα ανάλογος προς την συχνότητα εμφάνισής του στα κείμενα της γλώσσας του αλφάβητου. Άρα : όσο λιγότερο συχνά εμφανίζεται ένας χαρακτήρας τόσο περισσότερα bits περιέχει ο κωδικός που του ανατίθεται.



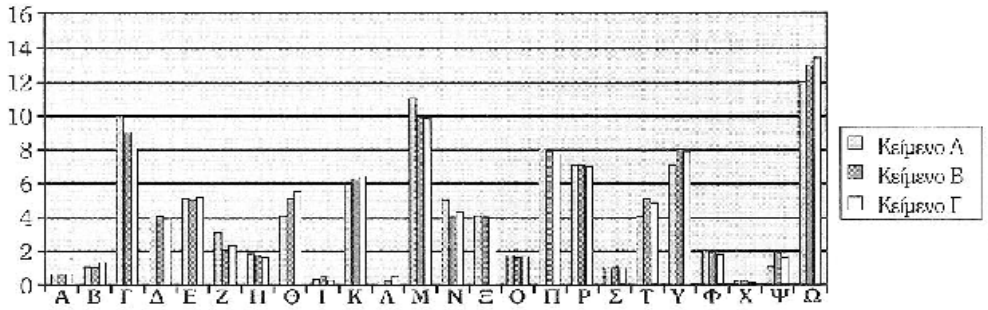

**Εικόνα 12:** ο πλεονασμός στην Ελληνική γλώσσα.

Ας επιστρέψουμε στη μετάθεση- κλειδί που είχαμε χρησιμοποιήσει στο παράδειγμα της προηγούμενης ενότητας, η οποία φαίνεται πιο κάτω:

| Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ω | Α | Ο | Η | Π | Ι | Ε | Β | Γ | Δ | Ζ | Θ | Κ | Λ | Μ | Ν | Ξ | Ρ | Υ | Τ | Σ | Ψ | Χ | Φ |

Με βάση αυτή τη μετάθεση, τα τρία κείμενα για τα οποία δείξαμε τη συχνότητα εμφάνισης χαρακτήρων προηγουμένως θα μας δείξουν την εξής συχνότητα εμφανίσεων που φαίνεται στο παρακάτω ραβδόγραμμα. (εικόνα 13)

**Συχνότητες εμφάνισης χαρακτήρων στα κρυπτογραφημένα κείμενα**




**Εικόνα 13:** Συχνότητες εμφάνισης χαρακτήρων στα κρυπτογραφημένα κείμενα.

**Τι παρατηρείται τώρα**; Το καινούριο ραβδόγραμμα, που αφορά πλέον τα κρυπτογραφημένα κείμενα, δεν είναι τίποτα παραπάνω από μία μετάθεση των ράβδων του αρχικού ραβδογράμματος που αντιστοιχεί ακριβώς στη μετάθεση- κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση των κειμένων!

Πώς όμως μπορεί να μας χρησιμεύσει το αρχικό ραβδόγραμμα εμφανίσεων χαρακτήρων, που βέβαια υποθέτουμε βάσιμα πως οφείλει να το ακολουθεί κάθε κείμενο γραμμένο στην Ελληνική γλώσσα; Ας υποθέσουμε ότι το ραβδόγραμμα είναι αυτό που αποτελείται από τις πιο δεξιές μπάρες στο πρώτο διάγραμμα, καθώς αυτό είναι πιο αξιόπιστο στατιστικά αντιστοιχώντας σε κείμενο που περιέχει πολλές χιλιάδες χαρακτήρων.

Έστω τώρα ότι έχουμε στα χέρια μας την κρυπτογραφημένη μορφή του κειμένου Γ, για την οποία υποθέτουμε πως έχει κρυπτογραφηθεί με βάση το γενικευμένο σχήμα αντικατάστασης και με ένα κλειδί που αντιστοιχεί σε μία μετάθεση των γραμμάτων του Ελληνικού αλφαβήτου.

Το πρόβλημα είναι φυσικά να βρεθεί αυτή η μετάθεση, ώστε να αποκρυπτογραφηθεί το κείμενο Γ.

**!** Το πρώτο βήμα είναι να κατασκευαστεί ένα ραβδόγραμμα συχνοτήτων εμφάνισης χαρακτήρων στο κρυπτογραφημένο κείμενο. Έστω ότι το ραβδόγραμμα αυτό αποτελείται από τις μεσαίες μπάρες που φαίνονται στο δεύτερο διάγραμμα.

**!** Το επόμενο βήμα μας είναι η σύγκριση του καθολικού ραβδογράμματος, που υποθέτουμε πάντα ότι κατά μέσο όρο ακολουθεί κάθε κείμενο στην Ελληνική γλώσσα, με το ραβδόγραμμα που πήραμε από το κρυπτογραφημένο κείμενο.

Στο παράδειγμά μας θα πρέπει να συγκρίνουμε το ραβδόγραμμα με τις πιο δεξιές μπάρες στο πρώτο διάγραμμα με το ραβδόγραμμα με τις μεσαίες μπάρες στο δεύτερο διάγραμμα. Η σύγκριση αυτή μπορεί να γίνει είτε οπτικά είτε με τη βοήθεια ηλεκτρονικού υπολογιστή διατάσσοντας, για παράδειγμα, τις μπάρες κατά αύξουσα σειρά με βάση το ύψος τους και αντιστοιχίζοντας μεταξύ τους τα αντίστοιχα γράμματα. Συγκεκριμένα, παρατηρούμε αμέσως ότι:

**ð** Ξεχωρίζουν στο δεύτερο διάγραμμα τρεις κορυφές στα γράμματα Ω, Μ και Γ, διατεταγμένα με βάση τη συχνότητα εμφάνισης. Οι κορυφές αυτές υπάρχουν και στο καθολικό ραβδόγραμμα στα γράμματα Α, Ο και Ι.

Άρα είναι λογικό να υποθέσουμε ότι στο κλειδί που χρησιμοποιήθηκε υπήρχαν οι αντιστοιχίες Α **à** Ω, Ο **à** Μ και Ι **à** Γ.

Βλέποντας το κλειδί, διαπιστώνουμε πράγματι ότι η υπόθεσή μας αυτή ήταν σωστή!

Ακόμα και οι τρεις αυτές αντιστοιχίες από μόνες τους μπορούν να μας αποκαλύψουν αρκετά για το αρχικό κείμενο.

ð Μπορούμε να συνεχίσουμε κατασκευάζοντας ανάλογες υποθέσεις και για τα υπόλοιπα γράμματα, τις οποίες και ελέγχουμε αποκρυπτογραφώντας όλο και μεγαλύτερο μέρος του κειμένου που έχουμε στα χέρια μας και βλέποντας εάν βγαίνει νόημα διαφορετικά αλλάζουμε ανάλογα τις αρχικές μας υποθέσεις.

Από την παραπάνω κρυπτανάλυση του γενικευμένου σχήματος αντικατάστασης διαπιστώνουμε δυο πράγματα:

1. Η ύπαρξη τεράστιου αριθμού πιθανών κλειδιών δεν είναι απαραίτητα αρκετή για να μας εξασφαλίσει ότι το σχήμα μας είναι ανθεκτικό.
2. Θα πρέπει πάντα να έχουμε κατά νου ότι μπορεί να υπάρχουν και άλλες κρυπταναλυτικές επιθέσεις σε ένα σχήμα πέρα από την προφανή επίθεση της «ωμής βίας».

Όμως, η πορεία της κρυπτογραφίας είναι ένας διαρκής αγώνας κατασκευής κρυπτογραφικών σχημάτων που υποκύπτουν σε επιθέσεις και μετά υπόκεινται σε βελτιώσεις για να δεχτούν κάποιες άλλες επιθέσεις κ.ο.κ. Συνεπώς, τώρα θα πρέπει να δούμε πώς θα γιατρέψουμε το γενικευμένο σχήμα αντικατάστασης ώστε να αντιστέκεται στην επίθεση που μόλις περιγράψαμε.

Ένας τρόπος για να το επιτύχουμε αυτό, που οδηγεί στους πολυαλφαβητικούς κρυπταλγόριθμους, είναι κάθε γράμμα ενός αλφάβητου να αντιστοιχίζεται σε πολλούς χαρακτήρες με βάση ένα συγκεκριμένο κανόνα.

Έτσι το γράμμα Α, για παράδειγμα, θα αντιστοιχίζεται στο ίδιο κείμενο στο γράμμα Ω (όπως στο παράδειγμά μας) την πρώτη φορά που το συναντούμε, στο γράμμα Γ τη δεύτερη φορά, στο γράμμα Ζ την επόμενη κ.ο.κ. έτσι η αρχική συχνότητα εμφάνισης του Α διασπάται σε πολλά μικρότερα κομμάτια!

## 1.5.5. Πολυαλφαβητικά σχήματα αντικατάστασης.

Τα σχήματα αντικατάστασης που έχουμε μελετήσει ως τώρα βασίζονταν στην απεικόνιση κάθε χαρακτήρα ενός αλφάβητου σε κάποιον άλλο χαρακτήρα. Η απεικόνιση αυτή όμως παρέμενε η ίδια καθ' όλη τη διάρκεια της κωδικοποίησης ενός μηνύματος.

Το γεγονός αυτό, όπως είδαμε, δημιουργούσε μια βασική αδυναμία στα σχήματα αυτά: στο κωδικοποιημένο μήνυμα περνούσε μια ιδιότητα που αφορούσε στο αρχικό μήνυμα, η συχνότητα εμφάνισης των χαρακτήρων του.

Μια λύση θα ήταν κάθε, γράμμα του αλφάβητου να μην απεικονίζεται κάθε φορά στο ίδιο γράμμα αλλά να υπάρχουν περισσότερες επιλογές για το ποιο γράμμα θα αντικαταστήσει. Τα σχήματα που προσφέρουν τη λύση αυτή καλούνται **πολυαλφαβητικά σχήματα αντικατάστασης** (polyalphabetic substitution ciphers).

Παράδειγμα ενός τέτοιου σχήματος είναι **το σχήμα vigenere**, που προτάθηκε από τον Blaise Vigenere από την αυλή του βασιλιά Ερρίκου του Γ΄της Γαλλίας. Σύμφωνα με αυτό, αρχικά δίνεται μια τυχαία συμβολοσειρά ή ακόμα και μια λέξη με γράμματα του αλφάβητου, έστω η λέξη ΑΥΡΙΟ. Τότε για να κωδικοποιήσουμε ένα μήνυμα, π.χ. ΤΑ ΣΧΕΔΙΑ ΑΛΛΑΞΑΝ, κάνουμε τα εξής:

- αντιστοιχίζουμε στο πρώτο γράμμα του μηνύματος το γράμμα που βρίσκεται τόσες θέσεις δεξιά στο αλφάβητο όσες μας λέει το πρώτο γράμμα της λέξης που δόθηκε.
- Εάν μετρώντας προς τα δεξιά προσπεράσουμε το τελευταίο γράμμα του αλφάβητου, τότε συνεχίζουμε τη μέτρηση από το πρώτο γράμμα.

Στο παράδειγμά μας:

- Το πρώτο γράμμα της λέξης που δόθηκε είναι το Α, που έχει τη θέση 1 στο αλφάβητο. Συνεπώς, το πρώτο γράμμα του μηνύματός μας, το Τ, θα το αντιστοιχίσουμε στο γράμμα που βρίσκεται μια θέση δεξιά του στο αλφάβητο, δηλαδή στο γράμμα Υ, που έχει θέση 20 στο αλφάβητο.
- Συνεπώς, το δεύτερο γράμμα του μηνύματός μας, το Α, αντιστοιχίζεται στο γράμμα που βρίσκεται 20 θέσεις δεξιά του στο αλφάβητο, δηλαδή στο Φ.
- το γράμμα Σ τώρα (ας αγνοήσουμε τα κενά μεταξύ των λέξεων) θα αντιστοιχιστεί στο γράμμα που βρίσκεται 17 θέσεις προς τα δεξιά του, καθώς το τρίτο γράμμα της λέξης που δόθηκε είναι το Ρ. Μετρώντας από την αρχή του αλφάβητου, καθώς τα γράμματα που βρίσκονται δεξιά από το Σ είναι λιγότερα από 17, αντιστοιχίζουμε το Σ στο γράμμα Λ.
- εάν στην πορεία εξαντληθούν τα γράμματα της λέξης που δόθηκε, τότε συνεχίζουμε πάλι με το πρώτο της γράμμα κ.ο.κ.

Τελικά, στο παράδειγμά μας, φτάνουμε στο εξής κωδικοποιημένο κείμενο:

ΥΦ ΛΗΥΕΕΣ ΚΒΜΦΗΚΔ.

Φυσικά, η αποκρυπτογράφηση μπορεί να γίνει με γνώση της αρχικής λέξης εκτελώντας τον αντίστροφο μετασχηματισμό, πηγαίνοντας αριστερά από τον τρέχοντα χαρακτήρα του κρυπτογραφημένου μηνύματος.

Παρατηρούμε αμέσως δυο πράγματα:

- δύο διαφορετικοί χαρακτήρες (Δ και Ι στο παράδειγμά μας) μπορεί ν απεικονίζονται στον ίδιο χαρακτήρα (τον Ε για παράδειγμα).
- Επίσης, που είναι και το πιο σημαντικό, ένα γράμμα του αρχικού μηνύματος μπορεί να απεικονίζεται σε πολλούς διαφορετικούς χαρακτήρες.

Στο παράδειγμά μας :

- το Α απεικονίζεται διαδοχικά στους χαρακτήρες Φ, Σ, Κ, ξανά Φ και Κ.
- Επιπλέον, η πληροφορία σχετικά με τον αριθμό εμφανίσεων του Α (που είναι 5 στο αρχικό κείμενο) δεν μεταφέρεται άμεσα στο κρυπτογραφημένο μήνυμα, όπως συνέβαινε με τα σχήματα αντικατάστασης.
- Είναι σαν να χρησιμοποιήθηκαν 5 διαφορετικά σχήματα αντικατάστασης μαζί.

Με αυτό τον τρόπο τα πολυαλφαβητικά σχήματα φαίνεται ότι αντιμετωπίζουν με επιτυχία το πρόβλημα του πλεονασμού των φυσικών γλωσσών. Αυτό επιτυγχάνεται με το να παρέχουν περισσότερες από μια απεικονίσεις που μπορεί να χρησιμοποιηθούν για την αντικατάσταση ενός χαρακτήρα στο αρχικό μήνυμα.

Στο σημείο αυτό δικαίως κάποιος θα αναρωτηθεί, εάν τελικά ανακαλύψαμε ένα πραγματικά ανθεκτικό σχήμα κρυπτογράφησης. Φαίνεται ότι τα πολυαλφαβητικά σχήματα εξαλείφουν κάθε συσχέτιση μεταξύ του αρχικού και του κρυπτογραφημένου κειμένου. Ή μήπως όχι;

Για να δούμε λίγο πιο προσεκτικά τι συμβαίνει με τα σχήματα αυτά.

Από τον τρόπο απεικόνισης των χαρακτήρων του αρχικού κειμένου με βάση μια δοσμένη λέξη, συμπεραίνουμε ότι : εάν δύο ίδια τμήματα (π.χ. λέξεις) του αρχικού κειμένου τύχει να έχουν κωδικοποιηθεί με το ίδιο μέρος της λέξης, τότε τα τμήματα αυτά θα μετασχηματιστούν στην ίδια ακολουθία χαρακτήρων.

Άρα, εάν μέσα στο κωδικοποιημένο κείμενο ανακαλύψουμε δύο ίδια τμήματα είναι αρκετά πιθανόν τα τμήματα αυτά να έχουν προέλθει από δύο ίδια τμήματα του αρχικού κειμένου, τα οποία έτυχε να συναντήσουν το ίδιο μέρος της δοσμένης λέξης.

Εάν έχει συμβεί κάτι τέτοιο, που είναι αρκετά πιθανό να συμβεί στην κωδικοποίηση ενός μεγάλου κειμένου, τότε ο αριθμός των χαρακτήρων ανάμεσα στα δυο τμήματα θα πρέπει να είναι ένα ακέραιο πολλαπλάσιο (π.χ. διπλάσιο, τριπλάσιο κ.λπ.) του μήκους της δοσμένης λέξης.

Οπότε, εάν μπορέσουμε να ανακαλύψουμε πολλά ζεύγη ίδιων τμημάτων στο κωδικοποιημένο κείμενο και βρούμε τον μεγαλύτερο ακέραιο που διαιρεί τις αποστάσεις μεταξύ των ζευγών (δηλαδή τον μέγιστο κοινό διαιρέτη τους), τότε είναι πολύ πιθανό να έχουμε ανακαλύψει το μήκος της λέξης που χρησιμοποιήθηκε για την κωδικοποίηση! **Αυτός ο τρόπος κρυπτανάλυσης ονομάζεται Kasiski.**

Μα θα αναρωτηθεί κάποιος: σε τι μπορεί να μας βοηθήσει η γνώση του μήκους του κλειδιού; Ακόμα και αν ανακαλύψουμε ότι η λέξη έχει 10 γράμματα, για παράδειγμα ο αριθμός των δυνατών λέξεων θα παρέμενε μεγάλος, περίπου ίσος με 2.000.000, και θα έπρεπε να δοκιμάσουμε την αποκρυπτογράφηση του κειμένου με κάθε μια από αυτές τις πιθανές λέξεις.

Όμως, τα πράγματα δεν είναι τόσο απελπιστικά όσο φαίνονται. Έστω ότι με βάση την ανάλυση των ζευγών ίδιων τμημάτων έχουμε φτάσει στο συμπέρασμα ότι ο αριθμός των γραμμάτων στη λέξη είναι t (t=5 στο παράδειγμά μας).

Τότε γνωρίζουμε:

1. ότι έχουν χρησιμοποιηθεί 5 διαφορετικά γενικευμένα (και όχι απαραίτητα χρησιμοποιώντας μετατόπιση στα δεξιά) σχήματα.
2. ότι στο κρυπτογραφημένο κείμενο οι χαρακτήρες που έχουν απόσταση t έχουν κωδικοποιηθεί με το ίδιο σχήμα αντικατάστασης!

Άρα μπορούμε να μοιράσουμε τους χαρακτήρες του κρυπτογραφημένου κειμένου σε t κατηγορίες ξεκινώντας :

¶ από τον πρώτο χαρακτήρα και μετρώντας χαρακτήρες ανά t,

¶ μετά από τον δεύτερο χαρακτήρα και μετρώντας πάλι ανά t, κ.ο.κ.

¶ Τέλος, εκτελούμε t κρυπταναλύσεις, γενικευμένου σχήματος αντικατάστασης, χρησιμοποιώντας τελικά τον πλεονασμό της γλώσσας στην οποία γράφτηκε το μήνυμα.

Εάν η γλώσσα του μηνύματος δεν είναι γνωστή, μπορούμε φυσικά να χρησιμοποιήσουμε στατιστικά στοιχεία των γνωστών γλωσσών και έτσι να δοκιμάζουμε κάθε φορά και μια διαφορετική γλώσσα μέχρι η αποκρυπτογράφησή μας να έχει νόημα.

Στο σημείο αυτό, αυτό που πρέπει να επισημάνουμε είναι ότι για μία ακόμη φορά η προσπάθεια για ανακάλυψη του τέλειου τρόπου κρυπτογράφησης δεν απέδωσε όσα περιμέναμε. Φάνηκε ότι αποφύγαμε την επίθεση με βάση τα στατιστικά στοιχεία που αφορούν τη γλώσσα, μόνο για να διαπιστώσουμε ότι η επίθεση αυτή ήταν μόλις λίγα βήματα πιο μακριά!

# Κεφάλαιο 2

# Σύγχρονες Μέθοδοι Κρυπτογράφησης

(Τα στοιχεία που αναφέρονται στο κεφάλαιο αυτό βρίσκονται στις πηγές ([1], [3], [4], [8], [11], [12], [14], [18], [19], [20], [23], [24], [27], [28], [30], [32], [37],[38], [39]).

Όπως προαναφέραμε, η κρυπτογραφία ήταν γνωστή από την αρχαιότητα. Με το πέρασμα των χρόνων και την ραγδαία εξέλιξη της τεχνολογίας οι απαιτήσεις για περισσότερο σύνθετες μεθόδους κρυπτογράφησης έχουν αυξηθεί. Σήμερα τεράστιες ποσότητες ευαίσθητων προσωπικών πληροφοριών, και όχι μόνο, ανταλλάσσονται μέσω δημόσιων δικτύων. Έτσι, η κρυπτογραφία έχει διευρυνθεί για να ανταποκρίνεται στη νέα αυτή πραγματικότητα.

Σε αυτό το κεφάλαιο θα περιγραφούν σύγχρονες μέθοδοι κρυπτογράφησης όπως είναι η συμμετρική και η ασύμμετρη κρυπτογράφηση καθώς και οι αλγόριθμοί τους. Επίσης, θα περιγραφεί η χρήση των ψηφιακών υπογραφών με τις οποίες η σύγχρονη κρυπτογραφία εξασφαλίζει την αυθεντικότητα των μηνυμάτων.

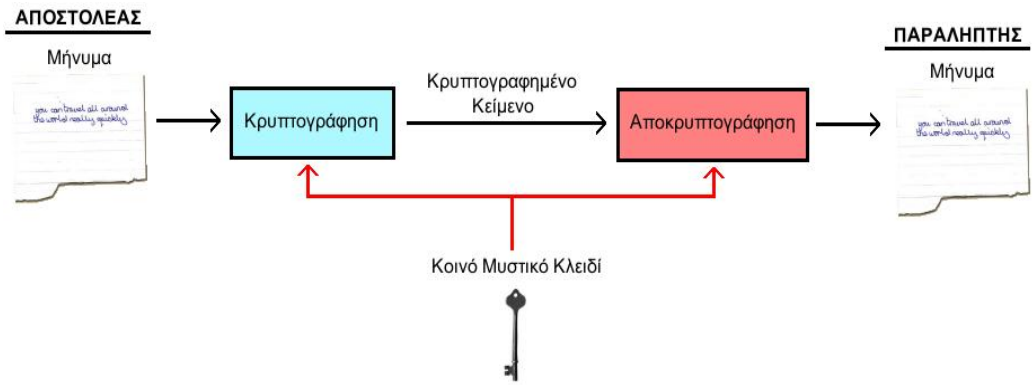
Ένα άλλο θέμα που θα μας απασχολήσει είναι η δύναμη και η αντοχή της κρυπτογράφησης και οι επιθέσεις στους αλγόριθμους συμμετρικού και δημόσιου κλειδιού. Παράλληλα θα αναφερθούμε σε προγράμματα κρυπτογράφησης που κυκλοφορούν στην αγορά, όπως το PGP, το S/MIME και το X.509, στο πρότυπο κρυπτογράφησης δημόσιου κλειδιού και σε πρωτόκολλα ασφαλείας όπως το SSL ,S-HTTP και το SET.

Τέλος, θα αναφερθούμε στο μέλλον της κρυπτογραφίας που έιναι η κβαντική κρυπτογραφία.

## 2.1 Συμμετρική κρυπτογραφία

Η παραδοσιακή μέθοδος κρυπτογραφίας είναι γνωστή σαν συμμετρική κρυπτογραφία. Οι αλγόριθμοι που χρησιμοποιούνται είναι οι DES, DESX, Triple DES, IDEA, AES, RC2, RC4 και RC5. Θεωρείται εύκολη και γρήγορη ως διαδικασία αν και δεν είναι ιδιαίτερα ασφαλής.

Σε αυτή την μέθοδο χρησιμοποιείται ένα κοινό κλειδί και για την κρυπτογράφηση και για την αποκρυπτογράφηση. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα συναλλασσόμενα μέρη. Ο αποστολέας κρυπτογραφεί το μήνυμα με βάση αυτό το κλειδί και ο παραλήπτης το αποκρυπτογραφεί με βάση το ίδιο κλειδί (Εικόνα 14).




**Εικόνα 14:** Η διαδικασία κρυπτογράφησης συμμετρικού κλειδιού.

Η ασφάλεια των αλγορίθμων βασίζεται στην μυστικότητα του κλειδιού γι' αυτό το λόγο το συμμετρικό κρυπτοσύστημα προϋποθέτει την ανταλλαγή του κλειδιού:

A. Μέσα από την φυσική παρουσία των προσώπων, πράγμα δύσκολο ή αδύνατο αφού πολλές φορές οι συναλλασσόμενοι βρίσκονται σε μεγάλη χιλιομετρική απόσταση μεταξύ τους ή δεν γνωρίζονται .

Β. Μέσα από ένα ασφαλές κανάλι επικοινωνίας. Φυσικά το διαδίκτυο δεν μπορεί να αποτελέσει κανάλι ασφαλούς επικοινωνίας, οπότε η χρήση της συμμετρικής κρυπτογράφησης σε εφαρμογές ηλεκτρονικού εμπορίου και ανταλλαγής ηλεκτρονικών μηνυμάτων ουσιαστικά δεν υφίσταται.

### 2.1.1 Αλγόριθμοι συμμετρικής κρυπτογράφησης :

1 DES - Data Encryption Standard: αποδίδεται στα ελληνικά με τον όρο Πρότυπο Κρυπτογράφησης Πληροφοριών. Δημιουργήθηκε από την κυβέρνηση των Ηνωμένων Πολιτειών Αμερικής τη δεκαετία του 1970 και αναπτύχθηκε από την IBM. Είναι ένας “μπλοκ” αλγόριθμος που χρησιμοποιεί κλειδί 56-bit και έχει πολλούς τύπους λειτουργιών, ανάλογα με τον σκοπό που χρησιμοποιείται. Αποτελεί έναν δυνατό αλγόριθμο, αλλά πιθανολογείται ότι μπορεί να δημιουργηθεί μια μηχανή που θα είναι ικανή να σπάσει ένα κρυπτογραφημένο μήνυμα σε μερικές ώρες. Πιθανολογείται πως τέτοιες μηχανές υπάρχουν, αν και καμία κυβέρνηση ή επίσημη εταιρία δεν παραδέχεται κάτι τέτοιο.

2 DESX: Είναι μια απλή μετατροπή του DES αλγορίθμου για να βελτιώσει την ασφάλεια και να κάνει την αναζήτηση κλειδιού δυσκολότερη.

2 Triple DES: Είναι ένας τρόπος να κάνεις τον DES τουλάχιστον δύο φορές πιο ασφαλή χρησιμοποιώντας τον DES αλγόριθμο τρεις φορές με τρία διαφορετικά κλειδιά. Αναλυτικότερα, χρησιμοποιεί τον απλό DES για να κρυπτογραφήσει τα δεδομένα, μετά τα αποκρυπτογραφεί μ' ένα άλλο κλειδί και κρυπτογραφεί ξανά το αποτέλεσμα μ' ένα άλλο κλειδί. Η κρυπτογράφηση που επιτυγχάνεται μ' αυτόν τον τρόπο είναι ισοδύναμη μ' ένα υποθετικό 112-bit DES.

- IDEA - International Data Encryption Algorithm: Αναπτύχθηκε στην Ζυρίχη της Ελβετίας από τους James L. Massey και τον Xuejia και δημοσιεύτηκε το 1990. Ουσιαστικά χρησιμοποιεί ένα κλειδί των 128-bit για να κάνει μια σειρά από μη γραμμικούς μαθηματικούς μετασχηματισμούς σ' ένα μπλοκ δεδομένων των 64 bit. Θεωρείται ότι είναι πολύ ασφαλής .

- AES - Advanced Encryption Standard **:** αποδίδεται στα ελληνικά με τον όρο Προηγμένο Πρότυπο Κρυπτογράφησης και σχεδιάστηκε για να αποτελέσει το νέο βασικό αλγόριθμο κρυπτογράφησης που θα χρησιμοποιηθεί από τις κυβερνητικές υπηρεσίες των ΗΠΑ, ως διάδοχος του DES.

- RC2: Είναι ένας μπλόκ αλγόριθμος ο οποίος και αναπτύχθηκε από τον Ronald Rivest και κρατείται σαν επαγγελματικό μυστικό από την RSA Data Security. Αυτός ο αλγόριθμος ανακαλύφθηκε από ένα ανώνυμο μήνυμα που βρέθηκε στο Usenet to 1996. Ο RC2 πωλείται με μια λειτουργία με την οποία μπορείς να χρησιμοποιήσεις κλειδιά από 1- bit έως 2048 -bit. Συχνά, όμως, το μήκος τους φθάνει στα 40-bit, για εφαρμογές που εξάγονται, με αποτέλεσμα να γίνεται πολύ ευάλωτος στην επίθεση έρευνας κλειδιού.

- RC4: Είναι ένας αλγόριθμος «συρμού» ο οποίος αναπτύχθηκε από τον Ronald Rivest. Αφορμή για την ανακάλυψη του αποτέλεσε ένα ανώνυμο μήνυμα που βρέθηκε στο Usenet το 1994.

- RC5: Είναι ένας μπλοκ αλγόριθμος ο οποίος αναπτύχθηκε από τον Ronald Rivest και δημοσιεύτηκε το 1994. Δίνει την δυνατότητα στο χρήστη να ορίζει το μήκος κλειδιού, το μέγεθος του «μπλοκ» δεδομένων και το πόσες φορές θα γίνει η κρυπτογράφηση.

### 2.1.2 Πλεονεκτήματα – Μειονεκτήματα συμμετρικής κρυπτογράφησης.

Βασικό πλεονέκτημά της θεωρείται ότι είναι η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης η οποία:

< είναι πολύ γρήγορη,

< δεν καταναλώνει σημαντική υπολογιστική ισχύ.

Μειονεκτήματα της μεθόδου είναι:

= Πρακτικά αδυνατεί να προσφέρει ουσιαστικά ασφαλή διαχείριση κλειδιών σε δημόσια δίκτυα με πληθώρα χρηστών. Συγκεκριμένα, αν δύο μέρη συμφωνούν πάνω σε ένα κοινό ιδιωτικό κλειδί για να ανταλλάξουν τα μηνύματά τους, για Ν ανταποκριτές χρειάζονται Ν ιδιωτικά κλειδιά. Αυτό σημαίνει ότι αν χρησιμοποιηθούν κοινά κλειδιά για δύο ανταποκριτές, τότε μπορεί να διαβάσει ο ένας τα μηνύματα του άλλου.

= Αντιμετωπίζει πρόβλημα στο θέμα της αυθεντικοποίησης γιατί είναι αδύνατο να αποδειχτεί η ταυτότητα αποστολέα και παραλήπτη του μηνύματος. Αν δύο ανταποκριτές μοιράζονται το ίδιο κλειδί, μπορούν να στείλουν κρυπτογραφημένο μήνυμα και να ισχυριστούν ότι το έστειλε ο άλλος.

Τη λύση σε αυτά τα προβλήματα έρχεται να δώσει η ασύμμετρη κρυπτογραφία.

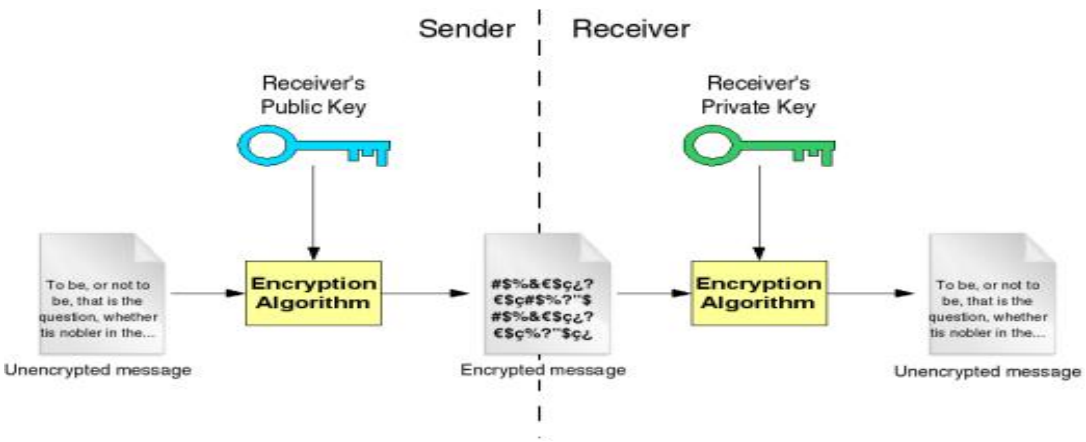
## 2.2 Ασύμμετρη Κρυπτογραφία.

Η ασύμμετρη κρυπτογραφία ή αλλιώς κρυπτογράφηση δημοσίου κλειδιού δημιουργήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield

Diffie και Martin Hellman για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίασε η συμμετρική κρυπτογράφηση.

Χαρακτηριστικό της είναι ότι χρησιμοποιεί ένα ζεύγος κλειδιών για την κρυπτογράφηση και την αποκρυπτογράφηση: το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα.

Συγκεκριμένα, 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. Για την εξυπηρέτηση αυτού του σκοπού δημιουργήθηκαν 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 (εικόνα 15). 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. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης, με τις υπάρχουσες δυνατότητες της τεχνολογίας, δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.




**Εικόνα 15**: Η διαδικασία κρυπτογράφησης δημόσιου κλειδιού.

Το αρχικό όφελος της ασύμμετρης κρυπτογραφίας είναι ότι επιτρέπει στους ανθρώπους που δεν έχουν καμία προϋπάρχουσα ρύθμιση ασφάλειας να ανταλλάξουν μηνύματα με ασφάλεια. Έτσι, τα μηνύματα που αποστέλλονται δεν είναι δυνατόν, να τροποποιηθούν κατά την διάρκεια της μετάδοσης τους, καθώς η οποιαδήποτε αλλοίωση τους τα καθιστά μη δυνάμενα να αποκρυπτογραφηθούν, κάτι που θα γίνει αμέσως αντιληπτό από τον παραλήπτη.

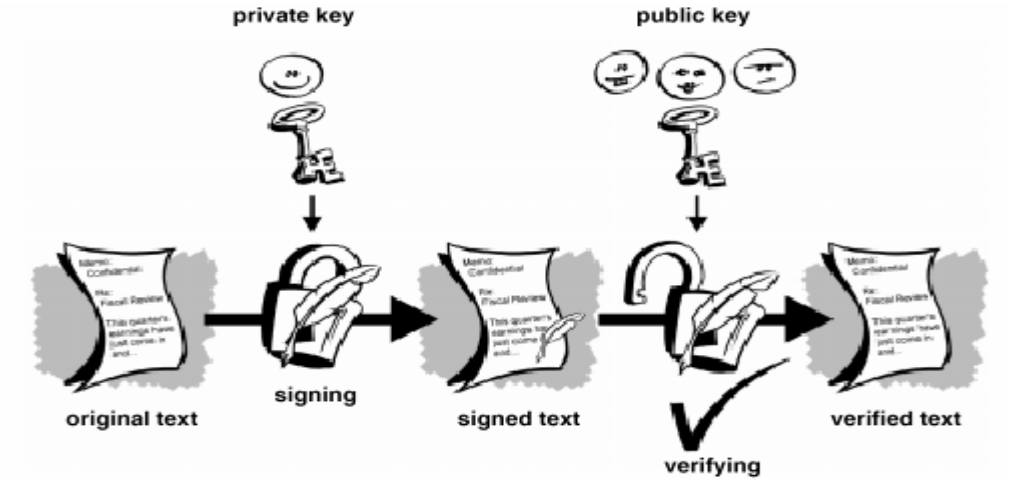
### 2.2.1 Αλγόριθμοι ασύμμετρης κρυπτογράφησης :

- RSA: Τα αρχικά του αναφέρονται στους δημιουργούς του αλγορίθμου (Rivest-Shamir-Adleman). Η βασική ασφάλεια στο RSA προέρχεται από το γεγονός ότι ενώ είναι σχετικά εύκολο να πολλαπλασιάσουμε δύο μεγάλους πρώτους αριθμούς και να πάρουμε το γινόμενο τους, είναι υπολογιστικά δύσκολο να κάνουμε το αντίστροφο, δηλ. το να βρούμε τους δύο πρώτους παράγοντες. Ο RSA επιτρέπει τη δημιουργία και την αποκάλυψη στον κόσμο ενός κλειδιού κρυπτογράφησης, ενώ αντίθετα δεν επιτρέπει την αποκρυπτογράφηση ενός μηνύματος. Μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση μηνυμάτων και για τη δημιουργία ψηφιακών υπογραφών, δηλαδή για την επιβεβαίωση της ταυτότητας του αποστολέα ενός μηνύματος.

- ElGamal: Ο δημιουργός αυτού του αλγόριθμου είναι ο Taher ELGamal. Κατασκεύασε ένα κρυπτογραφικό σύστημα δημοσίου κλειδιού που είναι βασισμένο στο πρωτόκολλο ανταλλαγής κλειδιών των Diffie-Hellman. Χρησιμοποιείται για την κρυπτογράφηση και για την δημιουργία ψηφιακών υπογραφών, με τον ίδιο τρόπο όπως ο αλγόριθμος RSA.

## 2.3 Ψηφιακές Υπογραφές – Ηλεκτρονικές Υπογραφές.

Μια συμβατική υπογραφή χρησιμοποιείται ως γνωστόν για την απόδειξη της γνησιότητας ενός εγγράφου. Αντίστοιχα, στα δίκτυα υπολογιστών χρειάζεται η χρήση ενός ηλεκτρονικού ισοδύναμου της συμβατικής υπογραφής, δηλαδή μιας ηλεκτρονικής υπογραφής. Η ψηφιακή υπογραφή, ως ένα είδος ηλεκτρονικής υπογραφής, είναι μια συμβολοσειρά από bits και εξαρτάται από το μήνυμα που συνοδεύει.




**Εικόνα 16:** Διαδικασία υλοποίησης ψηφιακής υπογραφής.

Πιο συγκεκριμένα, με τον όρο ψηφιακή ή ηλεκτρονική υπογραφή εννοούμε δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα, τα οποία χρησιμεύουν ως μέθοδος απόδειξης:

# Της ταυτότητας του αποστολέα ενός εγγράφου ή οποιασδήποτε πληροφορίας μπορεί να αποθηκευτεί σε έναν Η/Υ,

# της ακεραιότητας του εγγράφου,

# και της εξασφάλισης ότι κάποιος συγκεκριμένος παραλήπτης και μόνον αυτός θα μπορεί να διαβάσει το έγγραφο γνησιότητας.

Οι ψηφιακές υπογραφές αποτελούν το ηλεκτρονικό ισοδύναμο των χειρόγραφων υπογραφών, αφού σύμφωνα με το άρθρο 3 του προεδρικού διατάγματος 150/2001 εξομοιώνονται με τις ιδιόχειρες. Η ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής, αντικαθιστά την ιδιόχειρη υπογραφή τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο.

Για την ψηφιακή υπογραφή ενός εγγράφου χρησιμοποιείται η κρυπτογραφία δημόσιου κλειδιού – ασύμμετρη. Ο χρήστης διαθέτει δύο κλειδιά (το ιδιωτικό και το δημόσιο). Αν κάποιος γνωρίζει μόνο το ένα κλειδί είναι πρακτικά αδύνατον να καταφέρει τον υπολογισμό του άλλου. Η διαφοροποίηση έγκειται στο ότι για την δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

Η ηλεκτρονική υπογραφή πρέπει να πληροί τις παρακάτω προϋποθέσεις:

**R** Να συνδέεται μονοσήμαντα με τον υπογράφοντα.

**R** Να είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος.

**R** Να δημιουργείται με τη χρήση μέσων που ο υπογράφων θα μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο.

**R** Να συνδέεται με τα δεδομένα στα οποία αναφέρεται, έτσι ώστε να μπορεί να εντοπιστεί οποιαδήποτε μεταγενέστερη αλλοίωσή τους.

Στην διαδικασία της δημιουργίας και της επαλήθευσης της ηλεκτρονικής υπογραφής εμπλέκεται η έννοια της συνάρτησης κατακερματισμού (συνάρτηση one way hash).

Πρόκειται για μηχανισμούς που ενώ στην είσοδο τους δέχονται ένα οποιοδήποτε μήνυμα, μεγάλο ή μικρό, στην έξοδο τους δίνουν ένα σύντομο

κείμενο σταθερού μήκους που ονομάζεται σύνοψη – περίληψη (message digest), το οποίο συνδέεται μοναδικά με το αρχικό έγγραφο .

Η σύνοψη είναι μια μοναδική ψηφιακή αναπαράσταση του μηνύματος, γι' αυτό η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Το ενδιαφέρον με τις συναρτήσεις κατακερματισμού είναι ότι έχουν εξαιρετικά μεγάλη ευαισθησία στο περιεχόμενο του μηνύματος εισόδου. Αν αλλάξει έστω και ένα bit κειμένου, τότε δημιουργείται μια τελείως διαφορετική σύνοψη.

Είναι υπολογιστικά αδύνατον κάποιος να καταφέρει να εξάγει το αρχικό μήνυμα. Η ηλεκτρονική υπογραφή είναι στην ουσία κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα και η σύνοψη είναι διαφορετική για κάθε μήνυμα.

Θεωρώντας ότι ο αποστολέας έχει ένα συγκεκριμένο ζευγάρι κλειδιών από τα οποία το ιδιωτικό κλειδί είναι στην πλήρη κατοχή του, τότε το γεγονός ότι το χρησιμοποιεί για να κρυπτογραφήσει το μήνυμα, πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί (με το αντίστοιχο δημόσιο κλειδί), την ταυτότητα του αποστολέα. Αυτός είναι και ο τρόπος αυθεντικοποίησης της ταυτότητας του αποστολέα του μηνύματος.

**Συμπέρασμα:** Μια ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί μόνο εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχο του.

## 2.4 Υποδομή δημοσίου κλειδιού (Public Key Infrastructure).

Η Υποδομή Δημοσίου Κλειδιού αποτελεί ένα συνδυασμό λογισμικού, τεχνολογιών κρυπτογραφίας και υπηρεσιών, ο οποίος πιστοποιεί την ταυτότητα

κάθε φυσικού προσώπου που εμπλέκεται σε μια συναλλαγή στο Διαδίκτυο, και παράλληλα προστατεύει την ασφάλεια της συναλλαγής.

Ενσωματώνει ψηφιακά πιστοποιητικά, κρυπτογραφία δημόσιου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα. Η υλοποίησή της περιλαμβάνει την παροχή ψηφιακών πιστοποιητικών σε χρήστες, εξυπηρετητές (servers) και λογισμικό χρηστών. Παράλληλα προσφέρει μια σειρά εργαλείων για τη διαχείριση, ανανέωση και ανάκληση των πιστοποιητικών.

### 2.4.1 Οι βασικές λειτουργίες/υπηρεσίες των Υποδομών Δημόσιου Κλειδιού

**1.** Εμπιστευτικότητα (Confidentiality): Πρόκειται για την προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη πρόσβαση. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή τους. Η Υποδομή Δημόσιου Κλειδιού παρέχει κωδικοποίηση, αφού οι μηχανισμοί ελέγχου πρόσβασης πραγματοποιούνται κατά βάση από το συνδυασμό μεθόδων πιστοποίησης (authentication) και εξουσιοδότησης (authorization).

**2.** Ακεραιότητα (Integrity): Είναι η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάστασή τους. Παρέχεται από μηχανισμούς κρυπτογραφίας όπως οι ηλεκτρονικές υπογραφές.

**3.** Πιστοποίηση (Authentication): Πρόκειται για την επιβεβαίωση της ταυτότητας ενός ατόμου ή της πηγής αποστολής των πληροφοριών. Κάθε χρήστης που επιθυμεί να επιβεβαιώσει την ταυτότητα ενός άλλου προσώπου ή εξυπηρετητή με τον οποίο επικοινωνεί βασίζεται στην πιστοποίηση. Οι παραδοσιακές μέθοδοι πιστοποίησης είναι οι εξής:

¶ Με κάποιον κωδικό που γνωρίζουμε, όπως το PIN μιας τραπεζικής κάρτας ή το password ενός λογαριασμού.

¶ Με κάποιο αντικείμενο που έχουμε στην ιδιοκτησία μας, λόγου χάρη το κλειδί μιας πόρτας ή μια τραπεζική κάρτα.

¶ Με δακτυλικά αποτυπώματα, φωνή κ.λπ

**4.** Μη Άρνηση Αποδοχής (Non-Repudiation): Η Μη Άρνηση Αποδοχής συνδυάζει τις υπηρεσίες της Πιστοποίησης και της Ακεραιότητας. Ο αποστολέας των δεδομένων δεν μπορεί να αρνηθεί ότι δημιούργησε και απέστειλε το μήνυμα. Η ασύμμετρη κρυπτογραφία παρέχει ηλεκτρονικές υπογραφές, κατά συνέπεια μόνο ο αποστολέας του μηνύματος κατέχει τη συγκεκριμένη υπογραφή. Με αυτόν τον τρόπο, ο οποιοσδήποτε και φυσικά ο παραλήπτης του μηνύματος μπορεί να επιβεβαιώσει την ηλεκτρονική υπογραφή του αποστολέα.

## 2.5 Αρχή Πιστοποίησης

Το πιστοποιητικό (certificate) είναι ο τρόπος με τον οποίο η Υποδομή Δημόσιου Κλειδιού μεταδίδει τις τιμές των δημόσιων κλειδιών ή τις πληροφορίες που σχετίζονται με αυτά, ή και τα δύο. Η εκδότρια αρχή των πιστοποιητικών ονομάζεται Αρχή Πιστοποίησης (Certificate Authority - CA).

Οι Αρχές Πιστοποίησης διασφαλίζουν τη δημοσίευση και τη διανομή των δημόσιων κλειδιών και λαμβάνουν το δημόσιο κλειδί του ενδιαφερόμενου χρήστη. Εάν ο χρήστης:

¶ Ενεργεί ως ιδιώτης, θα πρέπει να παραχωρήσει όλα τα απαραίτητα στοιχεία που αποδεικνύουν την ταυτότητά του.

¶ Θεωρείται ότι ενεργεί εκ μέρους κάποιας επιχείρησης, οφείλει να παραχωρήσει όλες τις νομικές πληροφορίες που απαιτούνται για την αξιοπιστία και τη νόμιμη λειτουργία της.

Ουσιαστικά ένα ψηφιακό πιστοποιητικό αποτελεί μια ψηφιακά υπογεγραμμένη δήλωση από μια αρχή πιστοποίησης, η οποία:

**P** Προσδιορίζει την αρχή πιστοποίησης που το εξέδωσε.

**P** Περιέχει το όνομα και κάποιες άλλες πληροφορίες του εγγεγραμμένου.

**P** Περιέχει το δημόσιο κλειδί του εγγεγραμμένου, το οποίο είναι ψηφιακά υπογεγραμμένο από την αρχή πιστοποίησης που το εξέδωσε.

Για την πιστοποίηση της ταυτότητας των συναλλασσόμενων χρησιμοποιούνται τα πιστοποιητικά ασφαλείας, που εγγυώνται επιπλέον την ασφάλεια ενός δικτυακού τόπου. Υπάρχουν δύο είδη πιστοποιητικών:

/ Τα προσωπικά πιστοποιητικά, τα οποία αποτελούν ένα είδος εγγύησης ότι ο χρήστης είναι αυτός που δηλώνει ότι είναι. Σε αυτά καταχωρούνται προσωπικές πληροφορίες, όπως όνομα χρήστη και κωδικός πρόσβασης. Στη συνέχεια οι πληροφορίες αυτές αποθηκεύονται σε ένα πιστοποιητικό, το οποίο χρησιμοποιείται όταν στέλνονται προσωπικές πληροφορίες σε ένα διακομιστή ελέγχου ταυτότητας. Τέλος, ένα προσωπικό πιστοποιητικό επιτρέπει στο χρήστη να λαμβάνει κρυπτογραφημένα μηνύματα από τους υπόλοιπους χρήστες.

/ Τα πιστοποιητικά δικτυακών τόπων, τα οποία περιέχουν πληροφορίες που πιστοποιούν ότι η συγκεκριμένη ιστοσελίδα είναι γνήσια και ασφαλής. Αυτό διασφαλίζει ότι κανένα άλλο site δεν μπορεί να παρουσιαστεί με την ταυτότητα της γνήσιας και ασφαλούς τοποθεσίας. Επίσης, τα πιστοποιητικά δικτυακών τόπων χρονολογούνται κατά την έκδοσή τους. Όταν προσπαθείτε να συνδεθείτε με το website ενός οργανισμού, το πρόγραμμα ανάγνωσης επαληθεύει την ηλεκτρονική διεύθυνση Internet που είναι αποθηκευμένη στο πιστοποιητικό και ελέγχει την ημερομηνία λήξης του. Εάν οι πληροφορίες αυτές δεν είναι έγκυρες

ή εάν έχει παρέλθει η ημερομηνία λήξης εμφανίζεται προειδοποιητικό μήνυμα (Warning).

**Η γενική μορφή πιστοποιητικού περιέχει τα ακόλουθα στοιχεία:**

- Έκδοση:. Version 1,version 2, version 3.
- Serial Number: Είναι μία ακέραιη τιμή η οποία σχετίζεται με το πιστοποιητικό. Χαρακτηριστικό της είναι η μοναδικότητα της μέσα στο CA.
- Signature algorithm Identifier: Περιγράφει τον αλγόριθμο που χρησιμοποιείται για να υπογραφεί το πιστοποιητικό καθώς και τις σχετικές παραμέτρους.
- Όνομα εκδότη: Το όνομα της CA πού δημιούργησε και υπέγραψε αυτό το πιστοποιητικό.
- Περίοδος ισχύος: Περιέχει δύο ημερομηνίες, την πρώτη και την τελευταία μέρα που ισχύει το πιστοποιητικό.
- Όνομα θέματος: Το όνομα του χρήστη στον οποίο απευθύνεται το πιστοποιητικό. Έτσι επιβεβαιώνεται το δημόσιο κλειδί του θέματος και το αντίστοιχο ιδιωτικό κλειδί.
- Πληροφορίες δημόσιου κλειδιού: Περιλαμβάνει το δημόσιο κλειδί του θέματος, την αναγνώριση αλγορίθμου που θα χρησιμοποιηθεί για το κλειδί καθώς και τις σχετικές παραμέτρους.
- Αναγνώριση μοναδικού εκδότη: Είναι προαιρετικό πεδίο που χρησιμοποιείται για την αναγνώριση της CA.
- Αναγνώριση μοναδικού θέματος: Άλλο ένα προαιρετικό πεδίο που χρησιμοποιείται για την αναγνώριση του μοναδικού θέματος .
- Προεκτάσεις (extensions): Είναι μια σειρά από ένα ή περισσότερα πεδία που χρησιμεύουν στις προεκτάσεις.

- Υπογραφή: καλύπτει όλα τα υπόλοιπα πεδία του πιστοποιητικού. Περιέχει το μυστικό κωδικό των άλλων πεδίων κρυπτογραφημένο με το ιδιωτικό κλειδί της CA, καθώς και τον αλγόριθμο αναγνώρισης υπογραφής.

Τα πιστοποιητικά του χρήστη που δημιουργούνται από τη CA έχουν τα ακόλουθα χαρακτηριστικά:

**1.** Όποιος χρήστης έχει πρόσβαση στο δημόσιο κλειδί τις CA μπορεί να επαληθεύσει το δημόσιο κλειδί του χρήστη που είχε επικυρωθεί.

**2.** Κανένας άλλος οργανισμός εκτός από τη CA δεν μπορεί να τροποποιήσει το πιστοποιητικό χωρίς να ελεγχθεί.

**Σημείωση:** Η CA υπογράφει το πιστοποιητικό με το ιδιωτικό κλειδί της. Αν το αντίστοιχο δημόσιο κλειδί είναι γνωστό σε έναν χρήστη, τότε ο χρήστης μπορεί να επαληθεύσει αν έχει πιστοποιητικό που βρίσκεται σε ισχύ και υπογράφεται από τη CA.

**3.** Τα πιστοποιητικά δεν μπορούν να πλαστογραφηθούν, για αυτό το λόγο μπορούν να τοποθετηθούν στον κατάλογο χωρίς να χρειάζεται ιδιαίτερη προστασία. Αν όλοι οι χρήστες τοποθετούσαν στον κατάλογο της ίδιας CA τα πιστοποιητικά τους, τότε όχι μόνο θα είχαν πρόσβαση όλοι, αλλά θα έδειχναν και την κοινή τους εμπιστοσύνη στην συγκεκριμένη CA.

**4.** Όλα τα πιστοποιητικά των CA πρέπει να εμφανίζονται στον κατάλογο. Ο χρήστης πρέπει να γνωρίζει τη διαδικασία σύνδεσης, για να ακολουθήσει το μονοπάτι προς το δημόσιο κλειδί του πιστοποιητικού κάποιου χρήστη.

**5.** Τα πιστοποιητικά είναι οργανωμένα ιεραρχικά για να είναι η πλοήγηση πιο άμεση.

**6.** Κάθε πιστοποιητικό έχει χρόνο ισχύος, όπως μια πιστωτική κάρτα. Θα πρέπει να ανανεώνετε πριν την λήξη του για τους εξής λόγους:

- Το ιδιωτικό κλειδί του χρήστη θεωρείται ότι έχει εκτεθεί.
- Ο χρήστης δεν θα αναγνωρίζεται πλέον από τη CA.
- Το πιστοποιητικό της CA θεωρείται ότι έχει λήξει.

Κάθε CA είναι υποχρεωμένη να διατηρεί μια λίστα των καινούριων πιστοποιητικών αλλά όχι αυτών που έχουν λήξει.

## 2.6 Δύναμη και αντοχή κρυπτογράφησης.

Όλοι οι τύποι της κρυπτογραφίας δεν είναι ίδιοι. Άλλα συστήματα παρακάμπτονται εύκολα δηλαδή «σπάζονται». Άλλα αντιστέκονται αρκετά, ακόμα και στις πιο καλές επιθέσεις. Η ικανότητα ενός κρυπτογραφικού συστήματος να προστατεύσει την πληροφορία από μια επίθεση ονομάζεται αντοχή του. Η αντοχή εξαρτάται από πολλούς παράγοντες, μερικοί από αυτούς παρουσιάζονται παρακάτω:

**R** Η μυστικότητα του κλειδιού.

**R** Η δυσκολία να μαντέψουμε το κλειδί, ή να δοκιμάσουμε όλα τα πιθανά κλειδιά. Μακρύτερα κλειδιά είναι γενικά δυσκολότερο να μαντέψεις ή να βρεις.

**R** Η δυσκολία να αναστρέψουμε έναν αλγόριθμο κρυπτογράφησης χωρίς να γνωρίζουμε το κλειδί (σπάσιμο του αλγορίθμου κρυπτογράφησης).

**R** Η ύπαρξη άλλων δρόμων, όπως λέμε «πίσω πόρτα», με τους οποίους μπορούμε να αποκρυπτογραφήσουμε πιο εύκολα ένα αρχείο χωρίς να γνωρίζουμε το κλειδί κρυπτογράφησης.

**R** Η ικανότητα να αποκρυπτογραφήσουμε ένα ολόκληρο κωδικοποιημένο μήνυμα, αν γνωρίζαμε τον τρόπο με τον οποίο αποκρυπτογραφήθηκε ένα μέρος αυτού.

**R** Η ιδιοκτησία και η γνώση των χαρακτηριστικών της πληροφορίας που επιθυμούμε να κρυπτογραφήσουμε.

Ο στόχος στο σχεδιασμό κρυπτογραφικών συστημάτων είναι η δημιουργία ενός αλγόριθμου που θα είναι πολύ δύσκολο να αναστραφεί χωρίς το κλειδί. Η δυσκολία της αναστροφής αυτής πρέπει να είναι σχεδόν ισοδύναμη με την προσπάθεια που απαιτείται για να μαντέψουμε το κλειδί προσπαθώντας με πιθανές λύσεις κάθε φορά. Για να επιτευχθεί κάτι τέτοιο χρειάζεται να χρησιμοποιηθούν μαθηματικά υψηλού επιπέδου.

Όταν ένας καινούργιος αλγόριθμος σχεδιάζεται οι δημιουργοί του πιστεύουν ότι είναι τέλειος. Πιστεύουν πως είναι τόσο δυνατός ώστε δεν υπάρχει περίπτωση να αποκρυπτογραφηθεί η πληροφορία που κωδικοποιήθηκε χωρίς την χρήση του κατάλληλου κλειδιού. Επίσης, οι σχεδιαστές προσπαθούν να «σπάσουν» τον αλγόριθμο με είδη γνωστούς τρόπους επιθέσεων. Όμως με το πέρασμα του χρόνου, καινούργιες τεχνικές επίθεσης ανακαλύπτονται και δημοσιεύονται.

Για το λόγο αυτό, πρέπει να είμαστε ιδιαίτερα προσεκτικοί με καινούργιους κρυπτογραφικούς αλγόριθμους. Παρακάτω αναφέρονται διαφόρων ειδών επιθέσεις.

## 2.7 Ποιοι διακυβεύουν την ασφάλεια των συστημάτων

Μια πολύ σημαντική προϋπόθεση για την αναγνώριση των «εχθρών» είναι να κατανοηθεί το ποιοι ακριβώς είναι. Η έρευνα συνήθως ξεκινά εστιάζοντας στους τύπους επιθέσεων και στη ζημιά που μπορεί να προκύψει, παραγκωνίζοντας έτσι τη σημασία των μέσων που χρησιμοποιούνται για να διεκπεραιωθεί, τελικά με επιτυχία, η επίθεση. Ένας αποφασισμένος «εισβολέας» είναι διατεθειμένος να προσπαθήσει πολύ για να πετύχει το στόχο

του, δηλαδή να εισχωρήσει στο σύστημα. Αντίθετα, ένας αδιάφορος «εισβολέας» θα τα παρατήσει σχετικά γρήγορα. Στο σημείο αυτό, γίνεται αντιληπτό πως η επιμονή μας δίνει τη δυνατότητα να διαχωρίσουμε τους εχθρούς.

Τα ερωτήματα που πρέπει να απασχολήσουν τον διαχειριστή ασφαλείας ή οποιονδήποτε εμπλέκεται με ζητήματα ασφαλείας ηλεκτρονικού εμπορίου είναι τα εξής:

1. Ποιοι είναι ενδεχομένως οι εχθροί του συστήματος.
2. Ποιες οι πιθανές προθέσεις τους.
3. Ποιες είναι οι πηγές τους.
4. Τι μέσα διαθέτουν.

Έτσι προκύπτουν τα πιθανά μέσα επίθεσης που χρησιμοποιούν οι «εχθροί»:

**1. <u>Επιθέσεις στους αλγόριθμους συμμετρικού κλειδιού</u>**

Όταν σκοπεύουμε να χρησιμοποιήσουμε την κρυπτογραφία για να προστατεύσουμε πληροφορίες, τότε θα πρέπει να δεχθούμε ότι οι άνθρωποι που προσπαθούμε να κρύψουμε την πληροφορία θα την αντιγράψουν και θα προσπαθήσουν να την αποκρυπτογραφήσουν με δυναμικές επιθέσεις.

Οι επιθέσεις κατά κρυπτογραφημένων πληροφοριών χωρίζονται σε τρεις κατηγορίες. Αυτές είναι:

- Επιθέσεις αναζήτησης κλειδιού.
- Επιθέσεις κρυπτανάλυσης.
- Επιθέσεις βασισμένες στο σύστημα κρυπτογράφησης.

I. <u>*Επιθέσεις αναζήτησης κλειδιού*</u>: Ο ευκολότερος τρόπος να «σπάσεις» έναν κώδικα, είναι να δοκιμάζεις όλα τα πιθανά κλειδιά το ένα μετά το άλλο. Οι περισσότερες προσπάθειες θα αποτύχουν, αλλά κάποια θα επιτύχει και είτε θα

επιτρέψει στον επιτιθέμενο να μπει στο σύστημα είτε θα του επιτρέψει να αποκρυπτογραφήσει το κρυπτογράφημα. Αυτές οι επιθέσεις ονομάζονται επιθέσεις αναζήτησης κλειδιού.
Οι αναζητήσεις κλειδιών δεν είναι πάντα αποτελεσματικές. Μερικές φορές δεν υπάρχει καμία πιθανότητα και αυτό γιατί υπάρχουν πάρα πολλά κλειδιά να δοκιμαστούν και δεν υπάρχει αρκετός χρόνος να δοκιμαστούν όλα.
Αντίθετα, υπάρχουν επιθέσεις που είναι αρκετά απλές γιατί οι περισσότεροι χρήστες διαλέγουν κλειδιά βασισμένα σε μικρούς κωδικούς, με χαρακτήρες που μπορούν να εκτυπωθούν.

II. *Επιθέσεις κρυπτανάλυσης:* Μια επίθεση κρυπτανάλυσης μπορεί να έχει δύο στόχους.: Την αποκρυπτογράφηση ενός κρυπτογραφημένου κειμένου, συνεπώς την ανακάλυψη του καθαρού κειμένου, και την εύρεση του κλειδιού με το οποίο κρυπτογραφήθηκε το κείμενο. Οι επιθέσεις που ακολουθούν χρησιμοποιούνται, γενικά, όταν ο κρυπτογραφικός αλγόριθμος είναι γνωστός .

a. Επίθεση γνωστού plaintext (αρχικό αρχείο): Σε αυτού του είδους την επίθεση ο κρυπταναλυτής έχει ένα κομμάτι από το αρχικό αρχείο και το αντίστοιχο κομμάτι του κρυπτογραφημένου αρχείου (ciphertext). Αν και αυτό ίσως φαίνεται απίθανο γεγονός, είναι αρκετά συχνό όταν η κρυπτογραφία χρησιμοποιείται για να προστατεύσει τα ηλεκτρονικά γράμματα ή τους σκληρούς δίσκους. Ο στόχος μιας επίθεσης γνωστού plaintext είναι να προσδιορίσει το κλειδί κρυπτογράφησης, το οποίο μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση άλλων μηνυμάτων.

b. Επίθεση επιλεγμένου plaintext (αρχικό κείμενο): Σε αυτού του είδους την επίθεση ο κρυπταναλυτής μπορεί να έχει την ευκαιρία να επιτεθεί κρυπτογραφώντας επιλεγμένα κομμάτια δεδομένων. Έτσι δημιουργείται ένα αποτέλεσμα το οποίο μπορεί μετά να το αναλύσει. Ο στόχος μιας τέτοιας

επίθεσης είναι να προσδιορίσει ένα κλειδί κρυπτογράφησης, το οποίο θα μπορεί να χρησιμοποιηθεί στην συνέχεια για να αποκρυπτογραφήσει άλλα μηνύματα.

c. Κρυπτανάλυση διαφορών: Είναι μια μορφή επίθεσης επιλεγμένου αρχικού κειμένου που ασχολείται με το να αποκρυπτογραφεί πολλά κείμενα που είναι ελαφρώς διαφοροποιημένα το ένα με το άλλο και να συγκρίνει τα αποτελέσματα.

III. *Επιθέσεις βασισμένες στο σύστημα κρυπτογράφησης*: Αποτελεί έναν άλλο τρόπο επίθεσης κατά τον οποίο δεν κάνουμε επίθεση στον κρυπτογραφικό αλγόριθμο αυτό καθεαυτό, αλλά στο σύνολο του κρυπτογραφικού συστήματος. Ένα καλό παράδειγμα τέτοιας επίθεσης είναι ο VC-I Video κρυπτογραφικός αλγόριθμος που χρησιμοποιούνταν για την δορυφορική μετάδοση προγράμματος τηλεόρασης παλαιότερα. Για πολλά χρόνια υπήρχαν πειρατές που πουλούσαν αποκωδικοποιητές που μπορούσαν να υποκλέψουν τα κλειδιά μεταφοράς και ύστερα να τα χρησιμοποιήσουν για να αποκρυπτογραφήσουν την μετάδοση.

## 2. Επιθέσεις στους αλγόριθμους δημοσίου κλειδιού.

Οι αλγόριθμοι δημοσίου κλειδιού είναι θεωρητικά πιο ευάλωτοι στις επιθέσεις, γιατί ο επιτιθέμενος έχει ένα αντίγραφο του δημοσίου κλειδιού που χρησιμοποιήθηκε για την κρυπτογράφηση του μηνύματος. Η δουλειά του επιτιθέμενου είναι ακόμα ευκολότερη γιατί το ίδιο το μήνυμα πιθανώς να υποδηλώνει με ποιόν αλγόριθμο έχει κρυπτογραφηθεί.

Οι επιθέσεις στους αλγόριθμους δημοσίου κλειδιού χωρίζονται σε δύο κατηγορίες:

- Επιθέσεις παραγοντοποίησης.
- Αλγοριθμικές επιθέσεις.

I. *Επιθέσεις παραγοντοποίησης*: Αυτού του είδους οι επιθέσεις είναι γνωστές για την ευκολία στην κατανόηση τους. Αποσκοπούν στην άντληση του προσωπικού κλειδιού από το αντίστοιχο δημόσιο κλειδί. Για την υλοποίηση αυτών των επιθέσεων χρειάζεται να επιλύσουμε διάφορα είδη μαθηματικών προβλημάτων.

II. *Αλγοριθμικές επιθέσεις:* Αποτελούν έναν άλλο τρόπο επίθεσης, για τον οποίο απαιτείται να βρεθεί ένα βασικό ελάττωμα ή αδυναμία του μαθηματικού προβλήματος στο οποίο είναι βασισμένο το σύστημα κρυπτογράφησης. Αυτό έχει γίνει περισσότερες από μια φορές στο παρελθόν.

## 2.8 Προγράμματα Κρυπτογράφησης.

Στην αγορά κυκλοφορούν πολλά προγράμματα κρυπτογράφησης σχεδιασμένα για να καλύπτουν συγκεκριμένες εφαρμογές. Τα πιο δημοφιλή, από αυτά είναι το S/MINE και το PGP που χρησιμοποιούνται στο ηλεκτρονικό ταχυδρομείο και το X.509 που είναι το πρότυπο κρυπτογράφησης για καταλόγους X.500.

### 2.8.1 S/MIME.

Το S/MIME (Secure/ Multipurpose Internet Mail Extensions) είναι βασισμένο στην τεχνολογία RSA και αναπτύχθηκε για την ασφαλή ανταλλαγή ηλεκτρονικών μηνυμάτων.

Για την καλύτερη κατανόηση του S/MIME θα πρέπει αρχικά να αναλύσουμε την παραδοσιακή μορφή του ηλεκτρονικού ταχυδρομείου RFC822

και στην συνέχεια το MIME δηλαδή την μορφή του e-mail που αποτελεί την βάση.

**RFC822.**

Το **RFC822** είναι το πρότυπο που καθορίζει την μορφή των μηνυμάτων πού στέλνονται μέσω ηλεκτρονικού ταχυδρομείου.

Τα μηνύματα κειμένου που στέλνονται εμφανίζονται ως ένας φάκελος ο οποίος περιέχει ότι πληροφορία χρειάζεται για να εκτελεστεί η μετάδοση και η παράδοση. Ο παραλήπτης θα λάβει μόνο τα περιεχόμενα που εμπεριέχουν μια σειρά από πεδία κεφαλίδων που μπορούν να χρησιμοποιηθούν από το σύστημα ταχυδρομείου για τη δημιουργία φακέλων.

Η δομή του μηνύματος που διαμορφώνει το RFC822 είναι πολύ απλή και παρουσιάζεται παρακάτω: Ένα μήνυμα αποτελείται από τον κορμό (body) και από την επικεφαλίδα (header). Στον κορμό υπάρχουν δεδομένα που προορίζονται για τον χρήστη, γραμμένα στην αγγλική γλώσσα ενώ στις επικεφαλίδες περιλαμβάνονται δεδομένα που χρησιμοποιεί το πρόγραμμα του χρήστη, είναι δηλαδή ένα ASCII κείμενο, και συνήθως αποτελείται από λέξεις όπως: from , to , subject και data. Μεταξύ τους διαχωρίζονται από μια κενή γραμμή. Συχνά χρησιμοποιείται και το πεδίο message ID, δηλαδή η ταυτότητα του μηνύματος .

**MIME .**

Στο πρότυπο αυτό περιέχονται οι βάσεις για το ηλεκτρονικό ταχυδρομείο οι οποίες καθιερώθηκαν το 1982 και τότε αποτελούσαν ότι πιο εξελιγμένο υπήρχε. Σύμφωνα με τις πρώτες τυποποιήσεις τα ηλεκτρονικά μηνύματα υπόκεινται στους εξής περιορισμούς :

¶ Μπορούν να περιέχουν μόνο ASCII χαρακτήρες.

¶ Δεν ξεπερνούν συγκεκριμένο μήκος.

¶ Έχουν προβλήματα μετάφρασης από ASCII σε EBCDIC.

¶ Δεν μπορούν:

- να μεταδώσουν εκτελέσιμα αρχεία ή άλλα δυαδικά αντικείμενα.
- να μεταδώσουν δεδομένα που περιέχουν χαρακτήρες ξένων γλωσσών.
- να χειριστούν δεδομένα που περιέχονται σε μηνύματα X.400.

Το MIME ως επέκταση του RFC822 είχε σκοπό να λύσει αυτά τα προβλήματα με τρόπο που να είναι σύμφωνος με την υπάρχουσα εφαρμογή ( RFC822).

Συγκεκριμένα ένα μήνυμα συμβατό του MIME περιέχει:

**Ü** Πολλαπλά αντικείμενα.

**Ü** Κείμενο με απεριόριστο μήκος γραμμών.

**Ü** Σύνολα χαρακτήρων πέρα από το US και ASCII επιτρέποντας την σύνταξη μηνυμάτων σε διάφορες γλώσσες.

**Ü** Εμπλουτισμένο κείμενο, χρήση δηλαδή διαφόρων τυπογραφικών στοιχείων.

**Ü** Εικόνα, κινούμενη εικόνα, ήχο.

**Ü** Δυαδικά αρχεία ή αρχεία εφαρμογών.

**Ü** Δείκτες σε αρχεία αποθηκευμένα σε άλλους υπολογιστές.

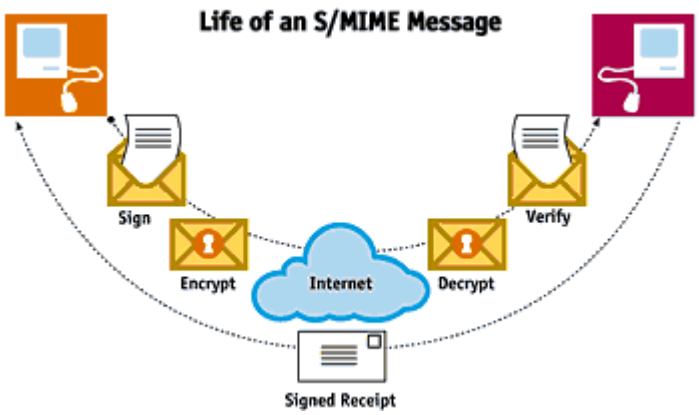
**Ü** Επίσης, ορίζονται πέντε καινούρια πεδία κεφαλίδας τα οποία παρέχουν πληροφορίες για το σώμα του μηνύματος .

Πίνακας επικεφαλίδων του MIME:

| **Επικεφαλίδες** | **Περιγραφή** |
|---|---|
| MIME-Version | Αριθμός έκδοσης το MIME |
| Content- type | Καθορίζει το είδος των δεδομένων που περιέχονται στο σώμα |
| Content–transfer- encoding | Η κωδικοποίηση των δεδομένων |
| Content-Id | Χρησιμοποιείται για να αναγνωρίσει τις ενότητες MIME |
| Content Description | Περιγραφή και ταυτοποίηση των δεδομένων |

**S/MIME.**

Το **S/MIME** είναι ένα πρωτόκολλο που χρησιμοποιείται από προγράμματα ηλεκτρονικού ταχυδρομείου για την εφαρμογή κρυπτογραφικών υπηρεσιών σε αποστέλλοντα μηνύματα και για την επεξεργασία προστατευμένων παραληφθέντων. Δίνει την δυνατότητα σε εταιρίες που σχεδιάζουν λογισμικό να αναπτύσσουν προγράμματα τέτοια ώστε ένα μήνυμα που κρυπτογραφήθηκε με ένα συγκεκριμένο πρόγραμμα να μπορεί να αποκρυπτογραφηθεί από ένα άλλο.




**Εικόνα 17:** Διαδικασία αποστολής μηνύματος με την χρήση του πρωτόκολλου S/MIME.

**Δημιουργία S/MIME μηνυμάτων.**

Τα μηνύματα S/MIME είναι συνδυασμός MIME μηνυμάτων και CMS αντικειμένων. Τα CMS αντικείμενα περιγράφουν το είδος της ασφάλειας που θέλουμε να εφαρμόσουμε και μπορεί να είναι Ψηφιακός Φάκελος (Enveloped-Data), Υπογεγραμμένα δεδομένα (Signed-Data) και άλλα. Μπορούν να χρησιμοποιηθούν όλοι οι τύποι δεδομένων του MIME χωρίς κανένα περιορισμό. Το MIME μήνυμα, μαζί με άλλες πληροφορίες (πιστοποιητικά, αναγνωριστικά αλγορίθμων κ.α.), επεξεργάζεται από τις διαδικασίες του CMS και παράγεται το CMS αντικείμενο, το οποίο τυλίγεται σε εξωτερικό MIME μήνυμα με κατάλληλες επικεφαλίδες.

**Προετοιμασία για την δημιουργία μηνυμάτων S/MIME.**

Η MIME οντότητα που θα ασφαλιστεί από το S/MIME μπορεί να είναι είτε μέρος ενός μηνύματος, είτε ολόκληρο μήνυμα. Σε περίπτωση που η MIME οντότητα ισοδυναμεί με ολόκληρό το μήνυμα, περιλαμβάνονται σ' αυτήν όλες οι MIME επικεφαλίδες (δεν περιλαμβάνονται οι επικεφαλίδες του RFC822) και φυσικά τα περιεχόμενα.

Η διαδικασία που προετοιμάζει το μήνυμα/οντότητα για επεξεργασία από το CMS αποτελείται από 3 βασικά βήματα:

**1.** Η MIME οντότητα κατασκευάζεται σύμφωνα με τις υποδείξεις του τοπικού περιβάλλοντος. Το σύνολο των χαρακτήρων και οι χαρακτήρες οριοθέτησης γραμμών καθορίζονται από το τοπικό σύστημα.

**2.** Η MIME οντότητα μετατρέπεται σε κανονική μορφή που είναι διεθνώς αναγνωρίσιμη, παρουσιάσιμη και ανεξάρτητη από την πλατφόρμα του εκάστοτε χρήστη. Ανάλογα με τον τύπο των δεδομένων διαφέρουν οι ενέργειες που πρέπει να γίνουν ώστε να προκύψει αυτή η μορφή.

**3.** Εφαρμόζεται κατάλληλη κωδικοποίηση μεταφοράς. Απαιτείται όλες οι MIME οντότητες που πρόκειται να ασφαλιστούν με το S/MIME να είναι σε

κωδικοποίηση 7bit για τη σίγουρη και σωστή μεταφορά τους. Αυτό συμβαίνει γιατί δεν είναι βέβαιο κατά πόσο υποστηρίζεται η μεταφορά μηνυμάτων με κωδικοποίηση 8bit ή binary σε όλο το μονοπάτι από τον αποστολέα στον παραλήπτη. Για αυτό το λόγο οι μηχανισμοί Quoted-Printable και Base64 είναι απαραίτητοι.

**Τύποι περιεχομένων S/MIME.**

**1. Enveloped Data:** (Δεδομένα σε φάκελο). Αποτελείται από κρυπτογραφημένα περιεχόμενα οποιουδήποτε τύπου και κρυπτογραφημένα κλειδιά-κρυπτογράφησης για έναν ή περισσότερους αποδέκτες. Ο συνδυασμός των κρυπτογραφημένων περιεχομένων και του κρυπτογραφημένου κλειδιού, είναι ένας "ψηφιακός φάκελος".

Για την επικοινωνία του κλειδιού-κρυπτογράφησης υπάρχουν τρεις (3) τεχνικές για κάθε παραλήπτη και μπορεί να χρησιμοποιηθεί οποιαδήποτε από αυτές:

Ñ key transport: (κλειδί μεταφοράς) το κλειδί κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη.
Ñ key agreement: (κλειδί συμφωνίας) το δημόσιο κλειδί τού παραλήπτη και το ιδιωτικό κλειδί τού αποστολέα χρησιμοποιούνται για να παράγουν (μέσω κατάλληλου αλγόριθμου) ένα συμμετρικό κλειδί, το οποίο κρυπτογραφεί το κλειδί κρυπτογράφησης.
Ñ symmetric key-agreement: το κλειδί-κρυπτογράφησης, κρυπτογραφείται με το συμμετρικό κλειδί που έχει πρωτύτερα διανεμηθεί.

Η διαδικασία κατασκευής των ψηφιακών φακέλων είναι:

**1.** Παράγεται το τυχαίο κλειδί κρυπτογράφησης.

**2.** Για κάθε παραλήπτη κρυπτογραφείται το κλειδί-κρυπτογράφησης.

**3.** Το κρυπτογραφημένο κλειδί και άλλες πληροφορίες που αφορούν κάθε παραλήπτη συλλέγονται στο πεδίο RecipientInfo. Το RecipientInfo, όπως και το SignerInfo, περιέχει τα πιστοποιητικά κάθε χρήστη, την τεχνική που χρησιμοποιήθηκε, τους αλγόριθμους και το κρυπτογραφημένο κλειδί.

**4.** Τα περιεχόμενα κρυπτογραφούνται με το κλειδί-κρυπτογράφησης.

**5.** Τα πεδία RecipientInfo για όλους τους παραλήπτες μαζί με τα κρυπτογραφημένα περιεχόμενα αποτελούν το αντικείμενο Enveloped Data.

Ο εκάστοτε παραλήπτης αφού ανακτήσει το κρυπτογραφημένο κλειδί ακολουθώντας την τεχνική που υποδεικνύεται στο RecipientInfo πεδίο, αποκρυπτογραφεί τα περιεχόμενα του μηνύματος.

**2. Signed Data.** Αποτελείται από περιεχόμενα οποιουδήποτε τύπου και κάποιες από τις υπογραφές αυτών. Τα περιεχόμενα μπορούν να υπογραφούν παράλληλα από πολλούς χρήστες. Η τυπική εφαρμογή αυτού του τύπου είναι για την υπογραφή απλών δεδομένων ή για την μεταφορά πιστοποιητικών.

Η διαδικασία σύμφωνα με την οποία κατασκευάζονται τα υπογεγραμμένα δεδομένα έχει ως εξής:

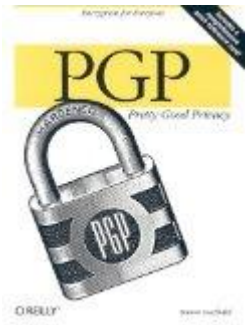
· Για κάθε υπογράφοντα παράγεται η συνοπτική τιμή (digest value) των περιεχομένων βάση αλγορίθμου, που εξαρτάται από τον υπογράφοντα. Εάν μαζί με τα περιεχόμενα υπογράφονται και συγκεκριμένες ιδιότητες, τότε παράγεται η digest value των περιεχομένων και η οποία εισάγεται σε ειδικό πεδίο, που ανήκουν οι προς υπογραφή ιδιότητες και το τελικό message digest είναι η digest value των ιδιοτήτων.

· Το message digest που προκύπτει από το προηγούμενο βήμα κρυπτογραφείται με το ιδιωτικό κλειδί κάθε υπογράφοντα ξεχωριστά.

· Για κάθε υπογράφοντα, το αποτέλεσμα της υπογραφής και άλλες πληροφορίες σχετικές με αυτόν συλλέγονται στο πεδίο SignerInfo. Το πεδίο αυτό υπάρχει μια φορά για κάθε χρήστη και αποτελείται από καταχωρήσεις που περιλαμβάνουν τα πιστοποιητικά της ταυτότητας του χρήστη, το δημόσιο κλειδί του, τους αλγόριθμους που χρησιμοποιήθηκαν και την υπογραφή του.

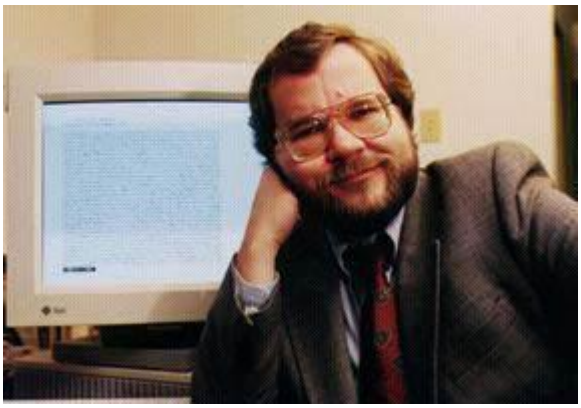
· Όλα τα πεδία SignerInfo, τα περιεχόμενα και επιπλέον πληροφορίες συλλέγονται και φτιάχνουν το αντικείμενο SignedData.

Ο παραλήπτης του μηνύματος υπολογίζει το message digest των περιεχομένων και με το δημόσιο κλειδί του αποστολέα ανακτά το κρυπτογραφημένο message digest που παρέλαβε με το μήνυμα. Συγκρίνει αυτά τα δύο, και εάν είναι ταυτόσημα, επαληθεύει επιτυχώς την υπογραφή.




## 2.8.2 PGP.

Το PGP είναι η ανακάλυψη του Phil Zimmermann (εικόνα 18) που κυκλοφόρησε στο Internet τον Ιούνιο του 1991. Είναι ένα ολοκληρωμένο σύστημα που προσφέρει προστασία των e-mails και των αρχείων γενικότερα. Επίσης, είναι ένα σύνολο από standards που περιγράφουν τα formats των κρυπτογραφημένων μηνυμάτων, των κλειδιών και των ψηφιακών υπογραφών.



**Εικόνα 18**: Ο δημιουργός του πρωτοκόλλου PGP Phil Zimmermann.

Ο Zimmermann για την δημιουργία του PGP έκανε τα ακόλουθα:

**R** Επέλεξε τους καλύτερους διαθέσιμους κρυπτογραφικούς αλγόριθμους ως βάση για εξέλιξη.

**R** Ολοκλήρωσε αυτούς τους αλγόριθμους σε μια εφαρμογή γενικού σκοπού η οποία είναι ανεξάρτητη από λειτουργικό σύστημα και επεξεργαστή, ενώ είναι βασισμένη σε μια μικρή σειρά από εντολές οι οποίες είναι εύκολες να χρησιμοποιηθούν.

**R** Έφτιαξε το πακέτο και την τεκμηρίωση του, περιλαμβάνοντας bulleting boards και εμπορικά δίκτυα, όπως το AOL (America On Line).

**R** Εισήλθε σε συμφωνία με μία εταιρία (Viacrypt now New Associates) για να δημιουργήσει μια ολοκληρωμένη, σύμφωνη και χαμηλού κόστους έκδοση του PGP.

Το PGP έχει αναπτυχθεί δραματικά και πλέον χρησιμοποιείται ευρέως. Αυτό μπορεί να οφείλεται σε πολλούς παράγοντες . Όπως:

**1.** Είναι διαθέσιμο δωρεάν, σε όλο τον κόσμο, σε εκδόσεις που λειτουργούν σε διάφορα platforms, συμπεριλαμβάνοντας το windows, UNIX, Macintosh και άλλα.

**2.** Η εμπορική έκδοση ικανοποιεί χρήστες οι οποίοι θέλουν ένα προϊόν που συνοδεύεται από υποστήριξη πώλησης.

**3.** Είναι βασισμένο σε αλγόριθμους οι οποίοι έχουν θεωρηθεί άκρως ασφαλείς. Συγκεκριμένα, το πακέτο παρέχεται:

- για κρυπτογράφηση δημόσιου κλειδιού RSA, DSS και Diffle-Helman
- για συμμετρική κρυπτογραφία CAST-128, IDEA και 3DES
- για μυστική κωδικοποίησης SHA-1.

**4.** Το πεδίο εφαρμογής του περιλαμβάνει :

- εταιρίες που επιθυμούν να επιλέξουν και να επιβάλλουν ένα τυποποιημένο σχέδιο για κρυπτογράφηση αρχείων και μηνυμάτων
- μεμονωμένα άτομα που επιθυμούν να επικοινωνήσουν με ασφάλεια μέσω internet και άλλων δικτύων.

**5.** Δεν έχει αναπτυχθεί ούτε ελέγχεται από καμία κυβέρνηση ή επίσημη οργάνωση.

Για αυτούς που ενστικτωδώς δεν εμπιστεύονται «το κατεστημένο» το PGP να είναι πολύ ελκυστικό .

Η ακριβής λειτουργία του PGP, στην διαχείριση των κλειδιών, αποτελείται από τις υπηρεσίες: πιστοποίηση, εμπιστευτικότητα, συμπίεση, τμηματοποίηση και συναρμολόγηση.

þ **Πιστοποίηση.** Για να πραγματοποιηθεί η πιστοποίηση του PGP πρέπει να ακολουθηθεί η εξής διαδικασία:

**1.** Ο αποστολέας δημιουργεί ένα μήνυμα.

**2.** Το SHA-1 χρησιμοποιείται για να παράγει ένα μυστικό κωδικό 160-bits.

**3.** Ο μυστικός κωδικός κρυπτογραφείται με τον αλγόριθμο RSA χρησιμοποιώντας το ιδιωτικό κλειδί του αποστολέα και το αποτέλεσμα ενσωματώνεται στο μήνυμα.

**4.** Ο παραλήπτης χρησιμοποιεί τον αλγόριθμο RSA και το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφήσει και να ανακτήσει τον μυστικό κωδικό.

**5.** Ο παραλήπτης παράγει ένα καινούριο μυστικό κωδικό για το μήνυμα και τον συγκρίνει με το αποκρυπτογραφημένο μυστικό κωδικό. Αν αυτοί οι δύο ταιριάζουν, το μήνυμα γίνεται αποδεκτό ως αυθεντικό.

Κάθε μήνυμα ή αρχείο πρέπει να φέρει και μια υπογραφή. Υπάρχουν δύο είδη υπογραφών:

1)Προσκολλημένες υπογραφές που όπως λέει και το όνομα τους είναι κολλημένες πάνω στο αρχείο –μήνυμα

2)Αμερόληπτες υπογραφές. Οι οποίες μπορούν:

-να αποθηκευτούν και να μεταδοθούν από το μήνυμα που υπογράφουν. Αυτό εξυπηρετεί πολλές περιπτώσεις, όπως όταν ένας χρήστης επιθυμεί να διατηρήσει μια ξεχωριστή καταγραφή υπογραφών όλων των μηνυμάτων που στάλθηκαν ή ελήφθησαν.

-να διακρίνουν μέσα από ένα εκτελέσιμο πρόγραμμα μεταγενέστερες μολύνσεις από ιούς.

- να χρησιμοποιηθούν στην περίπτωση που περισσότερες από μία ομάδες πρέπει να υπογράψουν ένα έγγραφο, όπως ένα νομικό συμβόλαιο.

Τρόποι που μπορούν να παραχθούν υπογραφές:

- Με την χρήση του αλγόριθμου RSA. Λόγω της δύναμής του, ο παραλήπτης επιβεβαιώνει ότι μόνο ο κάτοχος του αντίστοιχου ιδιωτικού κλειδιού μπορεί να παράγει την υπογραφή.
- Με την χρήση του αλγόριθμου SHA-1. Η δυναμική του αλγόριθμου αυτού βεβαιώνει τον παραλήπτη ότι κανένας άλλος δεν μπορεί να παράγει

καινούριο μήνυμα που να αντιστοιχεί στο μυστικό κωδικό και φυσικά ούτε στην υπογραφή του πρωτότυπου μηνύματος.

- Εναλλακτικά υπογραφές μπορούν να παραχθούν χρησιμοποιώντας DSS/SHA-1.

þ **Εμπιστευτικότητα**. Η υπηρεσία αυτή παρέχεται μέσω κρυπτογραφικών μηνυμάτων τα οποία είτε μεταδίδονται είτε αποθηκεύονται τοπικά ως αρχεία. Και στις δύο περιπτώσεις μπορεί να χρησιμοποιηθεί ο συμμετρικός αλγόριθμος κρυπτογραφίας CAST-128 (εναλλακτικά οι αλγόριθμοι IDEA ή DES) .

Τι προσφέρει η εμπιστευτικότητα: Η εμπιστευτικότητα έρχεται να δώσει λύση στο πρόβλημα της διανομής του κλειδιού που αναλύεται παρακάτω:
Στο PGP κάθε συμμετρικό κλειδί χρησιμοποιείται μόνο μια φορά. Δηλαδή, κάθε φορά που επρόκειτο να σταλεί ένα μήνυμα με την βοήθεια ενός τυχαίου αριθμού των 128bit δημιουργείται ένα νέο κλειδί, το κλειδί συνόδου ή αλλιώς κλειδί μιας χρήσεως. Το κλειδί αυτό μεταδίδεται προσκολλημένο στο μήνυμα και για να είναι ασφαλής η μεταφορά του, είναι αναγκαία η κρυπτογράφηση του με το δημόσιο κλειδί του παραλήπτη.

Συνοπτικά η διαδικασία είναι η εξής:

1. Ο αποστολέας παράγει:
   - ένα μήνυμα το οποίο κρυπτογραφείται με τον αλγόριθμο CAST-128 (ή IDEA ή 3DES)
   - ένα κλειδί με τον τρόπο που προαναφέρθηκε ,το οποίο κρυπτογραφείται με το RSA χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη.
2. Το κλειδί προσκολλημένο με το μήνυμα αποστέλλεται στον παραλήπτη
3. Ο παραλήπτης αποδέχεται το μήνυμα και το κλειδί συνόδου. Με το ιδιωτικό του κλειδί και την βοήθεια του RSA αποκρυπτογραφεί το κλειδί συνόδου, με το οποίο στην συνέχεια αποκρυπτογραφεί το μήνυμα.

þ **Εμπιστευτικότητα και Πιστοποίηση.** Και οι δύο αυτές υπηρεσίες μπορούν να χρησιμοποιηθούν για το ίδιο μήνυμα. Δηλαδή, ένα μήνυμα μπορεί να σταλεί και με υπογραφή και με το κλειδί συνόδου (οι υπόλοιπες διαδικασίες είναι ίδιες).

þ **Συμπίεση.** Το PGP συμπιέζει το μήνυμα μετά την εφαρμογή της υπογραφής και πριν την κρυπτογράφηση. Με αυτό τον τρόπο εξοικονομεί χώρο για την μετάδοση του e-mail και για την αποθήκευση του αρχείου. Όπως είναι λογικό η αποκρυπτογράφηση του κειμένου εφαρμόζεται μετά την συμπίεση ενισχύοντας την ασφάλειας της κρυπτογράφησης. Αυτό συμβαίνει γιατί το συμπιεσμένο μήνυμα έχει λιγότερο περίσσευμα από το αυθεντικό απλό κείμενο, έτσι η κρυπτανάλυση γίνεται πιο δύσκολη.

Η υπογραφή παράγεται πριν την συμπίεση για δύο λόγους:

**1.** Είναι προτιμότερο είναι να υπογράφεται ένα μη συμπιεσμένο μήνυμα. Έτσι κάποιος μπορεί να αποθηκεύσει μόνο το μη συμπιεσμένο μήνυμα μαζί με την υπογραφή για μελλοντική επαλήθευση. Αντίθετα, αν κάποιος υπογράψει ένα συμπιεσμένο μήνυμα τότε είναι απαραίτητο να αποθηκεύσει και μια συμπιεσμένη έκδοση του μηνύματος για τυχούσα μελλοντική επαλήθευση .

**2.** Ακόμη, αν κάποιος ήθελε να παράγει δυναμικά ένα ξανασυμπιεσμένο μήνυμα για επαλήθευση, η συμπίεση του αλγόριθμου PGP θα ήταν δύσκολη. Ο αλγόριθμος δεν είναι καθοριστικός, διάφορες εφαρμογές του αλγόριθμου πετυχαίνουν διαφορετικά αποτελέσματα.

þ **Τμηματοποίηση και Συναρμολόγηση.** Το e-mail έχει ανώτατο όριο μεγέθους μηνύματος . Για παράδειγμα σε πολλές εφαρμογές, στις οποίες μπορεί να έχεις πρόσβαση μέσω internet, επιβάλλουν μέγιστο μέγεθος 50000

octets. Αν το μήνυμα είναι μεγαλύτερο απ' αυτό πρέπει να σπάσει σε μικρότερα τμήματα το καθένα απ' τα οποία ταχυδρομείται ξεχωριστά.

Για να διευκολυνθεί αυτός ο περιορισμός, το PGP αυτόματα διαιρεί το μήνυμα που είναι πολύ μεγάλο σε τμήματα που είναι αρκετά μικρά έτσι ώστε να μπορούν να σταλούν μέσω e-mail. Η τμηματοποίηση γίνεται κατόπιν όλων των άλλων διαδικασιών, συμπεριλαμβάνοντας και την μετατροπή radix-64. Το κομμάτι του κλειδιού συνόδου και το κομμάτι τις υπογραφής εμφανίζονται μια φορά μόνο στην αρχή του πρώτου τμήματος. Στο τέλος της λήψης το PGP πρέπει να αφαιρέσει τις κεφαλίδες και να συναρμολογήσει όλο το μπλοκ.

**Σημείωση:** Αξίζει να αναφερθεί ότι ο εμπνευστής του, Phil Zimmermann, σύρθηκε στα δικαστήρια από το FBI με την κατηγόρια της παράνομης εξαγωγής όπλων (!!), αφού στις Η.Π.Α. η ισχυρή κρυπτογραφία θεωρείται όπλο, αλλά τελικά δεν καταδικάστηκε γιατί το δικαστήριο δεν μπόρεσε να οριοθετήσει σαφώς την έννοια της εξαγωγής στα πλαίσια του Internet.

### 2.8.3 X.509.

Το X.509 είναι ένα πρότυπο κρυπτογράφησης το οποίο είναι βασισμένο στην χρήση δημοσίων κλειδιών και ψηφιακών υπογραφών. Κατά τη χρήση του δεν επιβάλει ένα συγκεκριμένο αλγόριθμο αλλά συνιστά το RSA. Σχεδιάστηκε για να παρέχει την υποδομή πιστοποίησης στις υπηρεσίες καταλόγου του πρωτοκόλλου X.500. Το πρωτόκολλο αυτό αποτελεί μια ιεραρχική μέθοδο οργάνωσης ευρετηρίων, σχεδιάστηκε από το Διεθνή Οργανισμό Τυποποίησης (International Standards Organization-ISO) και ενσωματώθηκε στο διαδικτυακό πρωτόκολλο LDAP (Lightweight Directory Access Protocol).

| **Version** |
| --- |
| **Serial Number** |
| **Algorithm Identifier** |
| **Issuer** |
| **Period of Validity:**<br>-Not Before Date<br>-Not After Date |
| **Subject** |
| **Subject's Public Key**<br>-Algorithm<br>-Parameters<br>-Public Key |
| **Signature** |

**Εικόνα 19:** Η δομή ενός τυπικού X.509 πιστοποιητικού.

Το X.509 πιστοποιητικό περιλαμβάνει έναν αριθμό έκδοσης, ένα σειριακό αριθμό, πληροφορίες ταυτότητας, πληροφορίες σχετικά με τον αλγόριθμο και την υπογραφή της αρχής που το εκδίδει. Στην παραπάνω εικόνα (εικόνα 19) βλέπουμε την δομή ενός τυπικού X.509 πιστοποιητικού.

Το X. 509 βασίζεται στο πιστοποιητικό δημοσίου κλειδιού για κάθε χρήστη. Αυτό το πιστοποιητικό όπως έχουμε αναφέρει δημιουργείται από μια έμπιστη αρχή πιστοποίησης (CA- Certification Authority) και τοποθετείται σε κατάλογο από την CA ή από τον χρήστη. Ο server καταλόγου δεν είναι υπεύθυνος για την δημιουργία δημόσιων κλειδιών ή για την λειτουργία πιστοποίησης, απλώς παρέχει εύκολη πρόσβαση για να βλέπουν οι χρήστες πιστοποιητικά.

**Διαδικασίες πιστοποίησης.**

Το X.509 συμπεριλαμβάνει τρεις εναλλακτικές διαδικασίες πιστοποίησης που χρησιμοποιούν υπογραφές δημοσίου κλειδιού και έχουν σκοπό να χρησιμοποιηθούν για διάφορες εφαρμογές.

Σημείωση: Θεωρείται ότι και οι δύο πλευρές ξέρουν το δημόσιο κλειδί είτε παρατηρώντας τα πιστοποιητικά τους είτε από τον κατάλογο είτε επειδή το πιστοποιητικό συμπεριλαμβάνεται στα αρχικό μήνυμα.

**I. Πιστοποίηση μιας κατεύθυνσης.**

Η πιστοποίηση μιας κατεύθυνσης πραγματοποιείται με την μετάδοση πληροφοριών από τον χρήστη (A), στον χρήστη (B) και επιβεβαιώνει τα ακόλουθα:

¶ Την ταυτότητα του A

¶ Ότι το μήνυμα προήλθε από τον A.

¶ Ότι το μήνυμα προοριζόταν για τον B.

¶ Την ακεραιότητα και την αυθεντικότητα του μηνύματος (ότι δεν έχει σταλεί πολλές φορές ).

Το μήνυμα θα πρέπει να πληροί τις εξής προϋποθέσεις:

1) Να περιέχει την ημερομηνία έναρξης και λήξης (timestamp), έτσι ώστε να μπορούμε να γνωρίζουμε την καθυστέρηση στην διανομή μηνυμάτων.

2)Να περιέχει μια τιμή norce η οποία θα πρέπει να είναι μοναδική κατά την ημερομηνία λήξης του μηνύματος. Έτσι ο B αποθηκεύοντας την, μπορεί να απορρίπτει τα μηνύματα με την ίδια τιμή και να αποφύγει την επανάληψή της.

3) Να περιέχει την ταυτότητα του B.

4)Να είναι υπογεγραμμένο με το ιδιωτικό κλειδί του A.

## II. Πιστοποίηση Δύο Κατευθύνσεων.

Η πιστοποίηση δύο κατευθύνσεων επιτρέπει και στις δύο πλευρές να επικοινωνούν για να επαληθεύσουν την ταυτότητα η μία της άλλης. Πιστοποιεί τα ακόλουθα:

**1.** Την ταυτότητα του Β.

**2.** Ότι το μήνυμα απάντησης προήλθε από τον Β.

**3.** Ότι το μήνυμα προορίζεται για τον Α.

**4.** Την ακεραιότητα και αυθεντικότητα της απάντησης.

Το μήνυμα - απάντηση περιέχει:

· μία τιμή- norce από τον Α για να αξιολογήσει την απάντηση.

· την ημερομηνία έναρξης και λήξης (timestamp) και

· μία τιμή- norce που προέρχεται από τον Β.

## III. Πιστοποίηση τριών κατευθύνσεων.

Αυτή η διαδικασία δεν διαφέρει πολύ από τις προηγούμενες, απλά συμπεριλαμβάνει ένα ακόμα μήνυμα από τον Α στον Β το οποίο βοηθάει στο να αποφευχθούν οι επαναλήψεις των μηνυμάτων.

## 2.9 Πρωτόκολλα ασφαλείας.

### 2.9.1 Πρωτόκολλο SSL- Secure Sockets Layer.

Το SSL της Netscape Communications αποτελεί ένα αναγνωρισμένο πρωτόκολλο ασφαλούς επικοινωνίας στο web που έκανε την εμφάνισή του το 1994 και χρησιμοποιείται για την αποστολή εμπιστευτικών δεδομένων (π.χ. στοιχεία πιστωτικών καρτών). Πιο συγκεκριμένα, προστατεύει το κανάλι επικοινωνίας λειτουργώντας στα χαμηλά επίπεδα του μοντέλου διαστρωμάτωσης δικτύου (ISO), μεταξύ του επιπέδου εφαρμογών και του επιπέδου TCP/IP μετάδοσης. Συμπερασματικά, είναι ανεξάρτητο της εφαρμογής και κατά συνέπεια δέχεται την προσκόλληση άλλων πρωτοκόλλων πάνω του. Τα πρωτόκολλα αυτά είναι τα: HTTP (Hypertext Transfer Protocol), Telnet και FTP (File Transfer Protocol).

Το SSL αρχικά χρησιμοποιεί τεχνικές ασύμμετρης κρυπτογράφησης, ώστε να επιτευχθούν οι ακόλουθοι στόχοι:

1. Ο εξυπηρετητής αυθεντικοποιείται μέσω ψηφιακών πιστοποιητικών.
2. Η κοινή συμφωνία μεταξύ εξυπηρετητή και πελάτη για τη χρήση ενός συγκεκριμένου κλειδιού συνόδου, με το οποίο θα κρυπτογραφηθεί το υπόλοιπο της συναλλαγής. Όσο μεγαλύτερο είναι το μήκος του κλειδιού συνόδου τόσο πιο δύσκολη είναι η αποκρυπτογράφησή του.

Σε γενικές γραμμές το κλειδί συνόδου κρυπτογραφείται με το δημόσιο κλειδί του εξυπηρετητή, στέλνεται στον πελάτη και διαφέρει από σύνδεση σε σύνδεση. Η ηλεκτρονική επιχείρηση ή ο αντίστοιχος πάροχος υπηρεσιών internet (Internet Service Provider) για να καταφέρουν να χρησιμοποιήσουν το SSL πρωτόκολλο θα πρέπει να τοποθετήσουν τις web σελίδες σε έναν SSL ασφαλή εξυπηρετητή. Ο φυλλομετρητής και ο εξυπηρετητής, που θα

συνδεθούν σε μια SSL σύνοδο και θα πιστοποιηθούν, θα καθορίζουν το μήκος των δεδομένων που θα μεταδοθούν καθώς και την τεχνική κρυπτογράφησης που θα χρησιμοποιηθεί.

Το SSL πρωτόκολλο χρησιμοποιεί συμμετρικούς αλγορίθμους κρυπτογράφησης όπως είναι οι: RC2/RC4 για την έκδοση SSLv2, ενώ στην έκδοση SSLv3 παρέχονται και οι RC4 128 bits και Triple- DES. Όμως, το πρωτόκολλο αυτό έχει ένα πολύ σημαντικό μειονέκτημα: επιβραδύνει την επικοινωνία στο διαδίκτυο λόγω της κρυπτογράφησης- αποκρυπτογράφησης που απαιτείται από την αρχή της διαδικασίας.

### 2.9.2 Το πρωτόκολλο S-HTTP.

Το S-HTTP αποτελεί επέκταση του HTTP με στόχο την παροχή ασφάλειας. Το HTTP χρησιμοποιείται για τη μετάδοση και τη λήψη δεδομένων στο web και οι σχεδιαστές του δεν ήταν δυνατό να προβλέψουν ότι πάνω σε αυτό θα μπορούσε να στηριχθεί το ηλεκτρονικό εμπόριο, συνεπώς δεν διαθέτει την κατάλληλη υποδομή να εκμεταλλευτεί το δημόσιο κλειδί, αλλά ούτε να ενσωματώσει τεχνικές κρυπτογράφησης. Τα HTTP μηνύματα αποτελούνται από μια σειρά επικεφαλίδων, μια κενή γραμμή και ένα σώμα. Είναι ευθύνη του εξυπηρετητή να μορφοποιήσει την απάντηση με τρόπο που να καταλαβαίνει ο φυλλομετρητής. Φυσικά, οποιαδήποτε συσκευή ανήκει στο δίκτυο μπορεί να αποκτήσει την πληροφορία καθώς αυτή διέρχεται. Στο σημείο αυτό κάνει την εμφάνισή του το S-HTTP ώστε να διευθετήσει αυτό ακριβώς το πρόβλημα.

Στην ουσία σε ένα S-HTTP μήνυμα περιλαμβάνεται οποιαδήποτε έκδοση HTTP μηνύματος! Γενικά, σε μια σύνοδο (σύνδεση) ο εξυπηρετητής και ο πελάτης συμφωνούν σε μια κρυπτογραφική μέθοδο και ο τελευταίος στέλνει το δημόσιο κλειδί του. Ο εξυπηρετητής δημιουργεί ένα κλειδί συνόδου και το κρυπτογραφεί με το δημόσιο κλειδί του πελάτη. Όταν δεχτεί το κλειδί συνόδου ο πελάτης αποκρυπτογραφεί το μήνυμα ώστε να αποκτήσει το κλειδί. Στη

συνέχεια ο πελάτης και ο εξυπηρετητής ανταλλάσσουν τις επόμενες αιτήσεις και αποκρίσεις κρυπτογραφημένες με το κλειδί συνόδου.

Τέλος, το S-HTTP υποστηρίζει ψηφιακά πιστοποιητικά και ψηφιακές υπογραφές από την πλευρά του εξυπηρετητή, σε αντίθεση με το HTTP που οι σύνοδοι μένουν ζωντανές μέχρι ο φυλλομετρητής να ζητήσει τον τερματισμό τους.

### 2.9.3 Το πρωτόκολλο SET (Secure Electronic Transactions).

Αναπτύχθηκε από τη συνεργασία των Visa, Master Card, Microsoft, IBM, Netscape και ένα σύνολο άλλων οργανισμών το 1996 για να προσφέρει ασφάλεια στις συναλλαγές με πιστωτική κάρτα στο διαδίκτυο. Σε αντίθεση με το SSL που είναι πρωτόκολλο γενικού σκοπού, το SET(Secure Electronic Transactions) είναι εξειδικευμένο και διασφαλίζει τη ροή της επικοινωνίας μεταξύ των διαφόρων συμμετεχόντων στην ηλεκτρονική συναλλαγή. Το SET χρησιμοποιεί ψηφιακές υπογραφές και πιστοποιητικά, δημόσια και ιδιωτικά κλειδιά, αλλά και το SSL στο σχήμα ασφαλείας του, αφού πρέπει να εξασφαλίσει ένα τεράστιο σύνολο απαιτήσεων στη διεξαγωγή του ηλεκτρονικού εμπορίου (π.χ. την αυθεντικοποίηση του κατόχου μιας πιστωτικής κάρτας, την εμπιστευτικότητα των ηλεκτρονικών πληρωμών, την ακεραιότητα των δεδομένων, τη διασφάλιση βέλτιστων πρακτικών ασφαλείας για όλα τα εμπλεκόμενα μέρη κ.λπ.).

Εκτενέστερα, παρέχει τις ακόλουθες βασικές υπηρεσίες:

- μη αποποίηση της ευθύνης: το SET είναι πρωτόκολλο βασισμένο σε ψηφιακές υπογραφές, με αποτέλεσμα να έχει τη δυνατότητα να αποδεικνύει την προέλευση, την μετάδοση και την παράδοση των δεδομένων. Τώρα πια δεν δημιουργούνται παρεξηγήσεις του τύπου «αποποίηση της παραγγελίας»!

- πιστοποίηση: ο κάτοχος της πιστωτικής κάρτας, η τράπεζα που την έχει εκδώσει, ο πωλητής και η τράπεζα που διαχειρίζεται το λογαριασμό που καταθέτουν ψηφιακά πιστοποιητικά και υπογραφές συντελούν για την αυθεντικοποίηση των στοιχείων που δίνονται στο σύστημα.
- ακεραιότητα: τα στοιχεία της συναλλαγής είναι κρυπτογραφημένα με αποτέλεσμα να είναι «αδύνατη» η τροποποίησή τους, όπως για παράδειγμα η μεταβολή του ποσού συναλλαγής.
- εμπιστευτικότητα: τα χαρακτηριστικά της πιστωτικής κάρτας του πελάτη μεταβιβάζονται στη SET πύλη πληρωμών για έλεγχο της εγκυρότητάς τους, έτσι ώστε ο πωλητής να προχωρήσει, με σιγουριά πια, στην ολοκλήρωση της συναλλαγής.

Οι προδιαγραφές του πρωτοκόλλου SET απαιτούν την εγκατάσταση ειδικού λογισμικού στον ηλεκτρονικό υπολογιστή τόσο του πελάτη όσο και του εμπόρου. Επίσης, υπάρχει λογισμικό στην πλευρά του πωλητή για να αποκρυπτογραφεί τις πληροφορίες οικονομικής φύσεως και στην πλευρά της αρχής πιστοποίησης για να εκδίδει ψηφιακά πιστοποιητικά. Η κρυπτογράφηση δημοσίου κλειδιού χρησιμοποιείται για να προστατεύει τον αριθμό της πιστωτικής κάρτας. Δημόσια και ιδιωτική κρυπτογράφηση, αυθεντικοποίηση μηνύματος και πιστοποίηση κλειδιού, είναι τα βασικά χαρακτηριστικά του SET προτύπου.

## 2.10 Το μέλλον της κρυπτογραφίας.

Οι σημερινές τεχνολογίες κρυπτογράφησης, παρότι παρέχουν μεγάλο ποσοστό ασφάλειας έχει αποδεχθεί ότι δεν είναι άτρωτες. Την λύση στο πρόβλημα αυτό έρχεται να δώσει η **Κβαντική κρυπτογραφία.**

Το Κβαντικό Σύστημα Κρυπτογραφίας επιτρέπει τη μυστικότητα του κλειδιού και εγγυάται ότι κανένας ισχυρός υπολογιστής ή χακερ δεν μπορεί να το βρει. Αυτό γίνεται εφικτό με τη χρήση μεμονωμένων φωτονίων - τα σωματίδια του φωτός - για τη μεταφορά των αριθμητικών κλειδιών. Τα φωτόνια είναι τόσο ευαίσθητα που αν κάποιος ή κάτι προσπαθήσει να κατασκοπεύσει το ταξίδι τους μέσω των οπτικών ινών, η κωδικοποιημένη κατάσταση τους αλλάζει αυτόματα. Έτσι ο πομπός και ο παραλήπτης αμέσως καταλαβαίνουν αυτήν την παρέμβαση και δεν χρησιμοποιούν το κλειδί.

**Μειονεκτήματα:**

- Δυστυχώς τα κβαντικά κρυπτογραφημένα μηνύματα - που στέλνονται μέσω των οπτικών ινών - καλύπτουν μικρή απόσταση και μπορούν να εργαστούν από σημείο σε σημείο, δηλαδή με υπολογιστές κατευθείαν συνδεδεμένους ο ένας με τον άλλο, και όχι με υπολογιστές συνδεδεμένους σε δίκτυο.
- Η μεγαλύτερη απόσταση που έχουν διανύσει μέχρι τώρα είναι 120 χιλιόμετρα.

**Εμπορική εφαρμογή της κβαντικής κρυπτογράφησης:**

Έπειτα από μία δεκαετία εργαστηριακών δοκιμών, μέθοδοι κρυπτογράφησης που βασίζονται στις κβαντικές ιδιότητες του φωτός άρχισαν να χρησιμοποιούνται σε εμπορικές και κυβερνητικές εφαρμογές υψηλής ασφάλειας. Η αμερικανική εταιρεία Magiq και η ελβετική ID Quantique έχουν

ήδη πουλήσει εξοπλισμό κβαντικής κρυπτογράφησης, πιθανότατα σε κυβερνητικές και στρατιωτικές υπηρεσίες.

**Σημείωση:** Μία ομάδα ερευνητών του Τεχνολογικού Ινστιτούτου της Μασαχουσέτης (Massachusetts Institute of Technology) ανακοίνωσε ότι κατάφερε για πρώτη φορά να σπάσει ένα δίκτυο που ήταν προστατευμένο με κβαντική κρυπτογράφηση. Παραδέχτηκε, όμως, ότι η τεχνική τους δεν είναι ακόμη ικανή να καταφέρει να σπάσει πλήρως ένα πραγματικό κβαντικό δίκτυο, αλλά είναι θέμα χρόνου να το καταφέρουν.

# Κεφάλαιο 3

# Οι εφαρμογές της κρυπτογραφίας στην οικονομία

Η ανάπτυξη του ηλεκτρονικού εμπορίου ξεκινά τη δεκαετία του 1970 με την εμφάνιση των συστημάτων ηλεκτρονικής μεταφοράς χρηματικών πόρων μεταξύ τραπεζών. Η μεταφορά των χρηματικών πόρων γίνεται μέσω ασφαλών ιδιωτικών δικτύων, τα οποία αλλάζουν τη μορφή των παραδοσιακών χρηματοοικονομικών αγορών.

Στη δεκαετία του 1980 έκανε την εμφάνισή της η τεχνολογία ηλεκτρονικής επικοινωνίας που βασιζόταν στην αρχιτεκτονική της ανταλλαγής μηνυμάτων (συστήματα EDI και ηλεκτρονικό ταχυδρομείο). Με αυτόν τον τρόπο γίνεται εφικτή η διεκπεραίωση επικοινωνιακών δραστηριοτήτων ηλεκτρονικά, συνεπώς γρηγορότερα και με χαμηλότερο κόστος.

Στη δεκαετία του 1990 τα δίκτυα ηλεκτρονικής επικοινωνίας και το internet δίνουν τη δυνατότητα μιας νέας μορφής επικοινωνίας όπως το ηλεκτρονικό ταχυδρομείο, η ηλεκτρονική συνδιάσκεψη, η ηλεκτρονική συνομιλία, οι ομάδες αναζήτησης, η ηλεκτρονική μεταφορά αρχείων κλπ.

Έπειτα η εμφάνιση του παγκόσμιου ιστού, η ευρεία χρήση των windows και η επικράτηση των προσωπικών ηλεκτρονικών υπολογιστών συντελούν στην ανάπτυξη του ηλεκτρονικού εμπορίου.

Τέλος, το 2000 με την καθιέρωση μεθόδων κρυπτογράφησης του περιεχομένου των μηνυμάτων και εξακρίβωσης της ταυτότητας του αποστολέα, γίνονται πιο ασφαλείς οι διεθνείς ηλεκτρονικές συναλλαγές και κατά συνέπεια πιο προσιτές από τους χρήστες του διαδικτύου.

## 3.1 Ηλεκτρονικές επιχειρήσεις.

(Για την ενότητα που ακολουθεί χρησιμοποιήσαμε στοιχεία από τις πηγές [5], [6], [10], [23], [38]).

Τα τελευταία χρόνια η εξέλιξη του internet και των νέων τεχνολογιών πληροφοριών και επικοινωνίας άλλαξε τον τρόπο που οι επιχειρήσεις πραγματοποιούν τις δραστηριότητές τους. Χρησιμοποιώντας αυτό το ευέλικτο μέσο κατάφεραν να εκμεταλλευτούν τις δυνατότητές που τους προσφέρει και σε συνδυασμό με την υπάρχουσα εμπορική τους δραστηριότητα, να στηρίξουν και την ηλεκτρονική τους παρουσία. Ο ανταγωνισμός όμως είναι ιδιαίτερα σκληρός στην ψηφιακή οικονομία, επομένως οι επιχειρήσεις που θα καταφέρουν να προσαρμοστούν καλύτερα στα νέα δεδομένα θα είναι αυτές που θα αποκτήσουν και συγκριτικό πλεονέκτημα.

Ένας πολύ κρίσιμος αλλά και καθοριστικός παράγοντας για την ευρεία διάδοση, χρήση και αποδοχή του ηλεκτρονικού εμπορίου πάνω από ανοικτά συστήματα και δίκτυα είναι η ασφάλεια των συναλλαγών. Ο δισταγμός των περισσότερων επιχειρήσεων αλλά και των καταναλωτών οφείλεται κυρίως στην ανησυχία για την ασφάλεια του δικτύου αλλά και των συναλλαγών που λαμβάνουν χώρο σε αυτό. Υπάρχουν πολλές περιπτώσεις καταστροφής δεδομένων, εξαπάτησης/κλοπής χρημάτων, παραποίησης εγγράφων, υποκλοπής προσωπικών δεδομένων κλπ. γεγονότα που μεγαλώνουν την ανασφάλεια των χρηστών για τη διεκπεραίωση των συναλλαγών τους μέσω του διαδικτύου. Το διαδίκτυο, άλλωστε, βασίζεται σε ανοικτά πρότυπα που σε συνδυασμό με την ελεύθερη ανταλλαγή πληροφοριών μπορεί να οδηγήσουν στη σκέψη ότι διαδίκτυο και ασφάλεια είναι δυο όροι αμοιβαία αποκλειόμενοι. Αυτό, όμως, απέχει από την πραγματικότητα αφού μια ποικιλία προτύπων, πρωτοκόλλων και εφαρμογών που βασίζονται σε τεχνικές κρυπτογράφησης καλύπτουν το όλο

εύρος, από ασφάλεια σε επίπεδο πακέτου μέχρι ασφάλεια σε επίπεδο εφαρμογών.

Συμπερασματικά, η δημιουργία ασφαλούς περιβάλλοντος στο ηλεκτρονικό εμπόριο σημαίνει την προστασία των δικτυακών πόρων από ενδεχόμενες απειλές και κινδύνους και γενικότερα την εγγύηση του ίδιου, τουλάχιστον, επιπέδου ασφαλείας με το παραδοσιακό εμπόριο. Στο σημείο αυτό, κάνει την εμφάνισή του ο διαχειριστής (manager) ασφαλείας της ηλεκτρονικής επιχείρησης, ο οποίος θα πρέπει να ερευνήσει και να αναλύσει τους κινδύνους και στη συνέχεια καλείται να επιλέξει και να υλοποιήσει ένα πλάνο ασφαλείας. Το τελικό πλάνο/ σύστημα που θα επιλεγεί για να ελέγχει και να προστατεύει τις πληροφορίες της επιχείρησης που ταξιδεύουν στο διαδίκτυο, θα είναι αυτό που μεγιστοποιεί το λόγο *απόδοση προς κόστος*.

### 3.1.1 Το πέντε στα πέντε για τη δημιουργία ενός ασφαλούς περιβάλλοντος στο ηλεκτρονικό εμπόριο:

Για τη δημιουργία ενός ασφαλούς περιβάλλοντος στο ηλεκτρονικό εμπόριο πρέπει να ικανοποιούνται πέντε βασικές απαιτήσεις, οι οποίες εξαρτώνται άμεσα η μία από την άλλη και πρέπει να συμβαδίζουν με την πολιτική ασφαλείας που έχει επιλεγεί από το σύστημα. Επιγραμματικά οι απαιτήσεις αυτές είναι:

- ο έλεγχος αυθεντικότητας- authentication.
- η εξουσιοδότηση- authorization.
- η εμπιστευτικότητα- confidentiality.
- η ακεραιότητα- integrity.
- η μη αποποίηση της ευθύνης- non repudiation.

Αναλυτικότερα:

Η διαδικασία του **ελέγχου αυθεντικότητας** αποσκοπεί στην εξακρίβωση της ταυτότητας ενός χρήστη επιτυγχάνοντας έτσι τον αποκλεισμό περιπτώσεων ψηφιακής πλαστοπροσωπίας. Ο έλεγχος αυτός γίνεται με τη χρήση διαφόρων τεχνολογιών και συστημάτων, πριν από την έναρξη οποιασδήποτε ηλεκτρονικής συναλλαγής. Ειδικότερα, τα συστήματα ασφαλείας επιτυγχάνουν την πιστοποίηση συγκρίνοντας και επαληθεύοντας τις πληροφορίες που δίνει ο χρήστης, σε σχέση με αυτές που ήδη υπάρχουν στο σύστημα για αυτόν. Οι πιο συνηθισμένες μέθοδοι που χρησιμοποιούνται για τη διασφάλιση της αυθεντικότητας των χρηστών σε συστήματα και δίκτυα είναι:

- τα passwords (κωδικοί πρόσβασης)
- οι προσωπικοί κωδικοί αναγνώρισης (PINS, κλειδιά, κωδικοί καρτών κλπ)
- οι ψηφιακές υπογραφές και τα πιστοποιητικά.

Η **εξουσιοδότηση** περιλαμβάνει την παραχώρηση δικαιωμάτων του χρήστη Α στον Β, δηλαδή τον έλεγχο της πρόσβασης σε συγκεκριμένες πληροφορίες και υπηρεσίες όταν η ταυτότητα του χρήστη έχει εξακριβωθεί. Πιο συγκεκριμένα, η εξουσιοδότηση περιλαμβάνει μηχανισμούς ελέγχου πρόσβασης σε δικτυακούς τόπους και γενικότερα δικαιώματα πρόσβασης. Κατά συνέπεια περιορίζει τις ενέργειες ή τις λειτουργίες που οι χρήστες μπορούν να πραγματοποιήσουν σε ένα δικτυωμένο περιβάλλον. Τέλος, ο διαχειριστής καθορίζει και ελέγχει τα προνόμια και τις «άδειες» των εξουσιοδοτημένων χρηστών που είναι καταγεγραμμένα στη λίστα ελέγχου πρόσβασης.

Η **εμπιστευτικότητα** αποτελεί απαραίτητο στοιχείο της ιδιωτικότητας του χρήστη (user privacy) και αφορά την αποφυγή της μη εξουσιοδοτημένης χρήσης των πληροφοριών. Όσον αφορά το ηλεκτρονικό εμπόριο, η

εμπιστευτικότητα, παίζει πολύ σημαντικό ρόλο κυρίως στην προστασία οικονομικών δεδομένων ενός πελάτη, των οργανωτικών δομών της επιχείρησης, καθώς και άλλων διαφόρων τύπων ιδιωτικών πληροφοριών από μη εξουσιοδοτημένη πρόσβαση. Για να ικανοποιηθούν αυτές οι απαιτήσεις έχουν σχεδιαστεί τεχνικές κρυπτογράφησης και κωδικοποίησης. Παρ' όλα αυτά, για να συμβιβαστούν όλες οι παραπάνω απαιτήσεις πρέπει να περιλαμβάνονται στην εμπιστευτικότητα καθώς και στον έλεγχο αυθεντικότητας, φόρμες ελέγχου της ροής των  εν λόγω «κρίσιμων» πληροφοριών. Οι φόρμες αυτές καθορίζουν πότε ένα αντικείμενο θα ανακοινωθεί, ποια τιμή θα καθοριστεί και ποιος θα το χρεωθεί. Στο σημείο αυτό πρέπει να αναφερθεί το μέγεθος της σημαντικότητας της εμπιστευτικότητας για μια επιχείρηση που η οικονομία της είναι βασισμένη σε πληροφορίες: ένα μόνο κενό μπορεί να είναι καταστρεπτικό!

Η **ακεραιότητα** αφορά την αποφυγή της μη εξουσιοδοτημένης τροποποίησης των πληροφοριών κατά τη διάρκεια της μεταφοράς και της αποθήκευσής τους στο δίκτυο. Για τις ηλεκτρονικές συναλλαγές κρίνεται αναγκαία η βεβαιότητα ότι οι πληροφορίες θα φτάσουν στον προσδιορισμό τους όπως ακριβώς στάλθηκαν, χωρίς καμία προσθήκη, αφαίρεση, αναδιάταξη και γενικότερα τροποποίηση των μερών τους. Μια μέθοδος που ικανοποιεί αυτή την απαίτηση είναι οι ψηφιακές υπογραφές.

Τέλος, **η μη αποποίηση της ευθύνης** περιλαμβάνει μηχανισμούς ασφαλείας στην πραγματοποίηση κρίσιμων συναλλαγών και επικοινωνιών. Δίνεται βαρύτητα στη συνθήκη: κανένας από τους συναλλασσόμενους δεν έχει τη δυνατότητα να αρνηθεί τη συμμετοχή του σε μια συναλλαγή. Οι μηχανισμοί μη αποποίησης της ευθύνης οφείλουν, αν ερωτηθούν, να αποδείξουν την προέλευση, την μετάδοση και την παράδοση των δεδομένων.

**Τεχνικές που εγγυώνται την ασφάλεια των συναλλαγών**

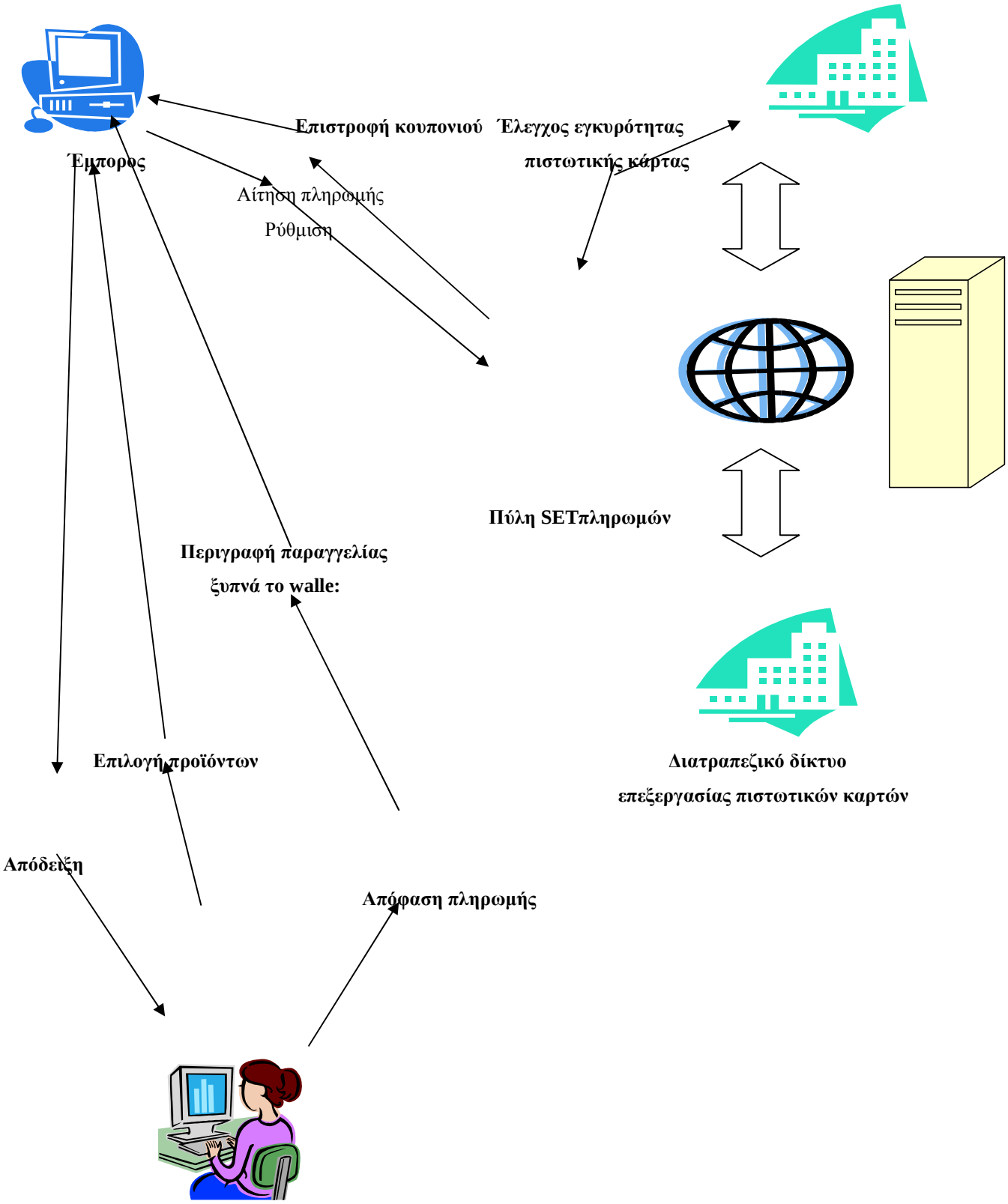
Η ασφάλεια των συναλλαγών στο web περιστρέφεται γύρω από δυο βασικά πρωτόκολλα, που αναλύθηκαν λεπτομερώς στο προηγούμενο κεφάλαιο το SSL και το S-HTTP, τα οποία προσφέρουν αυθεντικοποίηση στα πακέτα δεδομένων σε επίπεδο δικτύου, εμπιστευτικότητα και ακεραιότητα των δεδομένων στην μεταξύ τους επικοινωνία.

## 3.1.2 Υλοποίηση συναλλαγής με τη χρήση του πρωτοκόλλου SET- μέθοδοι πληρωμών.

Ο έμπορος ανοίγει λογαριασμό σε τράπεζα αποδέκτη (Acquiring Bank). Η τράπεζα αποδέκτης καθορίζει ποιες πιστωτικές κάρτες θα γίνονται δεκτές στις συναλλαγές. Ο πελάτης δίνει τα στοιχεία της πιστωτικής του κάρτας στον έμπορο πάνω στο διαδίκτυο. Ο έμπορος μεταβιβάζει με ασφάλεια τα στοιχεία που δέχτηκε στο διατραπεζικό σύστημα επεξεργασίας χρεώσεων και διαπιστώνει την πιστοληπτική ικανότητα του πελάτη, χάρη στην αυτόματη επικοινωνία με την τράπεζα έκδοσης της πιστωτικής κάρτας του πελάτη (Issuing Bank). Η μεταφορά των χρημάτων στο λογαριασμό των εμπόρων γίνεται σε μεταγενέστερο στάδιο λόγω των νομικών περιορισμών που διέπουν το ηλεκτρονικό εμπόριο.

Τα προαπαιτούμενα για την υλοποίηση του πρωτοκόλλου SET είναι:

1. Λογισμικό, ηλεκτρονικό πορτοφόλι (SET wallet) το οποίο είναι ενσωματωμένο στους φυλλομετρητές (browsers).
2. Πιστοποιητικό πωλητή, υπογεγραμμένο με το δημόσιο κλειδί της «τράπεζας αποδέκτη» και το δημόσιο κλειδί του εκδοτικού οργανισμού της κάρτας διαδοχικά.
3. Προαιρετικά πιστοποιητικό πελάτη από την τράπεζα έκδοσης της πιστωτικής κάρτας.




**Εικόνα 20:** Τα στάδια συναλλαγής.

Τα στάδια της συναλλαγής φαίνονται στο παραπάνω σχήμα (εικόνα 20) όπου:

1. Ο πελάτης αλληλεπιδρά με το web site του πωλητή για να διαλέξει τα προϊόντα που θα αγοράσει.

2. Ο πωλητής στέλνει μια περιγραφή της παραγγελίας η οποία ενεργοποιεί το SET πορτοφόλι του πελάτη.

3. Ο πελάτης ελέγχει την παραγγελία και μεταβιβάζει στη βαθμίδα SET του πωλητή την απόφασή του να πληρώσει.

4. Ο πωλητής στέλνει την αίτηση πληρωμής στη πύλη μεταγωγής πληρωμής (payment gateway). Στο SET ο πωλητής δε γνωρίζει τα εμπιστευτικά χαρακτηριστικά της πιστωτικής κάρτας του πελάτη, απλώς τα μεταβιβάζει στη SET πύλη πληρωμών για τον έλεγχο εγκυρότητας.

5. Η πύλη μεταγωγής πληρωμής ελέγχει την εγκυρότητα της πιστωτικής κάρτας του πελάτη μέσω του διατραπεζικού δικτύου επεξεργασίας πιστωτικών καρτών.

6. Η πύλη μεταγωγής πληρωμής επιστρέφει ένα κουπόνι κλεισίματος παραγγελίας στον πωλητή.

7. Ο πωλητής στέλνει απόδειξη στο πορτοφόλι του πελάτη (customer wallet).

8. Ο πωλητής χρησιμοποιεί το κουπόνι κλεισίματος παραγγελίας, αργότερα, για να ρυθμίσει την αποπληρωμή της εμπορικής πράξης.

Παρ’ όλες τις προσπάθειες που γίνονται για τη δημιουργία και την εξέλιξη των συστημάτων διασφάλισης των συναλλαγών, οι πιθανές απειλές αντιμετωπίζονται ως ένα βαθμό με επιτυχία. Συμπερασματικά, δεν έχει δημιουργηθεί ακόμη εκείνο το κλίμα που θα πείσει τους χρήστες ότι οι ηλεκτρονικές συναλλαγές είναι απολύτως ασφαλείς. Συνεπώς, το μέλλον του ηλεκτρονικού εμπορίου συνδέεται άρρηκτα με την βέλτιστη δυνατή λύση του προβλήματος της ασφάλειας των συναλλαγών.


## 3.2. Οι ηλεκτρονικές τραπεζικές συναλλαγές.

(Στην ενότητα που ακολουθεί χρησιμοποιήθηκαν στοιχεία από τις πηγές [5], [6], [10], [37]).

Ως ηλεκτρονική τράπεζα ορίζεται η "Αυτοματοποιημένη παροχή νέων και παραδοσιακών τραπεζικών προϊόντων και υπηρεσιών, απευθείας στους πελάτες, μέσω ηλεκτρονικών αλληλεπιδραστικών καναλιών επικοινωνίας."

Στον όρο e- banking περιλαμβάνονται τα συστήματα εκείνα που επιτρέπουν σε οικονομικούς οργανισμούς, ιδιώτες και επιχειρήσεις να έχουν πρόσβαση σε λογαριασμούς, να πραγματοποιούν ποικίλες χρηματοοικονομικές συναλλαγές και να λαμβάνουν χρήσιμες πληροφορίες για σχετικά προϊόντα και υπηρεσίες μέσω δημόσιων ή ιδιωτικών δικτύων.

Για την πρόσβαση στις διαθέσιμες υπηρεσίες οι πελάτες μπορούν να χρησιμοποιήσουν έξυπνες ηλεκτρονικές συσκευές, όπως προσωπικούς υπολογιστές, υπολογιστές χειρός (PDA), ATM ακόμη και κινητά τηλέφωνα.

Η ταχεία διάδοση του Internet σε παγκόσμιο επίπεδο και η βελτίωση των μεθόδων ασφαλούς σύνδεσης και ελέγχου της αξιοπιστίας των συναλλαγών έχουν δημιουργήσει νέες επιχειρηματικές ευκαιρίες για τους τραπεζικούς οργανισμούς. Επίσης, ο ανταγωνισμός έχει συμβάλει στη βελτίωση των παρεχόμενων υπηρεσιών e-banking, όπως έγκριση δανείων, άνοιγμα λογαριασμών, ηλεκτρονικές πληρωμές κ.α. Όμως, εκτός από οφέλη δημιουργήθηκαν και κίνδυνοι που πρέπει να απομονωθούν και να αντιμετωπιστούν από όσους τραπεζικούς οργανισμούς προσφέρουν υπηρεσίες e-banking.

### 3.2.1 Οι κατηγορίες Web sites που χρησιμοποιούνται στο e-banking

Web sites πληροφοριακού χαρακτήρα.

Μέσω των web site πληροφοριακού χαρακτήρα οι πελάτες έχουν τη δυνατότητα να έχουν πρόσβαση σε γενικές πληροφορίες που αφορούν στον εκάστοτε τραπεζικό οργανισμό, τις παρεχόμενες υπηρεσίες και προϊόντα, καθώς και σε αναλυτικές οδηγίες που αφορούν στη διαδικασία εγγραφής στις υπηρεσίες e-banking.

Οι υπεύθυνοι διαχείρισης κινδύνου θα πρέπει να λάβουν υπόψη τους τις εξής απειλές:

1. Τις πιθανές επιπτώσεις από την παροχή ανακριβών πληροφοριών σχετικά με προϊόντα, υπηρεσίες και χρεώσεις μέσω του web site.

2. Τον κίνδυνο πρόσβασης τρίτων σε εμπιστευτικές πληροφορίες επιχειρήσεων ή ιδιωτών, εάν το web site δεν είναι επαρκώς απομονωμένο από το εσωτερικό δίκτυο του τραπεζικού οργανισμού.

3. Τη διάδοση ιών και άλλων ζημιογόνων εφαρμογών σε υπολογιστές που επικοινωνούν με το web site του τραπεζικού οργανισμού.

4. Τη δυσφήμιση και κατά συνέπεια τη μείωση του κύρους του τραπεζικού οργανισμού, λόγω ατελειών και προβλημάτων στην παροχή των online υπηρεσιών.

5. την πιθανή παραμόρφωση του web site από τρίτους (π.χ. hackers) και την παρουσίαση ανάρμοστου ή προσβλητικού υλικού.

Web sites πραγματοποίησης συναλλαγών.

Τα εν λόγω web sites παρέχουν στους πελάτες τη δυνατότητα να πραγματοποιούν τραπεζικές συναλλαγές και να προμηθεύονται προϊόντα και υπηρεσίες. Οι τραπεζικές συναλλαγές αυτές μπορεί να είναι εξαιρετικά απλές ή πολύπλοκες.

### 3.2.2 Ασφάλεια ηλεκτρονικών τραπεζικών συναλλαγών.

Εφόσον, τυπικά τα web sites καθιστούν δυνατή την ηλεκτρονική ανταλλαγή εμπιστευτικών πληροφοριών για τους πελάτες και τη μεταφορά σημαντικών χρηματικών ποσών, απαιτείται υψηλό επίπεδο ασφάλειας για την προστασία τόσο των πελατών όσο και του ίδιου του τραπεζικού οργανισμού, που εκτίθεται σε πολύ περισσότερους κινδύνους.

Συνεπώς, κρίνεται απαραίτητο μεταξύ άλλων, να λαμβάνονται υπόψη τα εξής:

- Η εφαρμογή μηχανισμών ασφάλειας για την προστασία των προσωπικών δεδομένων των πελατών .
- Οι λειτουργίες εξακρίβωσης της ταυτότητας νέων ή παλιών πελατών που επιθυμούν να χρησιμοποιήσουν υπηρεσίες e-banking.
- Οι πιθανότητες πραγματοποίησης συναλλαγών δίχως έγκριση .

- Οι οικονομικές απώλειες σε περίπτωση που ο τραπεζικός οργανισμός δεν καταφέρει να εξακριβώσει την ταυτότητα αυτών που υποβάλλουν αιτήσεις για άνοιγμα νέων λογαριασμών ή πίστωσης on line.
- Η εκδοχή παραβίασης νόμων ή οδηγιών, που αφορούν στο απόρρητο πληροφοριών πελατών και στην αντιμετώπιση κυκλωμάτων ξεπλύματος χρημάτων και τρομοκρατίας.
- Οι πιθανότητες δυσφήμισης του τραπεζικού οργανισμού, δυσαρέστησης των πελατών καθώς και οι νομικές επιπτώσεις λόγω αποτυχιών ή καθυστερήσεων στην εκτέλεση τραπεζικών συναλλαγών.
- Τέλος, οι τυχούσες δυσλειτουργίες των υπηρεσιών e-banking από τη μη εγκεκριμένη αποκάλυψη εμπιστευτικών πληροφοριών των πελατών κατά τη διάρκεια της μετάδοσης ή αποθήκευσής τους.

Γενικά, στην περίπτωση του e-Banking τα πράγματα είναι κάπως περίπλοκα στο θέμα της τραπεζικής ευθύνης, αλλά υπάρχει σαφώς αυστηρότερος έλεγχος από την ίδια την τράπεζα σε ό,τι αφορά το επίπεδο ασφάλειας των συναλλαγών, σε σχέση με την αντίστοιχη ηλεκτρονική χρήση των πιστωτικών καρτών. Πρακτικά, η τράπεζα επιβάλλει μια σειρά πρόσθετων μηχανισμών ασφαλείας που δεν υπάρχουν στην περίπτωση των πιστωτικών καρτών, πράγμα που κάνει το σύστημα ουσιαστικά απαραβίαστο, αν η χρήση των μηχανισμών αυτών είναι σωστή από την πλευρά του πελάτη (π.χ. χρήση λίστας κωδικών TAN, Transaction Authorization Numbers – Αριθμοί Εξουσιοδότησης Συναλλαγής).

### 3.2.3 Κωδικοί TAN: Χρησιμότητα και τρόπος λειτουργίας.

Ο λόγος για τον οποίο οι κωδικοί TAN είναι πλέον απαραίτητοι σε κάθε συναλλαγή e-Banking είναι ότι η κάθε τράπεζα έχει τον απόλυτο έλεγχο της πολιτικής και των μηχανισμών ασφάλειας που επιθυμεί να εφαρμόσει. Έτσι μπορεί να επιβάλλει την εξουσιοδότηση κάθε εγχρήματης συναλλαγής ξεχωριστά με ειδικό κωδικό μιας χρήσης. Αυτό στην πράξη γίνεται με την

χορήγηση λίστας πρόσθετων κωδικών εξουσιοδότησης στους πελάτες του e-Banking, κάτι σαν password μιας χρήσης, προσωπικά σε κάθε πιστοποιημένο πελάτη της.

Το πλεονέκτημα των κωδικών TAN είναι:

- ότι πρόκειται για κωδικούς οι οποίοι δεν αποθηκεύονται πουθενά στο σύστημα του χρήστη-πελάτη, αντίθετα βρίσκονται σε τυπωμένη μορφή, άρα είναι αδύνατο να υποκλαπούν ηλεκτρονικά από το σύστημά του.
- Αντίστοιχα, στο σύστημα e-Banking της τράπεζας όπου τηρούνται αντίγραφα των κωδικών αυτών για αντιπαραβολή υπάρχουν τα κατάλληλα μέτρα εξασφάλισης της εμπιστευτικότητας σε πολύ υψηλό επίπεδο, έτσι ώστε η κλοπή τους, φυσική ή ηλεκτρονική, να είναι ουσιαστικά ανέφικτη. Κατά συνέπεια, ακόμα και αν ο κύριος κωδικός (username/password) του χρήστη-πελάτη παραβιαστεί και κάποιος τρίτος αποκτήσει πρόσβαση στον λογαριασμό του, δεν μπορεί να κάνει καμία εγχρήματη συναλλαγή αφού δεν διαθέτει αντίστοιχους έγκυρους κωδικούς TAN.

**Τρόπος λειτουργίας των κωδικών TAN και MAC.**

Η λογική της λειτουργίας των κωδικών TAN βασίζονται στην ιδέα της κρυπτογράφησης μέσω κωδικοβιβλίων (codebooks) μιας χρήσης ή αλλιώς συστημάτων one-time-pads, τα οποία είναι τα μόνα μοντέλα κρυπτογράφησης των οποίων το απαραβίαστο εξασφαλίζεται 100% και αποδεικνύεται θεωρητικά. Γι’ αυτό, άλλωστε, χρησιμοποιούνται ακόμη και σήμερα σε μερικούς τύπους στρατιωτικών επικοινωνιών (συστήματα χαμηλού ρυθμού μετάδοσης).

Στην περίπτωση των κωδικών TAN τα κωδικοβιβλία δεν χρησιμοποιούνται για κρυπτογράφηση αλλά για την χορήγηση κωδικών "γνησιότητας". Αυτή η μορφή αναφέρεται συχνά ως Κωδικός Αυθεντικοποίησης Μηνύματος (MAC – Message Authentication Code), ο

οποίος συνοδεύει κάθε μήνυμα και χρησιμοποιείται για την διάκριση των γνήσιων από τα πλαστά μηνύματα. Για να εξασφαλιστεί η κρυπτασφάλεια των "γνήσιων" κωδικών υπάρχει μια κοινή λίστα μυστικών κωδικών στα δύο άκρα της επικοινωνίας, δηλαδή ένα κωδικοβιβλίο με κωδικούς μιας χρήσης τους οποίους χρησιμοποιούν και διασταυρώνουν για τον έλεγχο κάθε μηνύματος.

Εντούτοις, το βασικό πρόβλημα είναι η μεταφορά και αποθήκευση των αντίστοιχων κωδικοβιβλίων με ασφαλή τρόπο και στα δύο μέρη που επικοινωνούν. Στους κωδικούς TAN αυτό εξασφαλίζεται από την ίδια την τράπεζα, απαιτώντας την προσωπική ταυτοποίηση και παράδοση της λίστας TAN στον ίδιο τον πελάτη αυτοπροσώπως και μάλιστα σε μορφή εν γένει μη-αποθηκεύσιμη στον Η/Υ του. Όμως η διαδικασία έκδοσης και προσωπικής παραλαβής της λίστας TAN είναι συχνά χρονοβόρα και δυσχερής, μια και ακυρώνει μέρος της ίδιας της έννοιας του e-Banking.

Για την εξασφάλιση της κρυπτασφάλειας του συστήματος των MAC, και ταυτόχρονα την άμεση συσχέτισή τους με το ίδιο το περιεχόμενο του μηνύματος, συχνά εφαρμόζονται δύο πρόσθετα στάδια επεξεργασίας και ένα μοναδικό μυστικό κλειδί. Αυτό γίνεται για να μην χρειάζεται η χρήση ειδικού κωδικοβιβλίου όπως προβλέπεται για το αρχικό μοντέλο των one-time-pads.

ð Συγκεκριμένα, το περιεχόμενο του μηνύματος περνά μέσα από μια διαδικασία επεξεργασίας που ονομάζεται «συνάρτηση κατακερματισμού "Μη Αντιστρέψιμη" ή "Μιας Κατεύθυνσης"» (One-Way Hashing Function). Κατά τη διαδικασία αυτή, αντιστοιχίζεται το σύνολο των δεδομένων του μηνύματος σε έναν μοναδικό κωδικό αναγνώρισης συγκεκριμένου μεγέθους (π.χ. 128 ή 256 bits) από τον οποίο δεν μπορεί να εξαχθεί το περιεχόμενο του αρχικού μηνύματος με κανέναν τρόπο, λόγω των μαθηματικών ιδιοτήτων της συγκεκριμένης συνάρτησης. Επιπλέον, είναι σχεδόν αδύνατο η συνάρτηση αυτή να δημιουργήσει τον ίδιο κωδικό αναγνώρισης για δύο διαφορετικά μηνύματα.

ð Στη συνέχεια, ο κωδικός αυτός κρυπτογραφείται με το μοναδικό μυστικό κλειδί κρυπτογράφησης πριν μεταδοθεί στο κανάλι μετάδοσης. Η διαδικασία ονομάζεται Keyed-HMAC (Hashed Message Authentication Code with Key) και ουσιαστικά κάνει περιττή την χρήση ειδικών κωδικοβιβλίων τύπου one-time-pad για αυτό το σκοπό, διατηρώντας έτσι εξαιρετικά μικρή θεωρητικά (αλλά όχι αδύνατη πλέον, όπως στο one-time-pad) την πιθανότητα παραβίασης της κρυπτασφάλειας του συστήματος.

Με το σύστημα των keyed-HMAC εξασφαλίζεται ότι:

¶ κανένας δεν μπορεί να "πειράξει" το αρχικό μήνυμα χωρίς να "ακυρώσει" το συγκεκριμένο κωδικό αυθεντικοποίησης του μηνύματος και

¶ ότι κανένας άλλος δεν μπορεί να παράγει γνήσιους κωδικούς αυθεντικοποίησης εφόσον δεν διαθέτει το αντίστοιχο μυστικό κλειδί.

Στην πράξη, το μοντέλο αυτό εφαρμόζεται στις επικοινωνίες σαν μία εύκολη και γρήγορη εναλλακτική λύση, έναντι της εφαρμογής των πιο πολύπλοκων και εξειδικευμένων μοντέλων ψηφιακών υπογραφών (digital signatures).

**Συσκευές δημιουργίας κωδικών TAN.**

Σε αναλογία με την εφαρμογή των keyed-HMAC, για την αντικατάσταση των κωδικοβιβλίων, υπάρχουν και άλλοι τρόποι να αντικατασταθεί η εκτυπωμένη λίστα TAN. Με μια αντίστοιχη συσκευή παραγωγής μεμονωμένων κωδικών από τον ίδιο τον πελάτη (πάντα απομονωμένη από τον Η/Υ τον οποίο χρησιμοποιεί για την πρόσβαση στο σύστημα e-Banking) που φυσικά συσχετίζεται άμεσα με τον αντίστοιχο μηχανισμό διασταύρωσής τους από το σύστημα της τράπεζας. Πρακτικά αυτό υλοποιείται με συνδυασμό τριών πραγμάτων:

(1) μια γεννήτρια ψευδοτυχαίων αριθμών (PRNG).

(2) ένα κύκλωμα χρονισμού υψηλής ακρίβειας (CLOCK).

(3) και με ένα μυστικό ηλεκτρονικό κλειδί της τράπεζας (KEY).

Αναλυτικότερα η βασική διαδικασία είναι η εξής:

Η γεννήτρια PRNG χρειάζεται έναν αρχικό κωδικό για να ξεκινήσει και στην συνέχεια μπορεί να παράγει αριθμούς οι οποίοι είναι "επαρκώς τυχαίοι", ώστε να μην είναι προβλέψιμοι με κανέναν τρόπο αν κάποιος δεν γνωρίζει τον κωδικό αρχικοποίησης. Αυτό είναι αρμοδιότητα της τράπεζας, δηλαδή να αρχικοποιεί τις συσκευές αυτές έτσι ώστε να μπορεί να "αναπαράγει" μόνο η ίδια την ακολουθία των αριθμών αυτών. Επιπλέον, το κύκλωμα CLOCK μπορεί να χρησιμοποιηθεί για να αρχικοποιεί και πάλι την συσκευή σε τακτά χρονικά διαστήματα, τα οποία επίσης γνωρίζει η τράπεζα χωρίς να χρειάζεται περαιτέρω επικοινωνία ή σύνδεση με την συσκευή του πελάτη. Αυτό συμβαίνει γιατί αρκεί απλά το CLOCK ή "ρολόι" της συσκευής TAN να είναι συγχρονισμένο με αυτό του συστήματος της τράπεζας. Για το λόγο αυτό το κύκλωμα CLOCK της κάθε συσκευής TAN πρέπει να είναι υψηλής πιστότητας, με ελάχιστη απόκλιση (π.χ. το πολύ 60 δευτερόλεπτα) στη διάρκεια ζωής της συσκευής (π.χ. 3 χρόνια).

Με τους δύο παραπάνω μηχανισμούς, δηλαδή τον κωδικό αρχικοποίησης του κυκλώματος PRNG και το κύκλωμα CLOCK για την περιοδική επαναρχικοποίηση, η συσκευή TAN μπορεί να παράγει πλέον "τυχαίους" κωδικούς TAN, προβλέψιμους μόνο από το αντίστοιχο σύστημα της ίδιας της τράπεζας.

Όμως, η τράπεζα πρέπει σαν πρόσθετο μέτρο ασφάλειας να έχει τη δυνατότητα να ελέγχει τη γνησιότητα των κωδικών TAN που εισάγει ο χρήστης-πελάτης της, για να αποκλειστεί η περίπτωση κάποιος να "ανακαλύψει" τις λεπτομέρειες σχεδίασης και αρχικοποίησης των κυκλωμάτων

PRNG και CLOCK της συσκευής TAN και να κατασκευάσει μια δική του, μη-πιστοποιημένη συσκευή για την παραγωγή ψευδών αλλά επαληθεύσιμων κωδικών.

Για το λόγο αυτό, το αποτέλεσμα των PRNG/CLOCK συνδυάζεται με το τρίτο στοιχείο του μηχανισμού, δηλαδή ένα μυστικό κλειδί (KEY), το οποίο γνωρίζει μόνο η τράπεζα και είναι αποθηκευμένο μέσα στη συσκευή TAN, χωρίς να υπάρχει δυνατότητα πρόσβασης σε αυτό από τον χρήστη-πελάτη.

Σε ορισμένες περιπτώσεις στην παραπάνω διαδικασία υπάρχει και μια δεύτερη φάση η οποία περιλαμβάνει την παραγωγή ενός πρόσθετου μικρότερου κωδικού ελέγχου (CHECK) μετά από κάθε κωδικό TAN. Αυτό γίνεται για να ενημερωθεί ο χρήστης-πελάτης για την επιτυχημένη και έγκυρη ολοκλήρωση της συναλλαγής του στο σύστημα e-Banking της τράπεζας. Με άλλα λόγια, ο πελάτης είναι αυτός που στο σημείο αυτό συγκρίνει τον κωδικό ελέγχου (CHECK) που επιστρέφει το σύστημα e-Banking της τράπεζας για να διαπιστώσει ότι όλα πήγαν καλά.

Τέλος, για την εξασφάλιση της ίδιας της συσκευής υπάρχει εσωτερικά φυσικός μηχανισμός "αυτοκαταστροφής" της συσκευής TAN σε περίπτωση που παραβιαστεί με φυσικό τρόπο. Αν, δηλαδή, κάποιος επιχειρήσει να την ανοίξει για να "διαβάσει" τα αντίστοιχα ηλεκτρονικά κυκλώματα, οι σημαντικές πληροφορίες (π.χ. KEY) διαγράφονται αυτόματα και μόνιμα από την συσκευή TAN, ώστε η ανάκτησή τους να είναι αδύνατη. Επιπλέον, ως μέρος των παραπάνω μηχανισμών, η τράπεζα αναγνωρίζει κάθε μεμονωμένη συσκευή TAN με έναν μοναδικό σειριακό αριθμό που βρίσκεται στο πίσω μέρος της και που "δεσμεύει" τη συγκεκριμένη συσκευή με τον λογαριασμό του αντίστοιχου πελάτη-χρήστη.

**Πρακτική χρήση και περιορισμοί κωδικών TAN.**

Σήμερα, οι συσκευές TAN που διατίθενται από τις ελληνικές τράπεζες ενσωματώνουν τους παραπάνω βασικούς μηχανισμούς με κατάλληλο τρόπο, αλλά όχι πάντα ταυτόσημο. Για παράδειγμα, σε κάποιες περιπτώσεις οι συσκευές TAN παράγουν κωδικούς μιας χρήσης μόνο μετά από αίτημα του χρήστη (πάτημα ενός ενσωματωμένου πλήκτρου), ενώ άλλες παράγουν συνεχώς κωδικούς οι οποίοι ανανεώνονται αυτόματα κάθε 60 δευτερόλεπτα, είτε χρησιμοποιούνται είτε όχι. Γενικά, δεν υπάρχει διαφορά στο επίπεδο ασφάλειας που προσφέρουν όμως οι ίδιες οι συσκευές TAN έχουν ένα συγκεκριμένο χρονικό διάστημα (ή αντίστοιχα πλήθος παραγόμενων κωδικών) "ασφαλούς χρήσης" πέρα από το οποίο η "τυχαιότητα" τους δεν θεωρείται πλέον εξασφαλισμένη. Συνήθως, το διάστημα αυτό είναι 3 χρόνια ή 2 εκατομμύρια κωδικοί TAN. Σε αυτή την περίπτωση, η συσκευή είτε αντικαθίσταται με νέα είτε αρχικοποιείται από την τράπεζα με νέους κωδικούς και είναι έτοιμη για χρήση για άλλο τόσο διάστημα, σαν να ήταν καινούργια.

Όπως είναι προφανές, η τεχνολογία και η υποδομή για την πλήρη εξασφάλιση των ηλεκτρονικών τραπεζικών συναλλαγών υπάρχει. Τα σημερινά συστήματα κρυπτασφάλισης είναι τόσο προσιτά και ταυτόχρονα τόσο ασφαλή που λίγοι συνειδητοποιούν τι ακριβώς συμβαίνει όταν κάποιος χρησιμοποιεί μια τραπεζική κάρτα σε ένα μηχάνημα αυτόματης ανάληψης χρημάτων (ATM).

## 3.3 ATM - Asynchronous Transfer Mode (Ασύγχρονος Τρόπος Μεταφοράς).

(Στην παράγραφο που ακολουθεί χρησιμοποιήθηκαν στοιχεία από τις πηγές [5], [9], [12], [50]).

Το ATM είναι μια ηλεκτρονική συσκευή η οποία προσφέρει ένα πλήθος τραπεζικών υπηρεσιών όπως αναλήψεις, καταθέσεις, εμβάσματα, πληρωμές

λογαριασμών κ.α. (Εικόνα 21). Στα ATM ο πελάτης αναγνωρίζεται με την χρήση μιας μοναδικής για τον καθένα κάρτας με μαγνητική ταινία, η οποία περιέχει πληροφορίες ασφαλείας, όπως για παράδειγμα την ημερομηνία λήξης της, το ονοματεπώνυμο του κατόχου της κλπ. Η κάρτα αυτή χρησιμοποιείται με ένα προσωπικό αριθμό αναγνώρισης (PIN) ο οποίος παρέχει ασφάλεια στον πελάτη.


**Εικόνα 21:** Ηλεκτρονική συσκευή ATM.

**Ένα ATM συνήθως αποτελείται από τις ακόλουθες συσκευές:**

- CPU : μία κεντρική μονάδα επεξεργασίας που χρησιμοποιείται για να ελέγχει τη διασύνδεση του χρήστη και τη συσκευή συναλλαγών.
- Αναγνώστη καρτών : χρησιμεύει για την αναγνώριση του πελάτη.
- PIN pad: μπορεί να είναι δύο μορφών είτε αφής ή απλό πληκτρολόγιο πχ σαν ένα κομπιουτεράκι
- Secure crypto processor : ασφαλής επεξεργαστής κρυπτογράφησης.
- Display: μία οθόνη που χρησιμοποιείται από τον πελάτη για την εκτέλεση της συναλλαγής.

- Βασικά κουμπιά λειτουργίας : τα οποία βρίσκονται συνήθως κοντά στην οθόνη και χρησιμοποιούνται για τις διάφορες επιλογές της συναλλαγής.
- Record Printer : ένα τυπογράφο ο οποίος παρέχει στον πελάτη το ιστορικό συναλλαγών του.
- Vault(αποθήκη): που χρησιμεύει για την αποθήκευση των τμημάτων του μηχανήματος που απαιτούν περιορισμένη πρόσβαση
- Housing: έναν ειδικό θάλαμο που χρησιμεύει στην απόδοση της σήμανσης ή απλά για αισθητική.

Πρόσφατα λόγω των αυξημένων απαιτήσεων πολλά ATM υιοθετούν αρχιτεκτονική προσωπικού υπολογιστή και είναι πλέον σε θέση να χρησιμοποιούν λειτουργικά συστήματα, όπως τα Microsoft Windows και Linux.

### 3.3.1 Λογισμικό.

Συνήθως οι πλατφόρμες που χρησιμοποιούνται στα ATM περιλαμβάνουν:

¶ Λογισμικά όπως RMX, OS/2 και λειτουργικά συστήματα της Microsoft( όπως το MS-DOS, PC-DOS, Windows NT, Windows 2000, Windows XP Professional ή Windows XP Embedded), εναλλακτικά τα Java, Linux και Unix.

¶ Κοινές εφαρμογές πρωτόκολλων συναλλαγής , όπως η Diebold 911ή 912, IBM PBM, και NCR NDC ή NCD, που έχουν περισσότερες ικανότητες. Οι περισσότεροι μεγάλοι κατασκευαστές ATM παρέχουν πακέτα λογισμικού που υλοποιούν αυτά τα πρωτόκολλα. Νεότερα πρωτόκολλα όπως IFX δεν έχουν γίνει ακόμα αποδεκτά.

Με το πέρασμα σε ένα πιο τυποποιημένο λογισμικό βάσης, τα χρηματοοικονομικά ιδρύματα έχουν δείξει ενδιαφέρον στο να επιλέξουν την εφαρμογή προγραμμάτων που έχουν την ικανότητα να οργανώνουν καλύτερα

τον εξοπλισμό τους. Το WOSA/xfs, γνωστό σήμερα ως CEN XFS, παρέχει ένα κοινό API για την πρόσβαση και το χειρισμό των διαφόρων συσκευών ενός ATM. J/XFS είναι μια Java εφαρμογή της CEN XFS API.

### 3.3.2 Δίκτυο ATM .

Το δίκτυο ATM είναι το πιο πετυχημένο και αναπτυγμένο εναλλακτικό τραπεζικό δίκτυο στον κόσμο. Προσφέρει μεγάλη εξοικονόμηση κόστους για τις τράπεζες και γρήγορη και ασφαλή εξυπηρέτηση των πελατών των τραπεζικών οργανισμών.

Τα περισσότερα ATM είναι συνδεδεμένα σε (interbank networks) διατραπεζικά δίκτυα, δίνοντας έτσι την δυνατότητα στους χρήστες να κάνουν συναλλαγές από ATM που δεν ανήκουν στην τράπεζα ή στην χώρα στην οποία έχουν τον λογαριασμό τους. Μερικά παραδείγματα από δίκτυα interbank είναι τα PLUS, Cirrus, Interac και LINK.

Επιπλέον, η λειτουργία ενός ATM σε περιοχές όπου δεν υπάρχουν τραπεζικά υποκαταστήματα ή σε ειδικούς χώρους όπως πολυκαταστήματα επιτρέπει τη παρουσία της τράπεζας στους χώρους αυτούς χωρίς λειτουργικά έξοδα και προσφέρει επιπλέον εξυπηρέτηση στον πελάτη.

Υπάρχουν δύο τύποι εγκαταστάσεων ATM :

¶ Τα εντός περιοχής: τα οποία είναι συνήθως πιο προηγμένα και έχουν τις λειτουργίες ενός πραγματικού τραπεζικού υποκαταστήματος, αλλά είναι πιο δαπανηρά.

¶ Τα εκτός περιοχής: τα οποία εγκαθίστανται από χρηματοοικονομικά ιδρύματα και από τα ISO (Independent Sales Organizations) και χρησιμοποιούνται κυρίως για μετρητά, οπότε συνήθως εγκαθίστανται φθηνότερες μόνο-λειτουργικές συσκευές ή λιγότερο δαπανηρές συσκευές με τις βασικές λειτουργίες.

### 3.3.3 Διαδικτύωση ATM.

Τα ATM στηρίζονται στην πιστοποίηση της χρηματοοικονομικής μεταφοράς από τον εκδότη της κάρτας μέσω του δικτύου επικοινωνίας, αυτό συνήθως γίνεται από το σύστημα μηνυμάτων ISO 8583.

Είναι συνήθως συνδεδεμένα στον επεξεργαστή συναλλαγής ATM (ATM Transaction Processor):

¶ είτε μέσω modem σε τηλεφωνική γραμμή. Προτιμούνται από μηχανές λιγότερου φόρτου εργασίας

¶ είτε άμεσα μέσω μισθωτής (leased) γραμμής. Προτιμούνται από τις γραμμές POTS γιατί χρειάζεται λιγότερος χρόνος για την εγκατάσταση μιας σύνδεσης, ωστόσο είναι συγκριτικά πιο ακριβές για να λειτουργήσουν.

Εκτός των μεθόδων που χρησιμοποιούνται για την ασφάλεια μεταφοράς και μυστικότητας, όλες οι συναλλαγές μεταξύ ATM και του επεξεργαστή συναλλαγής κρυπτογραφούνται με μεθόδους όπως η SSL.

### 3.3.4 Ασφάλεια συναλλαγών.

Η ασφάλεια συναλλαγών μέσω ATM στηρίζεται κυρίως στην ακεραιότητα του ασφαλούς επεξεργαστή κρυπτογράφησης (crypto processor).
Για την πρόληψη της απάτης χρησιμοποιείται κρυπτογράφηση των προσωπικών πληροφοριών, η οποία απαιτείται από το νόμο σε πολλές χώρες. Τα ευαίσθητα δεδομένα στις συναλλαγές μέσω ATM είναι συνήθως κωδικοποιημένα με DES, αλλά οι επεξεργαστές συναλλαγών απαιτούν συνήθως τη χρήση του Triple DES. Επίσης μπορούν να χρησιμοποιηθούν τεχνικές Remote key Loading για να διασφαλιστεί το απόρρητο της αρχής της χρήσης των κλειδιών κρυπτογράφησης. Τέλος, μπορεί να χρησιμοποιηθεί ο κωδικός πιστοποίησης

μηνύματος MAC για να διασφαλίσει ότι τα μηνύματα δεν έχουν παραβιαστεί κατά τη μετάδοση από το ATM στο οικονομικό δίκτυο.

## 3.4 Έξυπνες κάρτες.

(Στην παράγραφο που ακολουθεί χρησιμοποιήθηκαν στοιχεία από τις πηγές [2], [29], [28], [31], [32], [33], [34]).

Την δεκαετία του 1950 ο οργανισμός Diners Club εξέδωσε τις πρώτες πιστωτικές κάρτες. Στις κάρτες αυτές αναγραφόταν το όνομα του κατόχου τους στην εμπρόσθια όψη και η επίδειξη τους ήταν αρκετή ώστε ο κάτοχος τους να έχει πίστωση σε εστιατόρια, ξενοδοχεία κ.α. Αργότερα, το όνομα του κατόχου εμφανιζόταν σε ανάγλυφη μορφή (όπως σήμερα οι κάρτες ανάληψης χρημάτων) ώστε να διευκολύνεται η αποτύπωσή του. Οι επόμενες απέκτησαν μια μαγνητική λωρίδα η οποία και επέτρεπε την αποτύπωση του ονόματος.

Οι κάρτες αυτές μπορούσαν να πλαστογραφηθούν εύκολα, όμως αυτό τα επόμενα χρόνια με την ταυτόχρονη βελτίωση των πλαστικών καρτών και των microchips άλλαξε.

Η έξυπνη κάρτα δημιουργήθηκε από μια ιδέα για μια κάρτα με ενσωματωμένο κύκλωμα, που είχε ο δημοσιογράφος Ronald Moreno το 1969 στην Γαλλία. Χώρες όπως η Γερμανία (1967), η Ιαπωνία (1970) και οι Ηνωμένες Πολιτείες της Αμερικής (1972), ανεξάρτητα, βοήθησαν στην ανάπτυξης της. Τη δεκαετία όμως του 1980 η Ένωση Τραπεζικών Καρτών της Γαλλίας σε συνεργασία με σπουδαίες εταιρίες της εποχής στο χώρο της πληροφορικής, όπως η Bull και η Philips, ανέπτυξαν στη Γαλλία το δικό τους σύστημα ανάληψης μετρητών από τράπεζα. Το 1982-1984 έτρεξαν το πρώτο πιλοτικό πρόγραμμα για έξυπνες κάρτες. Οι δοκιμές είχαν τεράστια επιτυχία με ελάχιστα προβλήματα. Μια βελτίωση μόνο προέκυψε από αυτές, η ενσωμάτωση της μαγνητικής λωρίδας η οποία και διασφάλισε την συμβατότητα και την

αναγνωσιμότητα της κάρτας. Ακολούθως, οι Γαλλικές Τράπεζες εισήγαγαν την χρήση των έξυπνων καρτών για τραπεζικές λειτουργίες στο ευρύ κοινό.


**Εικόνα 22:** Μορφή έξυπνης κάρτας.

Οι έξυπνες κάρτες είναι μικροσκοπικοί υπολογιστές (εικόνα 22), που έχουν την μορφή μιας πιστωτικής κάρτας, πάνω στην οποία είναι ενσωματωμένο ένα ολοκληρωμένο κύκλωμα (chip) στην εμπρόσθια αριστερή πλευρά. Παράδειγμα τέτοιας κάρτας μπορεί να αποτελέσει η κάρτα SIM που χρησιμοποιείται στα κινητά τηλέφωνα. Μπορούν να λειτουργήσουν ως πιστωτικές, ως χρεωστικές ή ως κάρτες προσωπικών πληροφοριών.

**Βασικές λειτουργίες των έξυπνων καρτών:**

1. Αυθεντικοποίηση: Με τον όρο αυθεντικοποίηση εννοείται ότι μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν πρόσβαση σε συστήματα και κτίρια.
2. Αποθήκευση δεδομένων και αποθήκευση προσωπικών πληροφοριών: Μια έξυπνη κάρτα μπορεί να χρησιμοποιηθεί ως ηλεκτρονικό πορτοφόλι για να αποθηκεύει χρήματα και ως φορητή συσκευή αποθήκευσης – επεξεργασίας χιλιάδων bytes ηλεκτρονικών δεδομένων.

### 3.4.1 Κατηγορίες έξυπνων καρτών.

- Κάρτες μνήμης
- Κάρτες με ενσωματωμένο κύκλωμα μικροεπεξεργαστού
- Κάρτες μνήμης ολοκληρωμένου κυκλώματος
- Κάρτες οπτικής μνήμης

1. **Κάρτες μνήμης**: Οι κάρτες μνήμης έχουν την δυνατότητα αποθήκευσης των δεδομένων και όχι επεξεργασίας τους. Χωρίζονται σε τρεις υποκατηγορίες:

i. *Μη προστατευμένες:* Είναι οι κάρτες που περιέχουν μνήμη απευθείας προσβάσιμη, χωρίς περιορισμούς.

ii. *Προστατευμένες:* Είναι οι κάρτες που έχουν έστω και μία περιοχή μνήμης που χρειάζεται εξουσιοδότηση για την πρόσβαση της.

iii. *Κάρτες μνήμης με λογική ασφάλεια:* Είναι οι κάρτες που η πρόσβαση στην μνήμη τους γίνεται με έλεγχο, αλλά και η επεξεργασία της μνήμης γίνεται με περιορισμένους τρόπους.

**2. Κάρτες με ενσωματωμένο κύκλωμα μικροεπεξεργαστή**: Οι κάρτες μικροεπεξεργαστών παρέχουν μεγαλύτερη χωρητικότητα μνήμης και ασφάλεια δεδομένων ενώ μπορούν να διαχειριστούν τα δεδομένα επί της κάρτας. Χωρίζονται σε δύο υποκατηγορίες:

i.*Τραπεζικές:* Θεωρούνται όσες έχουν πιστωτική ή χρεωστική εφαρμογή.

ii.*Μη τραπεζικές:* Θεωρούνται όλες οι υπόλοιπες .Μερικά παραδείγματα είναι : Οι κάρτες πρόσβασης σε δίκτυα (access cards), οι κάρτες δώρων (gift cards) και οι προπληρωμένες κάρτες (pre-paid cards).

3. **Κάρτες μνήμης ολοκληρωμένου κυκλώματος:** Οι κάρτες αυτές αποθηκεύουν 1-4KB δεδομένων. Μειονέκτημα τους είναι ότι δεν μπορούν να τα διαχειριστούν λόγω έλλειψης επεξεργαστή. Για αυτό η χρήση τους περιορίζεται σε συγκεκριμένες λειτουργίες .

4. **Κάρτες οπτικής μνήμης:** Οι κάρτες αυτές μπορούν να αποθηκεύσουν έως 4MB δεδομένων. Δυστυχώς τα δεδομένα αυτά δεν είναι επεξεργάσιμα και δεν μπορούν να σβηστούν. Για αυτό οι κάρτες οπτικής μνήμης χρησιμοποιούνται για την αποθήκευση ιατρικών ιστορικών ή οποιονδήποτε άλλων αρχείων που χρειάζεται να διατηρηθούν στον χρόνο.

### 3.4.2 Ασφάλεια έξυπνων καρτών.

Οι απάτες εις βάρος των πιστωτικών καρτών γίνονται είτε με την χρήση πλαστών καρτών (ποσοστό περίπου 35%) κατόπιν αντιγραφής της μαγνητικής ταινίας, είτε με την χρήση κλεμμένων ή χαμένων καρτών (ποσοστό περίπου 37%), είτε σε απάτες μέσω του Internet (ποσοστό περίπου 28%). Την λύση στα προβλήματα αυτά έρχεται να δώσει η έξυπνη κάρτα, καθώς κάθε κάρτα διαθέτει ένα microchip στο οποίο είναι αποθηκευμένα τα στοιχεία του κατόχου της και οι κωδικοί ασφαλείας. Έτσι είναι σχεδόν αδύνατον κάποιος να αλλάξει ή να αντιγράψει τα στοιχεία αυτά. Αυτό οφείλεται στις πολύπλοκες κρυπτογραφικές τεχνικές που χρησιμοποιούνται για να κωδικοποιούνται και να αποκωδικοποιούνται οι πληροφορίες. Για την δημιουργία των έξυπνων καρτών χρησιμοποιήθηκε υψηλή τεχνολογία, τέθηκαν σε ισχύ οι πιο νέοι αλγόριθμοι, τοποθετήθηκαν επεξεργαστές και μνήμες μεγάλης χωρητικότητας, έτσι ώστε να σιγουρευτούν οι κατασκευαστές ότι οι συναλλαγές θα είναι ασφαλείς.

Επίσης, κάθε συναλλαγή πλέον δεν θα εγκρίνεται μόνο με την υπογραφή του κατόχου στην απόδειξη αλλά από ένα προσωπικό αριθμό αναγνώρισης (PIN).Έτσι, είναι εύκολη η επιβεβαίωση της ταυτότητας του νόμιμου κατόχου.

### 3.4.3. Το μέλλον των έξυπνων καρτών.

Οι έξυπνες κάρτες αναμένεται να απλοποιήσουν την ζωή μας και να λειτουργούν ως ένα ηλεκτρονικό πορτοφόλι. Στο μέλλον θα μπορούμε να την χρησιμοποιούμε σε ένα μεγάλο μέρος των καθημερινών συναλλαγών μας ακόμα

και για μικρά χρηματικά ποσά όπως να πληρώσουμε ένα καφέ ή στο χώρο των μέσων μαζικής μεταφοράς ως μέσο πληρωμής για την επιβίβαση στα αστικά λεωφορεία. Τοποθετώντας την κάρτα στην υποδοχή των ειδικών τερματικών (συσκευή γενικής χρήσης εισόδου – εξόδου) θα αφαιρείται το αντίστοιχο ποσό μέχρι μηδενισμού του υπολοίπου, ενώ θα υπάρχει η δυνατότητα επαναφόρτισης των χρηματικών μονάδων μέσω ηλεκτρονικών μέσων.

Βασική προϋπόθεση για την χρήση της έξυπνης κάρτας είναι μια σειρά τεχνολογικών αλλαγών που σχετίζονται με την εγκατάσταση μιας σειράς σύγχρονων τερματικών στα σημεία που θα χρησιμοποιείται η κάρτα.
Στην Ελληνική αγορά ήδη έχει εγκατασταθεί ένας μεγάλος αριθμός τερματικών που μπορούν να λειτουργήσουν στο περιβάλλον της έξυπνης κάρτας.

## 3.5 Ηλεκτρονική Δημοπρασία (e- auction).

(Στην παράγραφο που ακολουθεί χρησιμοποιήθηκαν στοιχεία από τις πηγές [13], [22], [26], [38]).

Η δημοπρασία είναι μια από τις κυριότερες λειτουργίες των ηλεκτρονικών αγορών. Ουσιαστικά αποτελούν την ηλεκτρονική εκδοχή των παραδοσιακών δημοπρασιών, με την διαφορά ότι δεν υποχρεώνουν τους ενδιαφερόμενους να συνευρίσκονται σε συγκεκριμένη φυσική τοποθεσία αλλά απλώς να συναλλάσσονται σε καθορισμένο χρονικό διάστημα μέσω της διαδικτυακής πλατφόρμας στην οποία είναι μέλη. Επιπλέον μπορεί να παρέχεται και μια πολυμεσική παρουσίαση των αγαθών. Συνήθως αυτού του είδους οι δημοπρασίες δεν περιορίζονται μόνο σε αυτές τις λειτουργίες και έτσι είναι δυνατόν να προσφέρουν ενσωμάτωση της διαδικασίας δημοπράτησης με τις διαδικασίες συμβάσεων, πληρωμών και παράδοσης.

Οι πηγές εσόδων για τον παροχέα της δημοπρασίας είναι τα οφέλη από την πώληση πλατφόρμας τεχνολογιών, από τις αμοιβές των συναλλαγών και

από τη διαφήμιση. Τα οφέλη για τους προμηθευτές και τους αγοραστές προέρχονται από την αυξημένη αποδοτικότητα, την εξοικονόμηση χρόνου και την μεγάλη ποικιλία αγαθών. Λόγω των μειωμένων εξόδων γίνεται εφικτή η προσφορά πώλησης μικρότερων ποσοτήτων σε χαμηλότερες τιμές (όταν πχ υπάρχει πλεόνασμα αποθεμάτων). Γενικά, τα οφέλη που απολαμβάνουν οι αγοραστές είναι η ελάττωση των γενικών εξόδων αγοράς καθώς και η μείωση των τιμών των προσφερόμενων αγαθών και υπηρεσιών. Παράλληλα οι προμηθευτές ωφελούνται από την ελάττωση των πλεοναζόντων στοκ τους και από τη μείωση των γενικών τους εξόδων, ενώ επιτυγχάνεται η καλύτερη διαχείριση του όγκου παραγωγής.

Παραδείγματα ηλεκτρονικών δημοπρασιών είναι το πρόγραμμα ESPRIT Infomar (περισσότερες πληροφορίες σχετικά με τα προγράμματα ESPRIT και ACTS στη διεύθυνση http://www.ispo.cec.be/ecommerce e/ecomproj.htm και το FastParts (www.fastparts.com). Άλλες πολύ γνωστές διευθύνσεις ηλεκτρονικών δημοπρασιών είναι οι ακόλουθες:

- http://www.ebay.com
- http://auctions.yahoo.com
- http://www.3nsold.com.

### 3.5.1 Τα είδη της δημοπρασίας

1. **Απλές δημοπρασίες ενός αντικειμένου:** Πρόκειται για το πιο διαδεδομένο είδος δημοπρασίας. Στο είδος αυτό ο πωλητής ξεκινάει με την κατώτατη αποδεκτή τιμή πώλησης (starting price) και δέχεται φανερές προσφορές από τους υποψήφιους αγοραστές, συνεχώς αυξανόμενες. Η δημοπρασία διεξάγεται για ορισμένο χρονικό διάστημα και νικητής

ανακηρύσσεται ο τελευταίος που έκανε προσφορά (που προφανώς είναι η μεγαλύτερη).

Το κλειδί για μια επιτυχημένη δημοπρασία αυτού του είδους είναι η ύπαρξη συναγωνισμού μεταξύ των χρηστών που συμμετέχουν, γεγονός που οδηγεί σε όλο και μεγαλύτερες προσφορές. Υπάρχει όμως η περίπτωση κάποιος να κερδίσει την δημοπρασία σε τιμή αρκετά χαμηλότερη της πραγματικής της αξίας, αφού μπορεί να αυξάνει την προσφορά του κατά ένα μικρό ποσό κάθε φορά (ώστε να πλειοδοτεί) και να μην πιέζεται να προσφέρει το ποσό που πραγματικά αποτιμά το αντικείμενο. Για αυτό το λόγο πολλές φορές είναι προτιμότερο να χρησιμοποιηθεί κάποιο άλλο είδος δημοπρασίας που είναι πιο αποδοτικό για τον πωλητή.

2. **Δημοπρασία πολλών αντικειμένων:** Στις δημοπρασίες αυτές δημοπρατούνται περισσότερα από ένα πανομοιότυπα αντικείμενα. Χαρακτηριστικό αυτού του είδους είναι ότι κάθε πλειοδότης θα πληρώσει ακριβώς το ίδιο ποσό με τους υπόλοιπους πλειοδότες, ανεξάρτητα από την προσφορά που έχει κάνει. Το ποσό αυτό είναι ίσο με την μικρότερη επιτυχημένη προσφορά που κερδίζει έστω και ένα αντικείμενο.

3. **Δημοπρασίες ξαφνικού θανάτου:** Αρχικά μοιάζει αρκετά με την απλή δημοπρασία ενός αντικειμένου ή την δημοπρασία πολλαπλών αντικειμένων, όμως στη συνέχεια η διαδικασία είναι τελείως διαφορετική. Τα χαρακτηριστικά είναι τα εξής:

- Ο πωλητής καθορίζει την αρχική τιμή εκκίνησης καθώς και την ελάχιστη τιμή που είναι διατεθειμένος να πουλήσει το αντικείμενα. Αν δεν δώσει ελάχιστη τιμή αυτή ορίζεται ίση με 1.

ð Ο πωλητής καθορίζει τον ρυθμό που μειώνεται η τιμή μιας δημοπρασίας ανά ώρα. Για παράδειγμα , αν ο πωλητής καθορίσει ένα ρυθμό ίσο με 1€ ανά ώρα σε μια δημοπρασία ξαφνικού θανάτου με αρχική τιμή εκκίνησης τα 100€, σε 5 ώρες η δημοπρασία θα έχει τιμή ίση με 95€.

ð Από τη στιγμή που η δημοπρασία εισάγεται στο σύστημα και ο χρόνος λήξης της πλησιάζει, η τιμή της συνεχώς μειώνεται σύμφωνα με το ρυθμό που έχει καθορισθεί. Δεν μπορεί πάντως να πέσει ποτέ κάτω από την ελάχιστη τιμή πώλησης, αν αυτή έχει ορισθεί.

ð Οποιοδήποτε μέλος κάνει προσφορά στην δημοπρασία, αυτομάτως κερδίζει τα τεμάχια που επιθυμεί στην τιμή που υπάρχει εκείνη τη στιγμή. Τα τεμάχια μειώνονται αντίστοιχα και η δημοπρασία συνεχίζεται μέχρι να εξαντληθούν όλα ή να λήξει ο χρόνος διεξαγωγής.

ð Όπως είναι προφανές ένας μπορεί να αγοράσει τεμάχια σε ακριβότερη τιμή από κάποιον άλλο. Όσο νωρίτερα κάνει κάποιος προσφορά, τόσο πιο ακριβά θα αγοράσει (αλλά τόσο μεγαλύτερες πιθανότητες έχει να πάρει τα τεμάχια που επιθυμεί).

Οι δημοπρασίες ξαφνικού θανάτου είναι αρκετά συναρπαστικές μιας και βάζουν τους υποψήφιους αγοραστές σε δίλημμα: να χτυπήσουν την δημοπρασία και να την κερδίσουν ή να περιμένουν να πέσει η τιμή της αλλά με το φόβο κάποιος άλλος να κάνει προσφορά και να μην προλάβουν; Έτσι λοιπόν υπάρχει ένα διαρκές άγχος στους υποψήφιους αγοραστές και αγωνία για την εξέλιξη της.

Σε μερικές περιπτώσεις οι δημοπρασίες ξαφνικού θανάτου είναι πιο επικερδείς για τους πωλητές απ’ ότι οι κανονικές δημοπρασίες:

| **Κανονική δημοπρασία** | **Δημοπρασία ξαφνικού θανάτου** |
|---|---|
| Συνήθως ο υποψήφιος αγοραστής ανεβάζει κάθε φορά την προσφορά του τόσο, όσο χρειάζεται για να κερδίζει. Δεν προσφέρει δηλαδή πάντα το μέγιστο ποσό που είναι διατεθειμένος να ξοδέψει για να αποκτήσει το αντικείμενο. | Ο αγοραστής που πραγματικά θέλει να κερδίσει το αντικείμενο δεν μπορεί να περιμένει πάρα πολύ πριν κάνει προσφορά. Αυτό σημαίνει ότι πιθανότατα η προσφορά θα γίνει αρκετά κοντά στην πραγματική αξία του αντικειμένου. |

**4.** **Δημοπρασίες ενός χτυπήματος:** Στην δημοπρασία αυτή δημοπρατείται ένα μόνο αντικείμενο. Ο πωλητής ορίζει την αρχική τιμή εκκίνησης και η διαδικασία ξεκινάει. Τα ιδιαίτερα χαρακτηριστικά είναι τα εξής:

- Κάθε υποψήφιος αγοραστής έχει την δυνατότητα να κάνει ΜΙΑ ΚΑΙ ΜΟΝΟ προσφορά, καθ' όλη την εξέλιξη της δημοπρασίας. Από την στιγμή που κάνει κάποια προσφορά, δεν μπορεί πλέον να συμμετέχει στην δημοπρασία ξανά.

- Όλες οι προσφορές είναι κλειστές και καμία προσφορά δεν είναι ορατή μέχρι την στιγμή που η δημοπρασία ολοκληρωθεί. Μόνο ο πωλητής μπορεί να βλέπει ανά πάσα στιγμή την εξέλιξη της.

- Μόλις η δημοπρασία τερματιστεί, οι προσφορές ανοίγουν για όλους και νικητής ανακηρύσσεται αυτός που έχει κάνει τη μεγαλύτερη προσφορά.

**Ενδιαφέρον στις δημοπρασίες ενός χτυπήματος παρουσιάζουν τα εξής:**

- Ο υποψήφιος αγοραστής πρέπει να κάνει πραγματικά την μεγαλύτερη προσφορά, στην οποία είναι διατεθειμένος να αγοράσει το αντικείμενο, και

ταυτόχρονα να είναι ευνοϊκή γι’ αυτόν αφού δεν θα έχει άλλη ευκαιρία να το ξαναεπιχειρήσει.

- Από την άλλη πλευρά μια μεγάλη προσφορά κάνει πιο πιθανή την απόκτηση του αντικειμένου όμως αυτό αυξάνει και την πιθανότητα η αγορά να μην είναι αρκετά κερδοφόρα. Μια καλή τακτική είναι η προσφορά ποσού κοντά στην πραγματική αξία του αντικειμένου, αποφεύγοντας την ατυχία που έχει κάποιος να κερδίσει μεν το αντικείμενο αλλά δίνοντας περισσότερα χρήματα από ότι πραγματικά κοστίζει.

Το είδος αυτό της δημοπρασίας χρησιμοποιείται ευρύτατα σε διαγωνισμούς του Δημόσιου Τομέα (διαγωνισμοί με σφραγισμένες προσφορές).

**5.** **<u>Δημοπρασίες χιονοστιβάδος:</u>** Στην δημοπρασία αυτή υλοποιείται ο μηχανισμός της χονδρικής πώλησης. Δηλαδή, αν αγοράσουμε μεγάλη ποσότητα αντικειμένων μπορούμε να επιτύχουμε καλύτερη τιμή ανά μονάδα προϊόντος (χονδρική αντί λιανικής).
Το πρόβλημα παρουσιάζεται στο ότι δύσκολα οι μεμονωμένοι χρήστες μπορούν να αγοράσουν μεγάλες ποσότητες αφού τις περισσότερες φορές δεν τις χρειάζονται. Γι’ αυτό το λόγο, πολλοί μεμονωμένοι αγοραστές συγκροτούν μια ομάδα η οποία προσπαθεί αγοράζοντας πολλά όμοια αντικείμενα να πετύχει καλύτερη τελική τιμή πώλησης από τον πωλητή.

**Διαδικασία υλοποίησης:**

Ο πωλητής των αντικειμένων καθορίζει την αρχική τιμή πώλησης καθώς και τα επίπεδα αγορών στα οποία η ανά μονάδα τιμή μειώνεται. Για παράδειγμα, μπορεί να καθορίσει αρχική τιμή πώλησης τα 100€. Αν αγορασθούν πάνω από 10 αντικείμενα η τιμή αυτή γίνεται 95€, αν αγορασθούν πάνω από 20 αντικείμενα γίνεται 90€ κ.ο.κ. Τελικά κερδισμένοι βγαίνουν τόσο

οι αγοραστές, αφού λειτουργώντας σαν ομάδα πετυχαίνουν καλύτερη τελική τιμή όσο και ο πωλητής αφού διαθέτει μαζικά πολλά αντικείμενα.

**6.** **<u>Δημοπρασία ζήτησης – Αντίστροφη δημοπρασία:</u>** Η δημοπρασία αυτή δημιουργείται από κάποιον που ζητάει να αγοράσει ένα ή περισσότερα αντικείμενα, ακολουθείται δηλαδή η αντίστροφη διαδικασία με αυτήν της κλασσικής δημοπρασίας. Προσφορές πλέον κάνουν οι υποψήφιοι πωλητές, οι οποίοι ανταγωνίζονται μεταξύ τους ώστε να δελεάσουν (συνήθως χαμηλώνοντας τις προσφορές τους) τον δημοπράτη και να του πουλήσουν αυτό που ζητάει.

**Διαδικασία υλοποίησης:**

Ο αγοραστής ορίζει την αρχική τιμή εκκίνησης καθώς και το αν επιτρέπει ελεύθερες ή υποχρεωτικά κατώτερες της τιμής εκκίνησης προσφορές και η διαδικασία ξεκινάει. Τα ιδιαίτερα χαρακτηριστικά μιας αντίστροφης δημοπρασίας (ζήτησης) είναι τα εξής:

- Οι προσφορές που γίνονται είναι δυνατό να συνοδεύονται και από μία περιγραφή που να εξηγεί τι ακριβώς προσφέρεται. Η περιγραφή αυτή μπορεί και να χρησιμοποιηθεί π.χ. από τον πωλητή για να δηλώσει στον αγοραστή ότι του δίνει και επιπλέον παροχές πέρα από αυτό που ζητάει ή για να περιγράψει με ακρίβεια αυτό που έχει στην κατοχή του.

- Ο αγοραστής δεν δεσμεύεται. Μετά το τέλος της διαδικασίας μπορεί να μην αποδεχθεί καμία προσφορά (άσχετα αν ικανοποιούνται φαινομενικά οι όροι του) ή ακόμα και να αποδεχθεί προσφορά που δεν είναι η χαμηλότερη (για λόγους δικούς του).

ü Μετά τη λήξη της δημοπρασίας ο αγοραστής (και δημιουργός της δημοπρασίας ζήτησης) μπορεί να αποδεχθεί μια προσφορά επισκεπτόμενος τη σελίδα των προσφορών. Εκεί υπάρχει κατάλληλο εικονίδιο με το οποίο γίνεται η διαδικασία αποδοχής και ειδοποιείται άμεσα ο πωλητής του οποίου η προσφορά έγινε αποδεκτή. Αποδοχή μιας προσφοράς δηλώνει πρόθεση αγοράς που δεν δύναται να αλλάξει και ενεργοποιεί την δυνατότητα για βαθμολόγηση της συναλλαγής.

ü Μπορεί να γίνει αποδοχή μόνο μιας προσφοράς ανά υποψήφιο πωλητή.

Το ενδιαφέρον σε αυτού του είδους τη δημοπρασία παρουσιάζεται στο γεγονός ότι οι υποψήφιοι πωλητές στην προσπάθειά τους να πουλήσουν το αντικείμενο στον αγοραστή αναγκάζονται να μειώνουν σταδιακά τις προσφορές τους, ώστε να τον δελεάσουν και να τους επιλέξει.

**7. <u>Δημοπρασίες συνεχών πωλήσεων:</u>** Στις δημοπρασίες αυτές δημοπρατούνται ένα ή περισσότερα πανομοιότυπα αντικείμενα. Χαρακτηριστικό αυτού του είδους είναι ότι έχει πολύ μεγάλη διάρκεια (90 ημέρες) καθώς και ότι υποστηρίζεται μόνο η άμεση αγορά αντικειμένων (ουσιαστικά πρόκειται για πώληση και χρησιμοποιείται καταχρηστικά ο όρος δημοπρασία). Η δημοπρασία τερματίζεται μόνο αν εξαντληθεί η διαθέσιμη ποσότητα των αντικειμένων που διατίθενται ή αν ο πωλητής την τερματίσει με δική του ενέργεια.

Οι δημοπρασίες συνεχών πωλήσεων έχουν ιδιαίτερο ενδιαφέρον για πωλητές οι οποίοι έχουν μεγάλο αριθμό όμοιων αντικειμένων και θέλουν να τα διαθέσουν χωρίς να δημιουργούν συνεχώς νέες δημοπρασίες, γλιτώνοντας έτσι πολύτιμο χρόνο.

**8.** **<u>Ανοικτές Δημοπρασίες:</u>** Στην δημοπρασία αυτή δημοπρατείται ένα μόνο αντικείμενο. Ο πωλητής ορίζει την αρχική τιμή εκκίνησης και η διαδικασία ξεκινάει. Η δημοπρασία ακολουθεί ακριβώς τους ίδιους κανόνες με τις δημοπρασίες ενός αντικειμένου.

<u>Το σημείο διαφοροποίησης του είδους αυτού</u> είναι ότι ο πωλητής δεν υποχρεώνεται μετά το τέλος της δημοπρασίας να πουλήσει το αντικείμενο στον μεγαλύτερο πλειοδότη. Είναι στην διακριτική του ευχέρεια αν τελικά θα αποφασίσει κάτι τέτοιο ή όχι. Αν το αποφασίσει, θα πρέπει να επισκεφθεί την σελίδα προσφορών της δημοπρασίας και να αποδεχθεί την προσφορά πατώντας κατάλληλο εικονίδιο που εμφανίζεται δίπλα από το αναγνωριστικό του μεγαλύτερου πλειοδότη.

**Λόγοι ύπαρξης ενός τέτοιου είδους δημοπρασίας:**

- Δημιουργείται ένα κλίμα ελευθερίας προσφορών που είναι δυνατό να δείξει στον πωλητή ποια είναι η πραγματική τιμή πώλησης του αντικειμένου και αν όντως υπάρχει ενδιαφέρον για τη δημοπρασία του.
- Ευκολότερη αποτύπωση της πραγματικής αξίας των αντικειμένων στην ελεύθερη αγορά.
- Δυνατότητα χρήσης αυτού του είδους δημοπρασίας από πωλητές που πωλούν τα ίδια αντικείμενα, ταυτόχρονα, σε διαφορετικά κανάλια πώλησης και επομένως αυξημένη πιθανότητα να «ξεπουλήσουν» στο τέλος της δημοπρασίας.

### <u>3.5.2 Καθορισμός παραμέτρων που διαφοροποιούν τις δημοπρασίες.</u>

- Ποιο ποσό θα πληρώσει ο τελικός πλειοδότης. Αυτό μπορεί να καθορισθεί ίσο με την προσφορά που έκανε ή ίσο με την δεύτερη μεγαλύτερη προσφορά (την προσφορά που έκανε δηλαδή ο αμέσως επόμενος πλειοδότης, αν

υπάρχει βέβαια). Η δεύτερη επιλογή μπορεί να χρησιμοποιηθεί για να αυξήσει τον ανταγωνισμό μεταξύ των υποψήφιων αγοραστών και συναντάται διεθνώς με τον όρο 'first bidder, second price auction'.

- Ελάχιστη τιμή πώλησης, η τιμή δηλαδή κάτω από την οποία δεν θέλει να πουλήσει το αντικείμενο, η οποία είναι άγνωστη για τους υποψήφιους πλειοδότες.

- Τιμή άμεσης αγοράς, η τιμή δηλαδή που κάποιος αγοράζει άμεσα το αντικείμενο και η δημοπρασία λήγει.

- 10% έκπτωση για το χρήστη που κάνει την πρώτη προσφορά. Η έκπτωση θα ισχύσει μόνο αν αυτός είναι και ο τελικός πλειοδότης. Συνήθως ο πωλητής ενεργοποιεί αυτή την επιλογή για να προτρέψει τους χρήστες να ανοίξουν την δημοπρασία του κάνοντας κάποια προσφορά.

- Απόκρυψη χρηστών. Με την επιλογή αυτή μόνο το ύψος των προσφορών θα είναι γνωστό σε όλους ενώ οι χρήστες που κάνουν προσφορές παραμένουν για πάντα κρυφοί. Μόνο ο πωλητής θα γνωρίζει την ταυτότητά τους. Αυτή η επιλογή συνήθως ενεργοποιείται σε δημοπρασίες που είναι ευαίσθητες στην αποκάλυψη των στοιχείων των χρηστών που συμμετέχουν.

- Αυτόματη παράταση δημοπρασίας. Η επιλογή αυτή ενεργοποιείται συνήθως για να αποφευχθούν περιπτώσεις που κάποιοι χρήστες περιμένουν μέχρι το τέλος και κάνουν προσφορά την τελευταία στιγμή για να μην υπάρχει χρόνος να αντιδράσουν οι υπόλοιποι (τεχνική διεθνώς γνωστή με τον όρο snipping). Η επιλογή αυτή παρατείνει τον χρόνο της δημοπρασίας όταν σημειωθεί χτύπημα στην δημοπρασία τα τελευταία 5 λεπτά της εξέλιξής της. Η

παράταση είναι τέτοια που να απομένουν 5 λεπτά από τη στιγμή που θα γίνει το χτύπημα.

### 3.5.3 Ασφάλεια.

Οι σε απευθείας σύνδεση δημοπρασίες μπορούν να χαρακτηρισθούν ως επισφαλείς, δεδομένου ότι οι συμμετέχοντες δεν είναι φυσικά παρόντες. Βασικές λύσεις στα προβλήματα ασφάλειας έρχονται να δώσουν τα ακόλουθα:

p Πιστοποίηση Server: Χρησιμοποιούνται Ψηφιακά Πιστοποιητικά της διεθνώς αναγνωρισμένης εταιρίας ασφαλείας VeriSign, τα οποία πιστοποιούν μοναδικά την ταυτότητα των servers (διακομιστές: υπολογιστικά συστήματα που χρησιμοποιούνται για τη διαχείριση των δικτυακών πόρων) της εταιρίας. Οι σελίδες αυτές έχουν χαρακτηριστικό σήμα ένα λουκέτο που εμφανίζεται στην οθόνη του χρήστη.

p Κρυπτογραφημένη Επικοινωνία: Σε επίπεδο επικοινωνίας μεταξύ χρηστών και servers έχει υιοθετηθεί το πρωτόκολλο SSL (Secure Socket Layers) έως 128bit, η πιο ισχυρή μορφή κρυπτογράφησης σήμερα. Οι σελίδες των servers που εγγυώνται κρυπτογραφημένη επικοινωνία διακρίνονται από το χαρακτηριστικό σήμα του λουκέτου που εμφανίζεται στην οθόνη του χρήστη.

p Πιστοποίηση Χρήστη: Σε πρώτο επίπεδο ελέγχεται με εισαγωγή username και password, που είναι μοναδικοί για κάθε χρήστη, τα οποία εκδίδονται και παραδίδονται με απόλυτη εμπιστευτικότητα. Παράλληλα εκδίδεται επιπλέον κωδικός έγκρισης (Approval Code), μοναδικός για κάθε χρήστη, που εισάγεται στο τελικό στάδιο κάθε συναλλαγής και πιστοποιεί την ταυτότητά του, εξασφαλίζοντας τη μέγιστη δυνατή ασφάλεια στις συναλλαγές.

# Κεφάλαιο 4

# Η κρυπτογραφία στα επικοινωνιακά δίκτυα

## 4.1 Η έννοια της εφαρμογής πολιτικής ασφάλειας.

(Στην παράγραφο που ακολουθεί χρησιμοποιήθηκαν στοιχεία από τις πηγές [12], [19], [51], [52]).

Η έννοια της ασφάλειας των δικτύων ποικίλλει ανάλογα με τις απαιτήσεις του κάθε χρήστη ή οργανισμού που χρησιμοποιεί το εκάστοτε δίκτυο. Γενικά, η δημιουργία ενός ασφαλούς δικτύου (secure network) θα γοήτευε οποιονδήποτε χρήστη! Πρακτικά όμως, τα δίκτυα δε μπορούμε να τα διαχωρίσουμε σε ασφαλή και μη ασφαλή γιατί το επίπεδο ασφαλείας εξαρτάται από το τι θεωρείται «πολύτιμο» για τον κάθε χρήστη.

Για παράδειγμα, ένα ηλεκτρονικό διατραπεζικό σύστημα επιτρέπει σε οικονομικούς οργανισμούς και ιδιώτες να έχουν πρόσβαση στους λογαριασμούς, να πραγματοποιούν διάφορες οικονομικές συναλλαγές και να λαμβάνουν πληροφορίες για σχετικά προϊόντα και υπηρεσίες μέσω δημοσίων ή ιδιωτικών δικτύων, αλλά μια πιθανή τροποποίηση των πληροφοριών αυτών μπορεί να «αποβεί μοιραία» για την υγιή λειτουργία του συστήματος. Συνεπώς, το σύστημα αυτό είναι σημαντικό να περιλαμβάνει μηχανισμούς ασφαλείας που θα αποκλείουν την αλλαγή των δεδομένων από αναρμόδιους.

Για κάποιο άλλο οργανισμό, αντίστοιχα, θα μπορούσε να χαρακτηριστεί ως «ασφαλές δίκτυο» ένα σύστημα που θα εμπόδιζε τους «ξένους» να έχουν πρόσβαση στο εσωτερικό του δίκτυο ή ένα σύστημα με το οποίο θα εξασφάλιζε τη διατήρηση της εμπιστευτικότητας των επικοινωνιών του.

Ουσιαστικά, οι περισσότεροι μεγάλοι οργανισμοί έχουν ανάγκη από έναν «σύνθετο ορισμό της ασφάλειας», ο οποίος θα εξασφαλίζει την προστασία του συστήματος από οποιαδήποτε απειλή προκύψει.

Τώρα, ο διαχειριστής ασφαλείας του δικτύου θα πρέπει να είναι σε θέση να ορίσει την πολιτική ασφαλείας (security policy) του οργανισμού. Η πολιτική αυτή δεν καθορίζει το πώς θα επιτευχθεί η προστασία του συστήματος, αλλά ξεκαθαρίζει επακριβώς τα στοιχεία που πρέπει να προστατεύονται.

Η πολυπλοκότητα για τον εντοπισμό της πλέον κατάλληλης πολιτικής ασφάλειας δικτύου οφείλεται στο γεγονός ότι δεν μπορεί να διαχωριστεί από την πολιτική ασφαλείας που χρησιμοποιείται για τα υπόλοιπα υπολογιστικά συστήματα που είναι συνδεδεμένα στο δίκτυο. Με λίγα λόγια, η πολιτική αυτή θα πρέπει να εφαρμόζεται και για τις πληροφορίες που περνούν από ένα δίκτυο και για τις πληροφορίες που είναι αποθηκευμένες στα υπολογιστικά συστήματα.

Τέλος, μια πολιτική ασφαλείας δεν μπορεί να αποτιμηθεί για τον απλούστατο λόγο ότι η αξία των πληροφοριών που πρέπει να προστατευτούν δε γίνεται να εκτιμηθεί. Επομένως, θα πρέπει να εφαρμοστεί η πολιτική αυτή που θα μεγιστοποιεί το λόγο ωφέλειας κόστος, κάτι που κάνει την εύρεση της καταλληλότερης πολιτικής ασφαλείας ακόμη πιο σύνθετη.

**Η απόδοση ευθυνών και ο διαμοιρασμός αρμοδιοτήτων.**

Πολλοί οργανισμοί δεν έχουν καθορίσει «υπεύθυνο ασφαλείας» των πληροφοριών, με αποτέλεσμα να μπορούν να σχεδιάσουν μια ικανή πολιτική ασφαλείας. Το ζήτημα αυτό μπορεί να διευθετηθεί αν ελέγξουμε την πρόσβαση στις πληροφορίες από δύο διαφορετικές σκοπιές, τον καταλογισμό και την εξουσιοδότηση.

- Καταλογισμός (accountability): Είναι ο τρόπος που τηρείται ένα ίχνος ελέγχου, διαμοιράζονται οι ευθύνες για κάθε στοιχείο δεδομένων στις αρμόδιες

ομάδες και ξεκαθαρίζεται ο τρόπος που θα τηρείται μια καταγραφή για την πρόσβαση και την αλλαγή.

- Εξουσιοδότηση (authorization): Αφορά στην απόδοση ευθυνών για κάθε στοιχείο πληροφοριών και στο πώς ανατίθενται σε άλλους. Δηλαδή ορίζει το ποιος είναι υπεύθυνος για το πού βρίσκονται οι πληροφορίες και πώς ένα υπεύθυνο άτομο εγκρίνει την πρόσβαση σε αυτές, καθώς και την αλλαγή αυτών.

**Οι μηχανισμοί διασφάλισης της ακεραιότητας.**

Οι μέθοδοι που χρησιμοποιούνται, για να εξασφαλίζεται η ακεραιότητα των δεδομένων από σκόπιμες αλλαγές είναι αυτές που κωδικοποιούν τα μεταδιδόμενα δεδομένα με ένα κώδικα πιστοποίησης μηνύματος (message authentication code, MAC), ο οποίος είναι αδύνατο να πλαστοποιηθεί από μη εξουσιοδοτημένο χρήστη ή πιθανό «παράνομο» εισβολέα.

Οι μέθοδοι αυτές χρησιμοποιούν μηχανισμούς κρυπτογραφικού κατακερματισμού (cryptographic hashing). Μία μέθοδος κρυπτογραφικού κατακερματισμού, για παράδειγμα, μπορεί να χρησιμοποιεί ένα απόρρητο κλειδί το οποίο γνωρίζουν μόνο ο αποστολέας και ο παραλήπτης του μηνύματος και χρησιμοποιείται στην κωδικοποίηση/ αποκωδικοποίηση του μηνύματος. Έτσι, ένας εισβολέας δεν μπορεί να διαβάσει το μήνυμα χωρίς να προκαλέσει λάθος και ο παραλήπτης γνωρίζει ότι το μήνυμα που θα αποκωδικοποιηθεί θα είναι και το αυθεντικό (παράδειγμα εφαρμογής συμμετρικής κρυπτογραφίας).

**Κωδικοί ελέγχου πρόσβασης- passwords.**

Ένας μηχανισμός ελέγχου πρόσβασης (password) χρησιμοποιείται από αρκετά υπολογιστικά συστήματα, έτσι ώστε να ελέγχεται η πρόσβαση στους πόρους τους. Ο κάθε χρήστης του συστήματος έχει ένα password το οποίο χρησιμοποιεί για να έχει πρόσβαση σε ένα προστατευόμενο πόρο. Ο

μηχανισμός αυτός είναι αποτελεσματικός σε ένα συμβατικό υπολογιστικό σύστημα, επειδή δεν αποκαλύπτονται οι κωδικοί αυτοί σε τρίτους.

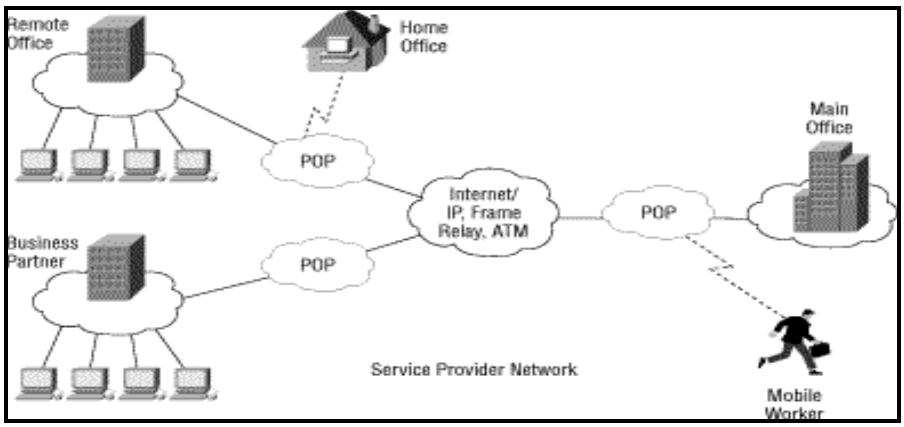
Δεν μπορούμε όμως να ισχυριστούμε πως το ίδιο συμβαίνει σε ένα δίκτυο, αφού ο εκάστοτε κωδικός πρόσβασης είναι εκτεθειμένος στην «κατασκοπεία» όταν αυτός μεταβιβάζεται. Αυτό συμβαίνει γιατί όποιος υποκλέπτει το δίκτυο μπορεί να αποκτήσει ένα αντίγραφο του κωδικού, όσο αυτός μεταφέρεται διαμέσου δικτύου.

Ιδιαίτερα εύκολη τη δουλειά των «υποκλοπέων» κάνει η χρήση κάποιου τοπικού δικτύου (LAN), εξαιτίας των πολλών τεχνολογιών LAN που επιτρέπουν σε οποιοδήποτε συνδεδεμένο κόμβο να συλλαμβάνει και να ανακτά ένα αντίγραφο όλων των πακέτων που ταξιδεύουν μέσω του δικτύου.

## 4.2 Τα Ιδεατά Ιδιωτικά Δίκτυα.

(Στην παράγραφο που ακολουθεί χρησιμοποιήθηκαν στοιχεία από τις πηγές [4], [5], [15)], [23], [35], [36]).

Τα Ιδεατά Ιδιωτικά Δίκτυα είναι ένας τρόπος διασύνδεσης δύο ή περισσοτέρων σημείων χρησιμοποιώντας ως υποδομή ένα δίκτυο δημόσιας χρήσης το οποίο εγγυάται την ασφάλεια της πληροφορίας από τρίτους. Δηλαδή με τέτοια δίκτυα μπορούμε να συνδέσουμε πολλά απομακρυσμένα σημεία μιας επιχείρησης, πιθανώς τους συνεργάτες της, του προμηθευτές της και τους πελάτες της με τέτοιο τρόπο ώστε η επιχείρηση να λειτουργεί ιδιωτικά, ταχύτερα, οικονομικότερα και αποτελεσματικότερα (εικόνα 23).




**Εικόνα 23:** Απεικόνιση Ιδεατού Ιδιωτικού Δικτύου.

## Γιατί χρησιμοποιούμε Ιδεατά Ιδιωτικά Δίκτυα;

**:** Η επιβίωση μιας επιχείρησης στις μέρες μας δεν είναι εύκολη υπόθεση εξαιτίας του ανταγωνισμού. Τα στελέχη θα πρέπει να έχουν πρόσβαση στα αρχεία της επιχείρησης ανά πάσα στιγμή. Με αυτό τον τρόπο θα μπορούν να λάβουν έγκυρα σωστές αποφάσεις πέραν του γραφείου από το σπίτι τους ή από οποιοδήποτε άλλο χώρο.

**:** Ακόμα όμως και στο εσωτερικό περιβάλλον της επιχείρησης η χρήση των Ιδεατών Ιδιωτικών Δικτύων (VPNs) είναι σημαντική. Τα κόστη που προκύπτουν από τη σχέση μιας εταιρίας με τον έξω από αυτήν κόσμο είναι μεγάλα. Για παράδειγμα αν οι πελάτες μπορούσαν να παραγγέλνουν απευθείας μέσα από το μηχανογραφικό σύστημα μιας εταιρίας και αντίθετα με τον ίδιο τρόπο τα στελέχη της εταιρίας από τους προμηθευτές της, τότε το κόστος θα μειωνόταν. Τα οικονομικά οφέλη και τα πλεονεκτήματα θα ήταν μεγαλύτερα εάν όλη αυτή η ιδέα επεκτεινόταν στα υποκαταστήματα και στους αντιπροσώπους. Θα υπήρχε ταχύτητα στην επικοινωνία, καλύτερη αξιοποίηση προσωπικού, ταχύτερη εξυπηρέτηση άρα αυξημένη αποτελεσματικότητα και εγκυρότητα.

**:** Η τεχνολογία των Ιδεατών Ιδιωτικών Δικτύων παρέχει την ενδοεταιρική τηλεφωνία μεγάλων αποστάσεων χωρίς χρονοχρέωση. Αν τα σημεία που συνδέονται με ένα τέτοιο δίκτυο βρίσκονται σε διαφορετικές πόλεις, η οικονομία που προκύπτουν από τους λογαριασμούς των τηλεφώνων είναι σημαντικές.

### 4.2.1 Οικονομικά οφέλη από την χρήση Ιδεατών Ιδιωτικών Δικτύων έναντι της παραδοσιακής δικτύωσης ευρείας περιοχής:

1. Η χρήση του δημόσιου δικτύου σημαίνει πολύ μικρότερα τηλεπικοινωνιακά κόστη, 20-80% ανάλογα με τον αριθμό των σημείων που θα συνδεθούν και των μεταξύ τους αποστάσεων.
2. Ο εξοπλισμός που χρησιμοποιείται για την υλοποίηση των Ιδεατών Ιδιωτικών Δικτύων συμπεριλαμβάνεται στην τιμή διάθεσή τους με την μορφή της ενοικίασης.
3. Η εγκατάσταση, η παρακολούθηση, η διαχείριση και η συντήρησή τους συμπεριλαμβάνονται στην αρχική τιμή τους. Αυτό σημαίνει ότι η επιχείρηση δεν επιβαρύνεται με επιπλέον κόστος όπως είναι το προσωπικό συντήρησης.

### 4.2.2 Μορφές Ιδεατών Ιδιωτικών Δικτύων (VPNs).

Υπάρχουν τρεις μορφές Ιδεατών Ιδιωτικών Δικτύων ανάλογα με τη ζητούμενη λειτουργικότητα: intranet, extranet και access VPNs.

@ Intranet VPNs : Τα Intranet VPNs αφορούν στη σύνδεση των γραφείων και των υποκαταστημάτων μιας εταιρείας. Στοχεύουν στον κεντρικό έλεγχο της υποδομής της εταιρείας, δηλαδή στο να επιτραπεί ακόμα και στα πιο απομακρυσμένα σημεία να χρησιμοποιούν την υποδομή (εφαρμογές λογιστικής,

αποθήκης, ανθρώπινων πόρων, μισθοδοσίας, ή άλλες εξειδικευμένες εφαρμογές) απευθείας από τα κεντρικά γραφεία της εταιρείας. Επίσης, εφαρμόζεται και η ενδοεταιρική τηλεφωνία, επιτρέποντας την επικοινωνία μεταξύ όλων αυτών των σημείων με εσωτερικές κλήσεις.

@ Extranet VPNs: Το extranet ιδεατό ιδιωτικό δίκτυο επεκτείνεται και στους συνεργάτες, πελάτες, προμηθευτές, δίκτυο μεταπωλητών κλπ. Η λειτουργικότητα είναι η ίδια, με εξαίρεση την εκτενέστερη πρόσβαση του κάθε μέλους του VPN στους πόρους της εταιρείας, ανάλογα με τα δικαιώματα που επιθυμεί η εταιρεία να αναθέσει. Η τηλεφωνία μεταξύ των εταιρειών εφαρμόζεται με μηδενικό κόστος για την επικοινωνία μεταξύ των εταιρειών που συμμετέχουν στο Ιδεατό Ιδιωτικό Δίκτυο.

@ Access VPNs**:** Τα access VPNs αφορούν στη σύνδεση μεμονωμένων στελεχών στο εταιρικό δίκτυο, από το σπίτι ή σε περιοδεία. Με αυτό το τρόπο κάποιο στέλεχος αποκτά πλήρη πρόσβαση στο εταιρικό δίκτυο, ίδια με αυτήν που θα είχε αν βρισκόταν στο γραφείο του μέσα στην επιχείρηση. Μπορεί να χρησιμοποιήσει την ενδοεταιρική τηλεφωνία μέσω του προσωπικού του υπολογιστή.

### 4.2.3 Προστατεύοντας το Δίκτυο: Ασφάλεια και Μηχανισμοί .

Οι διάφορες επιχειρήσεις θέλουν να είναι σίγουρες για την ασφάλεια που τους παρέχει το VPN δίκτυό τους, απέναντι σε εισβολείς που παρακολουθούν ή αλλοιώνουν δεδομένα της εταιρίας που μετακινούνται στο δίκτυο. Αυτό το πετυχαίνουν με την κρυπτογράφηση, την πιστοποίηση και τον έλεγχο πρόσβασης.

Τα βασικά στοιχεία ενός VPN δικτύου που αλληλοσυμπληρώνονται έτσι ώστε να παρέχουν ασφάλεια είναι:

- Τα Τούνελ και η Κρυπτογράφηση
- Η Πιστοποίηση Πακέτων
- Τα Firewalls και η Ανίχνευση Εισβολών
- Η Πιστοποίηση Χρηστών

**Τούνελ και Κρυπτογράφηση.**

Τα ιδεατά ιδιωτικά δίκτυα εφαρμόζουν την τεχνική των κρυπτογραφημένων τούνελ για τους ακόλουθους τρεις λόγους:

- για να προστατέψουν τα δεδομένα από το να αλλοιωθούν
- για να παρακολουθούν παράνομες οντότητες και
- για να πραγματοποιήσουν, εάν είναι αναγκαίο, την «κράτηση» πολλαπλών πρωτοκόλλων.

Σκοπός της τεχνικής αυτής είναι το μπέρδεμα των δεδομένων κάνοντας τα έτσι επεξεργάσιμα μόνο σε αυτούς για τους οποίους προορίζονται και από αυτούς που έχουν το δικαίωμα να τα στείλουν. Σε εφαρμογές όπου η ασφάλεια έρχεται σε δεύτερο λόγο, μπορεί να γίνει εφαρμογή της μεθόδου των τούνελ χωρίς τη χρήση κρυπτογράφησης.

Πιστοποίηση Πακέτων: Κατά την διακίνηση μιας πληροφορίας σημαντικό ρόλο παίζει η ακεραιότητα της. Σε ένα μη ασφαλές δίκτυο οι πληροφορίες μπορούν να υποκλαπούν, να τροποποιηθούν και να φτάσουν τελικά στο προορισμό τους παραποιημένες. Την λύση σε τέτοια προβλήματα δίνει η πιστοποίηση πακέτων. Σε κάθε πακέτο (πληροφορία) επικολλάται μια επικεφαλίδα, η οποία εξασφαλίζει την ζητούμενη ακεραιότητα.

Firewalls και Ανίχνευση Εισβολών, Καταγραφή Δεδομένων Ασφάλειας και Πιστοποίηση Χρηστών : Τα ιδεατά ιδιωτικά δίκτυα χρησιμοποιούν Firewalls, συστήματα για ανίχνευση εισβολών (πχ NetRanger), για καταγραφή δεδομένων ασφάλειας και ανίχνευση πιθανών ελλείψεων σε αυτήν (πχ

NetSonar) και συστήματα για πιστοποίηση χρηστών (πχ RADIUS και TACACS+).

**Το μέλλον.**

Μελλοντικά, τα ιδεατά ιδιωτικά δίκτυα θα παρέχουν υπηρεσίες σε όλα τα επίπεδα της ηλεκτρονικής επικοινωνίας των επιχειρήσεων. Στις υπηρεσίες αυτές θα περιλαμβάνονται η παραδοσιακή τηλεφωνική επικοινωνία και η δημιουργία του μοναδικού σημείου σύνδεσης της επιχείρησης με τον έξω από αυτή κόσμο, για όλες τις ανάγκες της.

## 4.3Ασύρματα Δίκτυα.

(Στην παράγραφο που ακολουθεί χρησιμοποιήθηκαν στοιχεία από τις πηγές [5], [6], [16], [19], [32], [44]).

Ένα ασύρματο δίκτυο είναι ένα τηλεφωνικό ή υπολογιστικό δίκτυο το οποίο χρησιμοποιεί ραδιοκύματα για την μεταφορά των πληροφοριών. Δηλαδή, η ανταλλαγή των δεδομένων μεταξύ υπολογιστών ή συσκευών γίνεται χωρίς να χρησιμοποιούνται καλώδια.

### 4.3.1 Κατηγορίες ασύρματων δικτύων.

Ένα ασύρματο δίκτυο μπορεί να είναι Τοπικό (WLAN), Μητροπολιτικό (WMAN) ή Ευρείας Περιοχής (WWAN), ενώ μια κλίμακα μεγέθους κάτω από αυτά είναι τα Ασύρματα Προσωπικά Δίκτυα.

**1. Τα Ασύρματα Τοπικά Δίκτυα (Wireless Local Area Networks – WLANs)** αποτελούν επεκτάσεις ή ανταγωνιστική τεχνολογία των σταθερών τοπικών δικτύων σε κτήρια ή περιοχές μικρού εύρους. Πολλαπλά φέροντα περιπλέκονται με βάση κυρίως την τεχνική διάχυτου φάσματος (spread-

spectrum), η οποία καταναλώνει μεγαλύτερο εύρος ζώνης σε σχέση με ανταγωνιστικές τεχνολογίες, εντούτοις προσφέρει υψηλές ταχύτητες. Τα συγκριτικά πλεονεκτήματα των Wireless LAN είναι:

- Η ευκολία και η ταχύτητα εγκατάστασης και λειτουργίας,
- Το χαμηλό λειτουργικό κόστος και το κόστος εξάπλωσης,
- Οι υψηλοί ρυθμοί μετάδοσης και λήψης δεδομένων,
- Οι μεγάλες δυνατότητες κλιμάκωσης.

**2.** **WMAN - Ασύρματα Μητροπολιτικά Δίκτυα**. Αυτά τα δίκτυα καλύπτουν μια γεωγραφική περιφέρεια (π.χ. μιας πόλης) .

**3.** **WWAN – Ασύρματα Δίκτυα Ευρείας Περιοχής** . Είναι τα δίκτυα για τα οποία χρησιμοποιείται τεχνολογία σχεδιασμένη να καλύπτει μια μεγάλη γεωγραφική περιφέρεια (π.χ. τα όρια μιας χώρας ή μιας ολόκληρης ηπείρου). Μειονέκτημα τους είναι ότι έχουν μεγάλη καθυστέρηση διάδοσης .

Γενικά, τα ασύρματα δίκτυα ακολουθούν κάποια πρωτόκολλα και πρότυπα μοντέλα τα οποία ορίζονται από Διεθνείς Οργανισμούς όπως το Ινστιτούτο Ηλεκτρολόγων Μηχανικών το οποίο ορίζει τα πρωτόκολλα.

### 4.3.2 Πρωτόκολλα που χρησιμοποιούνται στα ασύρματα τοπικά δίκτυα.

Τα Ασύρματα Τοπικά Δίκτυα χρησιμοποιούν τα πρωτόκολλα 802.11x., τα οποία περικλείουν πολλαπλά διαφορετικά πρωτόκολλα. Ο διαχωρισμός τους γίνεται από τα τελευταία γράμματα που υποδεικνύουν τις διάφορες ταχύτητες και συχνότητες που χρησιμοποιούνται. Το 802.1x είναι ένα σύγχρονο πρότυπο για πιστοποίηση σε ασύρματα δίκτυα με βασικό πλεονέκτημα ότι επιτρέπει στον κάθε χρήστη να χρησιμοποιεί κρυπτογράφηση στην ανταλλαγή δεδομένων μέσω του ασύρματου δικτύου.

Παρακάτω παρουσιάζονται τα πρωτόκολλα 802.11 που έχουν εμφανιστεί στην αγορά*:*

1. **Κλασικό 802.11.** Πλέον δεν χρησιμοποιείται. Έχει ρυθμό μετάδοσης 1-2 Mbps, συχνότητες μετάδοσης στην ζώνη των 2,4GHz.

2. **802.11b ή Wi-Fi.** Είναι εμπορικά το πιο επιτυχημένο. Έχει ρυθμό μετάδοσης 11 Mbps και συχνότητες μετάδοσης στη ζώνη των 2,4GHz.

3. **802.11g.** Είναι ο πιθανός διάδοχος του Wi-Fi. Έχει ρυθμό μετάδοσης 54 Mbps και συχνότητες μετάδοσης στην ζώνη των 2,4GHz.

4. **802.11a.** Πρωτοεμφανιζόμενο, έχει ρυθμό μετάδοσης 54 Mbps και συχνότητες μετάδοσης στην ζώνη των 5 GHz.

### 4.3.3 Ασύρματα προσωπικά δίκτυα.

Όπως προαναφέρθηκε μια ακόμα μορφή ασύρματων δικτύων είναι τα Ασύρματα Προσωπικά Δίκτυα (WPAN) τα οποία είναι χρήσιμα για την δικτύωση προσωπικών συσκευών μέσα στα όρια μιας μικρής περιοχής. Αυτά τα δίκτυα χρησιμοποιούν πρωτόκολλα όπως το Bluetooth ή τα HiperLAN.

Το **Bluetooth** πήρε το όνομα του από τον Harald Bluetooth, έναν Δανό βασιλιά που κατάφερε να ενώσει τις σκανδιναβικές χώρες. Όμως η ύπαρξη του μπορεί να μας ήταν άγνωστη αν η Ericsson δεν είχε δώσει το όνομα του στο νέο πρωτόκολλο ασύρματης επικοινωνίας που ανέπτυξε σε συνεργασία με άλλες μεγάλες εταιρίες όπως: IBM, Toshiba, Nokia, Motorola και υποστηρίζεται από ακόμα 1900 εταιρίες.

**Εικόνα 24**: Bluetooth.

Το Bluetooth (εικόνα 24) υποστηρίζει τόσο την άμεση επικοινωνία ανάμεσα σε δύο συσκευές (point to point) όσο και την επικοινωνία πολλών συσκευών. Η χωρητικότητά του είναι 8 συσκευές ανά δίκτυο, αλλά η μέθοδος εναλλαγής συχνοτήτων επιτρέπει σε περισσότερα από ένα δίκτυα να συνυπάρχουν στον ίδιο χώρο. Η ελάχιστη απόσταση ανάμεσα στον πομπό και το δέκτη είναι 10 εκατοστά και η μέγιστη 10 μέτρα.

Το Bluetooth είναι μια τεχνολογία δικτύωσης η οποία:

1. Δεν βασίζεται:

ü στον έλεγχο του χρήστη καθώς μπορεί να εντοπίσει αυτόματα και να επικοινωνήσει με άλλες συσκευές Bluetooth .

ü σε μεγάλα ποσά ενέργειας για αυτό και είναι ιδανικό για κινητές συσκευές που λειτουργούν με μπαταρία.

2. Επιπροσθέτως, δεν παρέχει ιδιαίτερα υψηλό επίπεδο ασφάλειας, ωστόσο η μικρή του εμβέλεια περιορίζει τον κίνδυνο.

3. Τέλος, το Bluetooth είναι αυτό που αναμένεται να έχει την πιο άμεση επικράτηση όλων των πρωτοκόλλων, κυρίως λόγω του χαμηλού του κόστους και της ευκολίας που προσφέρει.

Το πρωτόκολλο **HiperLan** αναπτύσσεται από το Ευρωπαϊκό Ινστιτούτο Τυποποίησης Τηλεπικοινωνιών (ETSI) και υποστηρίζεται από διάφορες εταιρίες

του χώρου. Μέχρι στιγμής προϊόντα που να στηρίζονται στο πρωτόκολλο αυτό παράγονται μόνο από λίγες εταιρίες. Το HiperLAN έχει την δυνατότητα της αυτόματης προώθησης των δεδομένων. Επίσης, υπερέχει στην ταχύτητα και έχει Δυνατότητα Ποιότητας Υπηρεσιών QoS (Quality Of Service). Με το QoS μπορούν τα πακέτα δεδομένων να κατηγοριοποιούνται και να αποκτούν διαφορετική σειρά προτεραιότητας. Ανάλογα με το είδος τους διακρίνονται σε δύο τύπους:

**u** Hiperlan Type 1: Πρόκειται για ένα πρότυπο τοπικού ασύρματου δικτύου το οποίο προορίζεται για τη δημιουργία υψηλών επιδόσεων ασύρματου δικτύου χωρίς την ύπαρξη ενσύρματης υποδομής. Πολλαπλά HIPERLAN μπορούν να συνυπάρξουν στην ίδια γεωγραφική περιοχή, χωρίς να επηρεάζονται μεταξύ τους. Το HIPERLAN/1 μπορεί επίσης να χρησιμοποιηθεί για την επέκταση των ενσύρματων τοπικών δικτύων.

Το HIPERLAN/1 μπορεί να προσφέρει διασύνδεση που βασίζεται σε κατευθυνόμενη επικοινωνία του τύπου one-to-one ή σε μεταδόσεις του τύπου one-to-many. Ο ρυθμός μετάδοσης φτάνει τα 19Mbit/s, ενώ η μπάντα λειτουργίας βρίσκεται στα 5GHz.

**v** Hiperlan Type 2: Η ραδιοεπαφή αυτή προορίζεται για να παρέχει ασύρματη πρόσβαση μικρής εμβέλειας (30m σε εσωτερικούς χώρους, έως και 150m σε εξωτερικούς) σε χρήστες ακίνητων ή κινούμενων τερματικών από τοπικό επίπεδο σε δίκτυα υποδομής IP, ATM και UMTS. Η επικοινωνία αυτή επιτυγχάνεται μέσω των σημείων πρόσβασης (Access Points) τα οποία είναι συνδεδεμένα απευθείας στο δίκτυο κορμού ενός δικτύου IP, ATM ή UMTS.

Τα δίκτυα HIPERLAN/2 έχουν δυνατότητες υποστήριξης μεταπομπών συνδέσεων μεταξύ των access points και των σταθμών βάσης των άλλων δικτύων 3$^{ης}$ γενιάς. Επιπλέον, από την πλευρά του χρήστη, ένα τέτοιο δίκτυο, διαθέτοντας τους απαιτούμενους ρυθμούς μετάδοσης, θα πρέπει να παρέχει την ποιότητα υπηρεσίας (QoS) αντίστοιχης των δικτύων IP και ATM. Έτσι, στο

HIPERLAN/2 υποστηρίζονται ρυθμοί μέχρι και 25Mbit/s, ενώ η μπάντα συχνοτήτων είναι η ίδια με αυτή του τύπου 1 (5GHz).

### 4.3.4 Ασφάλεια ασύρματων δικτύων.

Βασική προϋπόθεση για την ασφάλεια των Ασύρματων Δικτύων είναι η κρυπτογράφηση των δεδομένων που μεταφέρονται. Δηλαδή η διαδικασία μετατροπής των δεδομένων σε μία μορφή η οποία είναι αναγνωρίσιμη και κατανοητή μόνο από αυτούς που διαθέτουν μία ειδική πληροφορία, το κλειδί. Όσο πιο μεγάλο είναι το μέγεθος του κλειδιού – μετριέται σε bits – τόσο πιο δύσκολη είναι η αποκρυπτογράφησή του, δηλαδή η αποκάλυψη των δεδομένων. Για την κρυπτογράφηση των δεδομένων που μεταφέρονται μέσω ασύρματων δικτύων έχουν ήδη αναπτυχθεί πάρα πολλά πρότυπα.

Τα πιο διαδεδομένα είναι:

- Προστασία Ασύρματου Ισοδύναμη με Ενσύρματη (ΠΑΙΕ, WEP - Wired Equivalent Privacy): Αν και προσφέρει ένα επίπεδο προστασίας, δεν θεωρείται ιδιαίτερα αξιόπιστη. Μάλιστα υπάρχει συγκεκριμένη τεχνική, γνωστή ως «Επίθεση Καφέ Λάττε» (Caffe Latte Attack), με την οποία μέσα σε πολύ λίγα λεπτά αποκαλύπτεται το κλειδί κρυπτογράφησης του πρωτοκόλλου ΠΑΙΕ που χρησιμοποιήθηκε σε ένα ασύρματο δίκτυο. Αν και δεν αποτελεί την καλύτερη λύση, η τεχνολογία αυτή μπορεί να προστατέψει τα ασύρματα δίκτυα από "ερασιτέχνες" εισβολείς.

- Ασύρματη Προστατευμένη Πρόσβαση (ΑΑΠ, WPA - Wi-fi Protected Access). Αναπτύχθηκε από την συμμαχία WiFi (WiFi Alliance) με σκοπό να αντικαταστήσει το πρότυπο ΠΑΙΕ. Προσφέρει υψηλότερο επίπεδο ασφαλείας και είναι πιο εύκολη στη χρήση και στην παραμετροποίηση. Κυρίως χρησιμοποιείται σε επιχειρησιακά περιβάλλοντα γιατί στην πλειοψηφία των

οικιακών ασύρματων δικτύων η κρυπτογράφηση των δεδομένων εξακολουθεί να γίνεται βάση της ΠΑΙΕ.

Η τελευταία έκδοση της είναι η Ασύρματη Προστατευμένη Πρόσβαση 2 η οποία ενσωματώνει πρόσθετα πρωτόκολλα πιστοποίησης και πολύ πιο ισχυρούς αλγόριθμους κρυπτογράφησης.

Η επιλογή χρήσης κάποιου από τα παραπάνω πρότυπα εξαρτάται από την συσκευή πρόσβασης του Ασύρματου Δικτύου. Σε κάθε περίπτωση πάντως η ενεργοποίηση της κρυπτογράφησης των δεδομένων είναι απαραίτητη για την κωδικοποίηση, την ταυτοποίηση των δεδομένων καθώς και για την εξουσιοδότηση των κόμβων έτσι ώστε να εξασφαλίζετε η ασφάλεια. Για αυτό και όλες οι σύγχρονες συσκευές πρόσβασης και δρομολόγησης ενσωματώνουν μία ή περισσότερες τεχνικές κρυπτογράφησης.

**Δύο ακόμα μέθοδοι προστασίας των ασύρματων δικτύων:**

- Συστήματα Ανίχνευσης Εισβολής (ΣΑΕ, IDS – Intrusion Detection Systems): έχουν κυρίως παθητικό ρόλο αφού μπορούν να ανιχνεύσουν προσπάθειες κακόβουλης εισβολής σε ένα δίκτυο και να ενημερώσουν το διαχειριστή του, αλλά δεν μπορούν να τις αποτρέψουν.

- Συστήματα Πρόληψης Εισβολής (ΣΠΕ, IPS – Intrusion Prevention Systems): αντίθετα, τα ΣΠΕ, που στηρίζονται σε πιο προηγμένη τεχνολογία όταν ανιχνεύουν μία προσπάθεια εισβολής αυτομάτως προσπαθούν να την αποτρέψουν εφαρμόζοντας διάφορες τεχνικές.

Τόσο τα Συστήματα Ανίχνευσης Εισβολής όσο και τα Συστήματα Πρόληψης Εισβολής μπορούν να υλοποιηθούν ως λογισμικό ή ως συσκευή και βρίσκουν εφαρμογή τόσο στα ενσύρματα όσο και στα ασύρματα δίκτυα.

Πολύ σημαντική, ιδίως σε επιχειρηματικά περιβάλλοντα, είναι η ενημέρωση και η εκπαίδευση των χρηστών των ΑΤΔ σε θέματα ασφαλείας. Η ενημέρωση για τους κινδύνους που εγκυμονούν και η εφαρμογή αυστηρών πολιτικών ασφαλείας είναι επιτακτικά μέτρα για την αύξηση του επιπέδου ασφαλείας.

## 4.4 Το δίκτυο GSM - Κινητή τηλεφωνία.

(Στην παράγραφο που ακολουθεί χρησιμοποιήθηκαν στοιχεία από τις πηγές [19], [21], [32], [45], [46]).

Κάνοντας μια μικρή ιστορική αναδρομή θα πρέπει να αναφέρουμε ότι κινητά τηλέφωνα υπήρχαν πολύ πριν τη δημιουργία δικτύων GSM, ωστόσο υπόκειντο σε πολλούς περιορισμούς. Η αρχή έγινε τη δεκαετία του 1950 στη Βόρεια Αμερική και την Κεντρική και Βόρεια Ευρώπη, όπου οι συσκευές κινητής τηλεφωνίας είχαν το μέγεθος βαλίτσας και έμπαιναν στον αποθηκευτικό χώρο των αυτοκινήτων και συνοδεύονταν από ένα ακουστικό που ήταν στο χώρο των επιβατών (Εικόνα 25).


**Εικόνα 25:** Τηλέφωνο αναλογικής εποχής .

Εκείνη την περίοδο και ως τις αρχές της δεκαετίας του 1980 τα δίκτυα ήταν αναλογικά. Για να τηλεφωνήσει κάποιος θα έπρεπε:

- Να καλέσει μέσω τηλεφωνικού κέντρου και με την προϋπόθεση ότι τη στιγμή που καλούσε υπήρχε ελεύθερη γραμμή. Αν όλες οι γραμμές ήταν κατειλημμένες, τότε δε μπορούσε να πραγματοποιηθεί κλήση.
- Επίσης, ο καλών θα έπρεπε να γνωρίζει σε ποια περιοχή κινούνταν το άτομο το οποίο ήθελε να καλέσει στο τηλέφωνο.

Πάνω απ' όλα οι πρώτοι χρήστες κινητών τηλεφώνων ήταν οπλισμένοι με πολλή υπομονή, καθώς τα δίκτυα ήταν κακοφτιαγμένα και περιορισμένα, οι νέοι πελάτες έπρεπε να περιμένουν αρκετούς μήνες ακόμη και έναν ολόκληρο χρόνο μέχρι να εγκριθεί η σύνδεσή τους.

Εν τω μεταξύ, μετά την έλευση του τρανζίστορ οι συσκευές περιορίστηκαν στο μέγεθος, φτάνοντας το μέγεθος ενός κουτιού (Εικόνα 26).

**Εικόνα 26**: Συσκευή τηλεφώνου.

Στις αρχές της δεκαετίας του 1980 εγκαινιάζονται νέα δίκτυα τα οποία αν και αναλογικά ήταν πιο εκτεταμένα. Παράλληλα προσέφεραν περισσότερες δυνατότητες, κυρίως ότι πλέον ήταν εφικτό να καλέσει κάποιος άμεσα το άτομο που επιθυμούσε χωρίς να παρεμβαίνει κάποιο τηλεφωνικό κέντρο.

Αν και οι συσκευές δεν είχαν πλέον το μέγεθος που είχαν αυτές της δεκαετία του '50, το βάρος τους έφτανε τα 2,5 κιλά και ο κόσμος που τα χρησιμοποιούσε κυκλοφορούσε με μία μικρή συσκευή.

Παράλληλα στις ΗΠΑ ξεκίνησαν προσπάθειες από τις αρχές της δεκαετίας του '70 με πρωτοπόρο τη Motorola και την Bell να στήσουν τα πρώτα πραγματικά δίκτυα κινητής τηλεφωνίας και να κατασκευάσουν τα πρώτα κινητά τηλέφωνα.

Η Motorola παρουσίασε το πρώτο κανονικό και λειτουργικό κινητό τηλέφωνο το 1973, ενώ το πρώτο δίκτυο στήθηκε το 1978. Ωστόσο οι ΗΠΑ έμειναν τεχνολογικά πίσω από την Ευρώπη, η οποία καθιέρωσε το GSM προσφέροντας περισσότερες υπηρεσίες και καλύτερη απόδοση στους συνδρομητές.

### 4.4.1 Η έλευση του GSM .

Στις 7 Σεπτεμβρίου 1987 υπεγράφη στην Κοπεγχάγη συμφωνία μεταξύ εκπροσώπων 13 τηλεπικοινωνιακών οργανισμών ευρωπαϊκών χωρών, η οποία προέβλεπε την ανάπτυξη ενός διασυνοριακού ψηφιακού δικτύου κινητής τηλεφωνίας που θα κάλυπτε όλες τις συμμετέχουσες χώρες. Η συμφωνία προέβλεπε τα δίκτυα να κατασκευαστούν λεπτομερώς και η ισχύς του σήματος τους να είναι πολύ ισχυρή, έτσι ώστε οι συσκευές να καταναλώνουν παρά πολύ λίγη ενέργεια. Έτσι:

- μειώθηκε η διάρκεια λειτουργίας των συσκευών
- έγινε μικρότερο και πιο πρακτικό το μέγεθός τους,
- ενώ ταυτόχρονα δίνεται η δυνατότητα πραγματοποίησης αυτοματοποιημένης κλήσης και χωρίς περιορισμούς από το δίκτυο.

Με αυτό τον τρόπο γεννήθηκε το GSM (Global System for Mobile Communication).

**GSM** είναι ένα κυψελοειδές ψηφιακό σύστημα αμφίδρομης επικοινωνίας (full dublex) δεύτερης γενιάς (2G) που χρησιμοποιεί ηλεκτρομαγνητικά σήματα καθώς και την τεχνική πολλαπλής πρόσβασης με διαχωρισμό του διαθέσιμου φάσματος συχνοτήτων σε ένα αριθμό καναλιών και την διαίρεση αυτών σε χρονοθυρίδες για την μετάδοση σημάτων.

Χρησιμοποιώντας το GSM :

¶ Από τις αρχές της δεκαετίας του '90 ο χώρος των τηλεπικοινωνιών και της κινητής τηλεφωνίας γνώρισε ραγδαία ανάπτυξη. Τα δίκτυα 2G άρχισαν να επεκτείνονται με ταχύτατους ρυθμούς, ενώ στην αγορά κυκλοφορούσαν όλο και μικρότερα στο μέγεθος μοντέλα συσκευών κινητής τηλεφωνίας.

¶ Από τα μέσα της δεκαετίας '90 ξεκίνησε και η υπηρεσία αποστολής και λήψης γραπτών μηνυμάτων (sms).

¶ ενώ στις αρχές του 21ου αιώνα παρουσιάζονται τα πρώρα κινητά με έγχρωμη οθόνη. Τα δίκτυα αναβαθμίστηκαν στο 2,5 G, με το οποίο έγινε δυνατή η αποστολή και η λήψη φωτογραφιών και βίντεο, ενώ από το 2002 ξεκίνησε η λειτουργία των πρώτων δικτύων 3G που επιτρέπει την βιντεοκλήση (Εικόνα 27).


**Εικόνα 27:** Κινητό τηλέφωνο 3G.

Σήμερα, 21 χρόνια αργότερα, μπορεί να βρει κανείς δίκτυα κινητής τηλεφωνίας και στις 220 χώρες του πλανήτη πάνω στη βάση των χαρακτηριστικών που τέθηκαν τότε. Δισεκατομμύρια άνθρωποι πραγματοποιούν καθημερινά τηλεφωνήματα μέσω του GSM. Επιπλέον, μια

ολόκληρη βιομηχανία ζει και αναπτύσσεται πουλώντας κινητά τηλέφωνα και λειτουργώντας τα δίκτυα κινητής τηλεφωνίας.

Σύμφωνα με στοιχεία του Συνδέσμου GSM, του συνδέσμου των εταιρειών κινητής τηλεφωνίας με δίκτυο GSM, περίπου το 1,6% του παγκόσμιου ΑΕΠ παράγεται μέσω αυτού του δικτύου.

**Το δίκτυο GSM στην Ελλάδα.**

Στην Ελλάδα η ιστορία του GSM ξεκινάει το 1992, όταν προκηρύσσεται διαγωνισμός για την αδειοδότηση δύο γραμμών, τις οποίες κέρδισαν:

- η Telestet, που ξεκίνησε τη λειτουργία της στις 29 Ιουνίου 1993
- και λίγες ημέρες μετά, 1 Ιουλίου 1993, ξεκίνησε να προσφέρει τις υπηρεσίες της και η Panafon.

Αρχικά, το κόστος των συσκευών και των υπηρεσιών ήταν απαγορευτικό. Επιπλέον, οι προβλέψεις δεν ήταν ιδιαίτερα αισιόδοξες για την ελληνική αγορά καθώς οι ειδικοί υποστήριζαν πως ο αριθμός των χρηστών θα φτάσει μέχρι τα τέλη της δεκαετίας τους 200.000. Ωστόσο, σύντομα διαψεύστηκαν οι προβλέψεις αυτές.

Επιπροσθέτως, το 1998 μπήκε στην αγορά ο ΟΤΕ με τη θυγατρική του Cosmote, κερδίζοντας μέσα σε μικρό χρονικό διάστημα σημαντικό μερίδιο από την πελατεία.

Ο ανταγωνισμός που άρχιζε να αυξάνεται συνεχώς, οδήγησε σε μείωση των τιμών των υπηρεσιών. Ήδη το 2000 η Ελλάδα καταλάμβανε τις πρώτες θέσεις στην παγκόσμια κατάταξη στην αναλογία κινητών τηλεφώνων ανά κάτοικο, αλλά και του βαθμού τεχνολογικής ανάπτυξης στον συγκεκριμένο

τομέα.

Το 2003, ενόψει των Ολυμπιακών Αγώνων ξεκίνησε και η υπηρεσία 3G. Στο διάστημα των 14 χρόνων λειτουργίας της κινητής τηλεφωνίας με δίκτυο GSM στην Ελλάδα, οι δύο πρώτες εταιρείες εξαγοράστηκαν από αντίστοιχες του εξωτερικού, η Panafon από τη Vodafone και η Telestet πρόσφατα από μεγάλο αιγυπτιακό όμιλο και φέρει την επωνυμία TIM.

### 4.4.2 GSM Ασφάλεια και Κρυπτογράφηση.

Τα κίνητρα για ασφάλεια στα τηλεπικοινωνιακά δίκτυα κινητής τηλεφωνίας είναι η εξασφάλιση των συνομιλιών και των σημάτων από υποκλοπές καθώς και η αποτροπή απάτης με τη χρήση κινητών τηλεφώνων.

1. Με τα παλαιότερα αναλογικά συστήματα κινητής τηλεφωνίας όπως τα Advanced Mobile Phone System (AMPS) και τα Total Access Communication System (TACS), είναι σχετικά απλό ακόμα και για έναν ερασιτέχνη να υποκλέψει τηλεφωνικές συνομιλίες με την χρήση ενός ανιχνευτή (scanner).
Μια πολύ δημοσιευμένη αντίστοιχη υπόθεση που αφορούσε στην υποκλοπή, καταγραφή και δημοσίευση στα ΜΜΕ, ήταν αυτή της τηλεφωνικής συνομιλίας ενός μέλους της Βρετανικής Βασιλικής οικογένειας.

2. Ένα άλλο θέμα ασφάλειας για την κινητή τηλεφωνία αφορά την μετάδοση «στον αέρα» πιστοποιητικών ταυτότητας όπως είναι το Electronic Serial Number (ESN), μέσω των αναλογικών συστημάτων. Με την χρήση πιο σύνθετων συστημάτων είναι εφικτό να λάβει κάποιος το νούμερο ESN και να το χρησιμοποιήσει για να διαπράξει απάτες μέσω του κινητού τηλεφώνου κλωνοποιώντας ένα άλλο κινητό τηλέφωνο και κάνοντας κλήσεις μέσω αυτού.

Το ύψος της απάτης μέσω κινητών εκτιμάται για το 2003 μόνο για την αγορά των ΗΠΑ εκτιμάται ότι ανέρχεται σε 500 δισ. δολάρια.

3. Η διαδικασία με την οποία δηλώνεται στο σύστημα η τοποθεσία ενός Σταθμού Κινητής Τηλεφωνίας είναι επίσης ευάλωτη σε υποκλοπή και επιτρέπει την παρακολούθηση της θέσης ενός συνδρομητή ακόμα και όταν δεν υπάρχει κλήση σε εξέλιξη.

**Γιατί το GSM είναι ασφαλές :**

¶ Οι μηχανισμοί ασφάλειας και αυθεντικότητας που είναι ενσωματωμένοι στο GSM το καθιστούν το πιο ασφαλές σύστημα κινητής τηλεφωνίας που είναι διαθέσιμο, ιδιαίτερα σε σχέση με τα αναλογικά συστήματα.

¶ Μέρος της αυξημένης ασφάλειας του GSM οφείλεται στο γεγονός ότι είναι ένα ψηφιακό σύστημα που χρησιμοποιεί έναν αλγόριθμο κωδικοποίησης φωνής, Gaussian Minimum Shift Keying (GMSK) ψηφιακή διαμόρφωση και αρχιτεκτονική Time Division Multiple Access (TDMA).

**Αρχιτεκτονικές που χρησιμοποιεί το GSM:**

- Το **TDMA** αποτελεί μια από τις παλαιότερες τεχνολογίες ψηφιακής ασύρματης επικοινωνίας και θεωρείται η λιγότερο προηγμένη ψηφιακή τεχνολογία, λόγω της αισθητής έλλειψης ευελιξίας. (Παρ' όλα αυτά αποτελεί τη βάση για την εξέλιξη πολλών συστημάτων κινητής τηλεφωνίας.).
- Μια άλλη διαδεδομένη και πιο πρόσφατη ψηφιακή κυψελωτή τεχνολογία που χρησιμοποιεί τεχνικές εξαπλωμένου φάσματος είναι το **CDMA** (Code-Division Multiple Access), το οποίο σε αντίθεση με ανταγωνιστικά του συστήματα που χρησιμοποιούν την τεχνολογία TDMA, όπως το GSM και το CDMA, δεν εκχωρεί μια συγκεκριμένη συχνότητα σε κάθε χρήστη. Αντίθετα, κάθε κανάλι χρησιμοποιεί όλο το διαθέσιμο φάσμα. Οι μεμονωμένες συνομιλίες

κωδικοποιούνται με μια ψευδοτυχαία ψηφιακή ακολουθία. Πολλές συνομιλίες πραγματοποιούνται ταυτόχρονα με την αποστολή των δεδομένων επικοινωνίας σε ομάδες συνδυασμένων bit, καταχωρώντας σε κάθε ομάδα στην οποία ανήκει μια συνομιλία ένα διαφορετικό κωδικό. Επομένως, στο άλλο άκρο, κάθε επικοινωνία μπορεί να ανασυναρμολογείται με τη σωστή σειρά, χρησιμοποιώντας τους σωστούς κωδικούς που επισυνάπτονται σε συγκεκριμένες ομάδες bit.

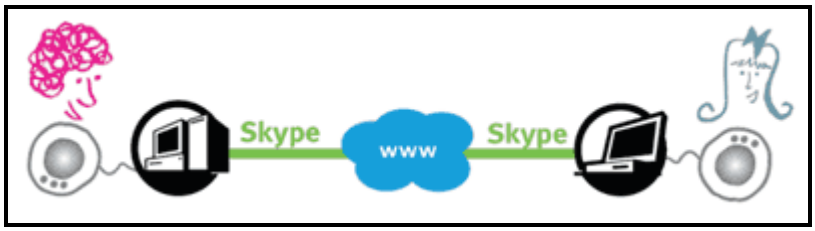
Η υποκλοπή και ανακατασκευή του σήματος απαιτεί πολύ εξειδικευμένα και ακριβά μηχανήματα για να εκτελέσουν την λήψη, τον συγχρονισμό και αποκωδικοποίηση του σήματος.

**Σήμερα όμως η ασφάλεια ακόμα και του πιο προηγμένου συστήματος GSM είναι σε αμφισβήτηση.** Πάρα πολλά περιστατικά σε όλο τον κόσμο δείχνουν ότι οι υποκλοπές στο δίκτυο GSM είναι εύκολο να πραγματοποιηθούν ακόμα και με απλά και φθηνά μηχανήματα που είναι διαθέσιμα στην αγορά. Για αυτό το λόγο :

Η πιο αποτελεσματική λύση εξασφάλισης του τηλεφωνικού απορρήτου αποδεικνύεται η κρυπτογράφηση των κλήσεων μεταξύ δύο κινητών τηλεφώνων. Με τη λύση αυτή, η κρυπτογράφηση και η αποκρυπτογράφηση γίνεται στις κινητές τηλεφωνικές συσκευές και δεν εξαρτάται από την ποιότητα της ασφάλειας του δικτύου GSM.

## 4.5 Τηλεφωνία μέσω διαδικτύου.

(Στην ενότητα που ακολουθεί χρησιμοποιήθηκαν στοιχεία από τις πηγές [12], [17], [19], [20], [32], [41]).




Το **Voice over IP** ή **VoIP** ή τηλεφωνία μέσω διαδικτύου ή σωστότερα **Voice Over Internet**, δηλαδή Φωνή Πάνω από το Πρωτόκολλο του διαδικτύου, χαρακτηρίζει μια ομάδα πρωτοκόλλων-τεχνολογιών, η οποία προσφέρει φωνητική συνομιλία σε πραγματικό χρόνο με σχετικά καλή ποιότητα πλέον και στην ουσία χωρίς κόστος.

Οι συνομιλίες αυτές παραδοσιακά γίνονταν αποκλειστικά μέσω ηλεκτρονικού υπολογιστή που ήταν συνδεδεμένος με το Διαδίκτυο (Internet) και διέθετε μικρόφωνο, ακουστικά και το κατάλληλο λογισμικό. Η κλήση κατέληγε σε ένα άλλο, ανάλογα εξοπλισμένο, ηλεκτρονικό υπολογιστή χωρίς να υπάρχει κάποια επιπλέον χρέωση, εκτός από αυτή της πρόσβασης στο Διαδίκτυο, αφού στη συγκεκριμένη επικοινωνία δεν μεσολαβεί κάποιος παραδοσιακός φορέας τηλεπικοινωνιών (π.χ. ΟΤΕ) παρά μόνο το Διαδίκτυο.

Τον τελευταίο καιρό έχουν εμφανιστεί οι λεγόμενοι εναλλακτικοί (ιντερνετικοί) τηλεπικοινωνιακοί φορείς, οι οποίοι προσφέρουν προώθηση των κλήσεων VoIP σε σταθερά δίκτυα τηλεπικοινωνιών με εξαιρετικά χαμηλό κόστος, αλλά όχι το αντίστροφο.

**Αξιοποίηση της υπάρχουσας υποδομής.**

Όλες οι σύγχρονες δικτυακές υποδομές βασίζονται πλέον σε πρωτόκολλο IP, αλλά και σε ολόκληρο το Διαδίκτυο. Γι' αυτό, δεν είναι δύσκολο να αντιληφθεί κανείς πόσο εύκολο και χρήσιμο θα ήταν να αξιοποιηθεί μία τέτοια τεχνολογία.

**Πλεονεκτήματα.**

Τα πλεονεκτήματα της VoIP τεχνολογίας θα πρέπει να συγκριθούν πάντα με την συμβατική τηλεφωνία, δηλαδή, την γνωστή υπηρεσία τηλεφωνίας με την οποία είμαστε όλοι εξοικειωμένοι. Μερικά από αυτά τα πλεονεκτήματα είναι:

- **Φθηνή υπηρεσία:** επειδή χρησιμοποιείται η υπηρεσία μέσω ενός δημοσίου δικτύου (Διαδίκτυο), η μεταφορά φωνής μεταξύ δύο σημείων μπορεί να γίνει χωρίς χρέωση.
- **Πρόσβαση:** ένας χρήστης μπορεί να έχει πρόσβαση στην υπηρεσία από οποιοδήποτε σημείο υπάρχει δίκτυο. Δεν περιορίζετε από ένα συγκεκριμένο καλώδιο το οποίο έρχεται στο σπίτι του.
- **Πλούσια υπηρεσία:** επειδή είναι δικτυακή υπηρεσία, το VoIP μπορεί να συνδυαστεί και με άλλες υπηρεσίες (όπως βίντεο για παράδειγμα) για να κάνει την εμπειρία του χρήστη πιο πλούσια.

**Τα μειονεκτήματα.**

Όπως με κάθε τι καλό, υπάρχουν και κάποια μειονεκτήματα:

- **Ποιότητα φωνής:** Η τεχνολογία VoIP προσπαθεί να περάσει φωνή πάνω από μία υποδομή η οποία δεν σχεδιάστηκε αρχικά γι' αυτό το σκοπό. Επίσης, η φωνή περνάει πάνω από ένα δίκτυο το οποίο μεταφέρει κι άλλα δεδομένα, κάτι το οποίο μπορεί να δημιουργήσει διακοπές στην συνομιλία. Ωστόσο, μέτρα μπορούν και έχουν παρθεί ώστε να εξασφαλιστεί η ποιότητα της φωνής

δίνοντας σχεδόν την ίδια ποιότητα με την συμβατική τηλεφωνία και σχεδόν την ίδια διαθεσιμότητα.

**Οφέλη από το VoIP.**

Η υπηρεσία VoIP για καταναλωτές επεκτείνεται συνεχώς σε ολόκληρη τη χώρα και τώρα προσφέρει αυτές τις δυνατότητες τόσο για τους πελάτες συμβατικής τηλεφωνίας όσο και για τους πελάτες κινητής τηλεφωνίας:

- **Εύκολη εγκατάσταση και χρήση:** Σε πολλές περιοχές, δεν χρειάζεται καν υπολογιστής. Η υπηρεσία είναι διαθέσιμη μέσω του τηλεφώνου με τη χρήση ενός μικρού προσαρμογέα. Πολλοί από τους κυριότερους παρόχους τηλεφωνίας, καλωδιακών δικτύων ή Διαδικτύου επίσης σχεδιάζουν να παρέχουν υπεραστική κλήση μαζί με άλλα πακέτα υπηρεσιών.
- **Αποθήκευση φωνής:** Είναι δυνατή η πρόσβαση στο ηλεκτρονικό φωνητικό μήνυμα VoIP, η αποθήκευση των συνομιλιών στον υπολογιστή σας και η αναπαραγωγή τους όποτε χρειάζεται.

**Κίνδυνοι του VoIP.**

- **Κλοπή:** Οι εισβολείς που μπορούν να έχουν πρόσβαση σε διακομιστές VoIP, μπορούν επίσης να επιτύχουν πρόσβαση και στα αποθηκευμένα φωνητικά δεδομένα, καθώς και στην ίδια την τηλεφωνική υπηρεσία, να κρυφακούν ή να κάνουν και δωρεάν κλήσεις χρεώνοντας το λογαριασμό σας.
- **Επίθεση από ιούς:** Εάν ένας διακομιστής VoIP έχει μολυνθεί από ιό, μπορεί να χαθεί η τηλεφωνική υπηρεσία. Μπορεί επίσης να επηρεαστούν και άλλοι υπολογιστές που συνδέονται σε αυτό το σύστημα.
- **Τεχνολογία που δεν υπόκειται σε κανονισμούς:** Αν και υπάρχει διαδικασία σύνταξης κανονισμών, οι χρήστες αυτή τη στιγμή είναι εκτεθειμένοι

σε κάποιους τύπους επιθέσεων και απατών. Για παράδειγμα, οι τηλε-πωλητές μπορούν να χρησιμοποιήσουν το VoIP για να παραδώσουν τεράστιο όγκο τυποποιημένων φωνητικών μηνυμάτων σε καταναλωτές.

**Ασφάλεια.**

Το VoIP είναι ευάλωτο σε όλα τα θέματα ασφαλείας. Δηλαδή μπορεί να επηρεαστεί από ιούς, worms(σκουλήκια) και άρνηση εξυπηρέτησης (DoS), πλαστογράφηση, πρόσβαση από τρίτους χωρίς άδεια, απάτη.

Οι δύο κύριες μέθοδοι ασφάλειας για τους χρήστες του VoIP είναι :

διοχέτευση και κρυπτογράφηση.

Αυτά τα μέτρα ασφαλείας παρέχουν έναν μηχανισμό εμπιστοσύνης που βοηθά στην ασφαλή χρήση των προσωπικών δεδομένων κάθε χρήστη μέσω του VoIP.

Στην πράξη τώρα:

- Οι περισσότεροι πάροχοι VoIP χρησιμοποιούν μια μέθοδο κρυπτογράφησης που ονομάζεται Secure Sockets Layer ή SSL.
- Οι μεγάλες εταιρείες χρησιμοποιούν παρόμοιους μηχανισμούς ασφαλείας – κρυπτογράφησης για όλες τις κινήσεις τους.
- Οι οργανισμοί που χρησιμοποιούν VoIP ως μέσο επικοινωνίας στηρίζουν την ασφάλεια τους σε πολλαπλά επίπεδα. Δηλαδή το VoIP δίκτυο χωρίζεται σε ασφαλείς ζώνες οι οποίες προστατεύονται με μηχανισμούς όπως ελέγχους πρόσβασης , τείχη, πρόληψη της διείσδυσης και άλλους.

Το πλεονέκτημα αυτής της στρατηγικής είναι: ότι επιτρέπει στους οργανισμούς να εφαρμόσουν ισχυρή ταυτότητα και κρυπτογράφηση τόσο στα δίκτυα δεδομένων, όσο και στα δίκτυα φωνής.

**Ένα σύστημα για να είναι ασφαλές θα πρέπει:**

¶ Να προβαίνει σε ελέγχους ταυτότητας και ελέγχους πρόσβασης.

¶ Να μπορεί να κρυπτογραφεί.

¶ Να παρέχει διαδικασία ελέγχου των κλήσεων, καθώς και διευκολύνσεις.

**Εφαρμογές**

Σήμερα υπάρχει πληθώρα εφαρμογών, συμπεριλαμβανομένων των, KiX Voipbuster, MSN Messenger, Skype κ.ά., οι οποίες προσφέρουν τηλεφωνία μέσω διαδικτύου. Το πιο ευρέως διαδεδομένο από τα παραπάνω είναι το Skype και το MSN. Τα τηλεφωνικά κέντρα αυτά αναλαμβάνουν να μετατρέψουν την τηλεφωνία σε μια τηλεφωνία χωρίς κόστος χρήσης.

Περιγραφή του Skype.

Το Skype είναι με εξαιρετικά δημοφιλής εφαρμογή-υπηρεσία τηλεφωνία μέσω διαδικτύου με εκατομμύρια χρήστες ανά τον κόσμο. Αρχικά ακολούθησε το μοντέλο φωνητικής επικοινωνίας VoIP από Η/Υ σε Η/Υ. Πλέον προσφέρει κλήσεις σε οποιοδήποτε μέρος του κόσμου, σε οποιοδήποτε δίκτυο τηλεφωνίας, σταθερής και κινητής, με χαμηλές χρεώσεις. Να σημειωθεί επίσης ότι κλήσεις στο εσωτερικό δίκτυο των εφαρμογών είναι δωρεάν. Οι κλήσεις που χρεώνονται είναι αυτές που γίνονται προς δίκτυα άλλων φορέων.

## 4.6 Συστήματα Τακτικών Επικοινωνιών.

(Στην ενότητα που ακολουθεί χρησιμοποιήθηκαν στοιχεία από τις πηγές [42], [43], [44]).

### 4.6.1 WISPR.

Το WISPR είναι νέας γενιάς πλατφόρμα ψηφιακής τεχνολογίας. Συντελεί στην ανάπτυξη και στη σύνθεση συστημάτων ενδοεπικοινωνίας, ολοκλήρωσης τακτικών επικοινωνιών και ευέλικτης διαχειρίσεις συμβατικών μέσων επικοινωνίας (VHF, HF, UHF, κ.α). Διαθέτει συσκευές κρυπτογράφησης και συχνά έχει εφαρμογή στις χερσαίες αεροπορικές και ναυτικές δυνάμεις για κινητούς και σταθερούς χρήστες ( Εικόνα 28).

**Εικόνα 28**: WISPR πλατφόρμα ψηφιακής τεχνολογίας.

Το WISPR παρέχει:

- δυνατότητα ταυτόχρονης υποστήριξης υπηρεσιών φωνής, δεδομένων και ελέγχου ασυρμάτων.
- κατανεμημένη και ανοικτή αρχιτεκτονική που επιτρέπει την επιλεκτική σύνθεσή του για διαφορετικές εφαρμογές ανάλογα με τις επιχειρησιακές ανάγκες του χρήστη.
- Άλλη μια σημαντική καινοτομία του συστήματος που είναι η ικανότητα σχηματισμού ασύρματου τοπικού δικτύου μικρής εμβέλειας Wireless LAN, βασισμένη στην τεχνική ευρέως φάσματος.

Το ασύρματο δίκτυο μικρής εμβέλειας WLAN του συστήματος WISPR προσφέρει τρεις βασικές κατηγορίες υπηρεσιών φωνής , δεδομένων και τηλεχειρισμού. Αναλυτικότερα :

1. Η φωνητική επικοινωνία είναι αμφίδρομη για κάθε χειριστή, ανεξάρτητα από τυχούσες ταυτόχρονες μεταδόσεις δεδομένων ή τηλεχειρισμού Σ/Α.
2. Η μετάδοση δεδομένων είναι αμφίδρομη, με υψηλή ταχύτητα μεταφοράς μεταξύ κ οχημάτων, μεταξύ οχημάτων και πεζών ή μεταξύ πεζών . Η υψηλή ταχύτητα μεταφοράς επιτρέπει εφαρμογές μετάδοσης κινούμενης εικόνας σε πραγματικό χρόνο, real time video. Οι υπηρεσίες αυτές χαρακτηρίζονται από μετάδοση με χαμηλό βαθμό ανίχνευσης. Παράλληλα χρησιμοποιούνται τεχνικές κατά των παρεμβολών και η δυνατότητα κρυπτογράφησης.
3. Ο τηλεχειρισμός και η πρόσβαση στους ασύρματους σταθμούς TRC (VHF & HF) είναι πλήρης.

### 4.6.2 Συσκευές Κρυπτογράφησης - SecLine

1. **SecLine MBit :** είναι μια συσκευή στρατιωτικών προδιαγραφών που χρησιμοποιείται στην ταυτόχρονη πολυκάναλη κρυπτογράφηση / αποκρυπτογράφηση δεδομένων δέσμης (bulk encryption) σε υψηλές ταχύτητες. Είναι εξειδικευμένη για τις επιχειρησιακές ανάγκες των Ενόπλων Δυνάμεων. Η συσκευή SecLine MBit προορίζεται για την κάλυψη αναγκών ασφαλείας των μεταδιδόμενων δεδομένων σε συνδέσεις τηλεφωνικών δικτύων και σε ψηφιακά συστήματα επικοινωνιών έτσι ώστε, είτε είναι ασύρματα είτε ενσύρματα είτε οπτικής ίνας, να διασφαλίζεται πλήρως η μετάδοση των δεδομένων.

Η SecLine MBit λειτουργεί σε δύο τρόπους:

¶ σαν συσκευή κρυπτογράφησης δέσμης δεδομένων κρυπτογραφώντας όλη την πληροφορία

¶ σαν μία συσκευή που κρυπτογραφεί συγκεκριμένα κανάλια πληροφοριών (κανάλια E1).

Η SecLine MBit χρησιμοποιεί έναν πιστοποιημένο μη-γραμμικό αλγόριθμο κρυπτογράφησης που προσφέρει ύψιστη ασφάλεια κατά τη διάρκεια μετάδοσης δεδομένων.

2. **SecLine a-PLUS :** είναι μια ψηφιακή συσκευή υψηλών προδιαγραφών ασφαλείας που χρησιμοποιείται για την κρυπτογράφηση / αποκρυπτογράφηση τηλεομοιοτυπίας (fax), φωνής (voice) και δεδομένων (data).

Η συσκευή SECLINE a - PLUS προορίζεται για την κάλυψη αναγκών ασφαλείας των μεταδιδόμενων πληροφοριών σε συνδέσεις τηλεφωνικών δικτύων, έτσι ώστε να διασφαλίζεται πλήρως η μετάδοση εγγράφων φαξ , φωνής και δεδομένων.

Συγκεκριμένα, η SECLINE a-PLUS μπορεί να συνδεθεί μεταξύ μιας κοινής τηλεομοιοτυπικής συσκευής φαξ ή ενός Fax Modem ή ενός Η/Υ ή μιας τηλεφωνικής συσκευής και του τηλεπικοινωνιακού δικτύου (π.χ. κυκλώματα ΟΤΕ, στρατιωτικά κυκλώματα, διάφορα επικοινωνιακά συστήματα PSTN, PABX). Δεν απαιτεί ιδιαίτερα χαρακτηριστικά, όπως θύρες δεδομένων ή άλλες μονάδες διασύνδεσης. Υποστηρίζει όλα τα πρόσφατης τεχνολογίας πρωτόκολλα επικοινωνίας και έχει τη δυνατότητα αυτόματης μετάπτωσης της ταχύτητας επικοινωνίας και επαναφορά, ανάλογα με την κατάσταση του τηλεπικοινωνιακού δικτύου για επικοινωνία χωρίς σφάλματα.

3. **SecLine IP :** είναι μία συσκευή η οποία παρέχει ασφάλεια στην επικοινωνία σε δίκτυα Ethernet IP. Τοποθετείται στο άκρο ενός τοπικού δικτύου (LAN) παρέχοντας ασφάλεια στην εισερχόμενη και εξερχόμενη κυκλοφορία. Χρησιμοποιεί ένα κρυπτογραφικό αλγόριθμο που προσφέρει ύψιστη ασφάλεια κατά την μετάδοση δεδομένων. Ενδεικτικά η συσκευή SECLINE IP μπορεί να τοποθετηθεί ανάμεσα στο switch/hub, στο οποίο συγκεντρώνεται η κίνηση του

τοπικού δικτύου, και στο gateway (router), το οποίο διαχειρίζεται την κίνηση του τοπικού δικτύου προς τα άλλα δίκτυα.

## 4.7 Παγκόσμιος Ιστός (World Wide Web).

Στην ενότητα που ακολουθεί χρησιμοποιήθηκαν στοιχεία από τις πηγές [(10), (19), (47), (48), (49), (50)].

Ο Παγκόσμιος Ιστός (World Wide Web), δηλαδή το w.w.w., είναι ένας παγκόσμιος κοινότοπος πληροφοριών που επιτρέπει σε όλους να εισέλθουν για να διαβάσουν ή να γράψουν οτιδήποτε. Αυτό επιτυγχάνεται με τη σύνδεση ενός υπολογιστή στο Διαδίκτυο.


Πολλοί μπερδεύουν το Web με το Internet αλλά πρόκειται για διαφορετικά πράγματα. Το Διαδίκτυο είναι απλά ένα μέσο να λειτουργήσει το Web, ακριβώς όπως μία τηλεφωνική γραμμή είναι το μέσο με το οποίο γίνονται οι τηλεφωνικές συνδιαλέξεις. Το Web επίσης παρέχει τη γλώσσα για να δημοσιευτούν αλλά και το πρωτόκολλο για να διακινηθούν τα δεδομένα του στο Internet.

**Πότε δημιουργήθηκε το W.W.W και από ποιους**

Είναι πολλοί αυτοί που οραματίστηκαν την ανάπτυξη ενός διασυνδεδεμένου συστήματος από πληροφορίες και δεδομένα. Ένας από αυτούς ήταν ο διευθυντής του γραφείου Επιστημονικής Έρευνας και Ανάπτυξης των

ΗΠΑ Δόκτωρ Vannevar Bush ο οποίος τη δεκαετία του ΄40 δημιούργησε ένα σύστημα που το ονόμασε memex.

Ωστόσο το Web με την σημερινή του μορφή δημιουργήθηκε στα τέλη της δεκαετίας του ΄80 στα εργαστήρια του Cern στην Γενεύη (Το Cern είναι ένα διεθνές κέντρο ερευνών όπου διεξάγονται πειράματα με σωματίδια υψηλών ενεργειών σε επιταχυντές). **Οι δημιουργοί του Web είναι ο Άγγλος Tim Berners-Lee και ο Γάλλος Robert Caillau.** Και οι δύο δούλευαν στο Cern και το 1989 συνεργάστηκαν για την δημιουργία ενός συνδεδεμένου συστήματος πληροφοριών που θα ήταν προσβάσιμο από όλους τους υπολογιστές που χρησιμοποιούνταν στο Cern εκείνη την περίοδο.

Ο Tim Berners-Lee είχε την ιδέα να δημιουργήσει ένα σύστημα που θα επέτρεπε σε ερευνητές, από απομακρυσμένα μεταξύ τους μέρη του κόσμου, να οργανώσουν και να συνδέσουν όλο τον όγκο των εγγράφων που διέθεταν. Έτσι, πρότεινε την εισαγωγή συνδέσμων (links) μέσα στο κείμενο του κάθε εγγράφου, ώστε να είναι δυνατή η πρόσβαση από οποιοδήποτε και σε οποιοδήποτε έγγραφο. Άρα κάποιος καθώς διαβάζει ένα έγγραφο θα μπορεί μέσω των links να δει και να διαβάσει όλα τα σχετικά έγγραφα που είναι συνδεδεμένα με το αρχικό.

Αυτό απαιτούσε τη δημιουργία μίας γλώσσας κατανοητής από όλους τους υπολογιστές και παράλληλα ενός πρωτοκόλλου (τρόπο επικοινωνίας μεταξύ των υπολογιστών) που θα έκανε δυνατή την ανάκτηση των εγγράφων με την βοήθεια συνδέσμων. Έτσι δημιουργήθηκε η γλώσσα HTML (Hypertex Markup Language) και το πρωτόκολλο του Web http (Hypertext Transfer Protocol).
« Το σύνολο όλων των ενωμένων μεταξύ τους εγγράφων είναι το Web »

**Πότε δόθηκε προς χρήση το w.w.w**

Το 1991 το Web δόθηκε προς χρήση από το Cern, έτσι ξεκίνησε η προσπάθεια να γίνει γνωστό. Στην αρχή η πρόοδος ήταν αργή, αλλά με τη δημιουργία ενός προγράμματος που είχε το όνομα Mosaic το οποίο έδινε την δυνατότητα στους χρήστες να μπορούν να βλέπουν εκτός από κείμενο και γραφικά, ο ρυθμός της ανάπτυξής του εκτινάχτηκε.

**Τι είναι ο Παγκόσμιος Ιστός**

Ο Παγκόσμιος Ιστός ή World Wide Web (WWW) είναι ένας εικονικός «χώρος» όπου η επικοινωνία γίνεται μέσω ειδικών εγγράφων υπερκειμένου (hypertext), που ονομάζονται ιστοσελίδες (web pages). Οι ιστοσελίδες είναι αποθηκευμένες σε υπολογιστές (web servers - εξυπηρετητές ιστού) που τρέχουν με ειδικό λογισμικό για αυτό το σκοπό έχουν μεγάλη υπολογιστική ισχύ και μόνιμη σύνδεση με το Internet, ώστε να είναι συνεχώς διαθέσιμες στους χρήστες.

Ο χρήστης για να έχει τη δυνατότητα να τις χρησιμοποιήσει αρκεί να διαθέτει ένα πρόγραμμα που να μεταφέρει τις ιστοσελίδες από τον web server στον τοπικό υπολογιστή. Τα προγράμματα αυτά ονομάζονται web browsers (φυλλομετρητής ιστού).

Οι πιο διαδεδομένοι browsers σήμερα είναι οι:

¶ Internet Explorer της Microsoft κυρίως επειδή διανέμεται δωρεάν μαζί με τα προγράμματα της εταιρείας και

¶ Netscape Navigator της Netscape που επίσης διανέμεται δωρεάν για εκπαιδευτική χρήση.

Οι browsers, αυτοί, παρέχουν τις ίδιες λειτουργικότητες στη χρήση του web και δίνουν τη δυνατότητα για ανάγνωση e-mail, news, δημιουργία ιστοσελίδων κ.α., μέσω των αντίστοιχων ενσωματωμένων προγραμμάτων.

**Λειτουργία της υπηρεσίας .**


Η λειτουργία της υπηρεσίας αυτής βασίζεται στο μοντέλο πελάτη/εξυπηρετητή (client/server model) και απαιτεί συνεργασία του web browser (client) με τον web server. Κατά τη μεταξύ τους επικοινωνία χρησιμοποιείται το πρωτόκολλο HTTP (HyperText Transfer Protocol - πρωτόκολλο μεταφοράς υπερκειμένου) και οι δραστηριότητες που πραγματοποιούνται είναι:

**1.** Ο browser αναλαμβάνει να:

- επικοινωνήσει με τον server και να «κατεβάσει» τις ιστοσελίδες, δηλαδή να τις μεταφέρει στον τοπικό υπολογιστή.
- παρουσιάσει στον χρήστη το περιεχόμενο των ιστοσελίδων το οποίο μπορεί να περιέχει κείμενο, εικόνες, ήχο, video, κ.ά.

**2.** Ο server αναλαμβάνει να:

- είναι σε συνεχή διαθεσιμότητα ώστε να ανταποκρίνεται στις κλήσεις των πελατών και να παρέχει τις ιστοσελίδες
- τρέχει ειδικά προγράμματα (CGI scripts, Java Servlets κ.α.) για την καλύτερη λειτουργία του

**Χρήση της υπηρεσίας**

Η χρήση της υπηρεσίας είναι πολύ απλή, γεγονός που την κάνει πολύ δημοφιλή. Σε κάποιο browser αρκεί να δώσουμε την ακριβή τοποθεσία και το

όνομα της ιστοσελίδας που θέλουμε, τα στοιχεία αυτά περιέχονται μέσα στο URL (Uniform Resource Locator) της ιστοσελίδας.

Τα URLs των ιστοσελίδων έχουν την μορφή :

http://Διεύθυνση server[/υποκατάλογος][/όνομα αρχείου]

π.χ. http://www.teipat.gr/plirofories/doc/anakoin2008/pr11908.doc

Στο παραπάνω παράδειγμα www.teipat.gr είναι η διεύθυνση του server και "doc" το όνομα του υποκαταλόγου στον οποίο βρίσκεται αποθηκευμένη η ιστοσελίδα pr11908.doc

Επέκταση του πρωτοκόλλου HTTP είναι το HTTPS (Secure HTTP) μέσω του οποίου η επικοινωνία μεταξύ browser και server γίνεται κρυπτογραφημένα. Αυτό υλοποιείται με την προσθήκη του SSL (Secure Sockets Layer) πρωτοκόλλου στο HTTP, το οποίο εξασφαλίζει:

- Προστασία από την υποκλοπή σημαντικών για την ασφάλεια δεδομένων (π.χ. passwords).
- Κρυπτογραφημένη μεταφορά αρχείων και ιστοσελίδων.
- Ελεγμένη μεταφορά των πληροφοριών, εξασφαλίζοντας πως κανείς δεν θα παρέμβει για να τις τροποποιήσει.

## Παράρτημα

(Στην ενότητα που ακολουθεί χρησιμοποιήθηκαν στοιχεία από την πηγή [50]).

**Κρατικός έλεγχος στην ισχυρή κρυπτογραφία.**

Όπως μπορούμε να κατανοήσουμε όλοι μας, η χρήση προϊόντων ισχυρής κρυπτογραφίας εκτός από το ότι μας διασφαλίζουν το απόρρητο των προσωπικών και λοιπών δεδομένων μας, μπορούν να δημιουργήσουν πληθώρα προβλημάτων στις διωκτικές αρχές. Και αυτό γιατί πλέον δεν θα μπορούν εύκολα να παρακολουθούν τις κινήσεις υπόπτων μέσα στο Διαδίκτυο. Το Internet δηλαδή μπορούμε να το παρομοιάσουμε ως ένα απόρθητο φρούριο που δίνει το δικαίωμα σε κάθε χρήστη να προβαίνει σε οποιαδήποτε νόμιμη ή άνομη συναλλαγή επιθυμεί. Συνέπεια αυτών, είναι η έντονη προσπάθεια πολλών κυβερνήσεων να ελέγξουν την αγορά κρυπτογραφίας.

**α) Έλεγχος εξαγωγής ισχυρής κρυπτογραφίας.**

Ο λόγος που πολλά κράτη έχουν θεσπίσει νόμους, με τους οποίους ελέγχουν την εξαγωγή προϊόντων κρυπτογράφησης είναι ότι επιδιώκουν να στερήσουν από τους πιθανούς αντιπάλους τους τα προϊόντα ισχυρής κρυπτογραφίας που αυτοί έχουν δημιουργήσει. Και αυτό γιατί θέλουν να εξασφαλίσουν το απόρρητο των διπλωματικών και στρατιωτικών τους επικοινωνιών.

**β) Έλεγχος εσωτερικής χρήσης προϊόντων ισχυρής κρυπτογραφίας.**

Ο έλεγχος της εσωτερικής χρήσης προϊόντων ισχυρής κρυπτογραφίας για μη κρατικούς σκοπούς είναι ακόμα θέμα συζήτησης και αναμένεται να παραμείνει έτσι για αρκετό καιρό ακόμα. Και αυτό γιατί ενώ οι διωκτικές αρχές

για τους λόγους που προαναφέραμε επιθυμούν να δημιουργηθεί, μεγάλες επιχειρήσεις, οργανώσεις χρηστών, hackers έχουν επιδοθεί σε έναν αγώνα κατά αυτού, προασπίζοντας έτσι την ελευθερία λόγου, το δικαίωμα προστασίας της προσωπικής ζωής, τους νόμους της ελεύθερης αγοράς και πολλά άλλα.

Διάφοροι μέθοδοι ελέγχου που προωθούνται :

1) Οι Η.Π.Α προωθούν την μέθοδο key-escrow. Σύμφωνα με αυτήν κάθε χρήστης υποχρεούται -ή 'υποχρεούται εθελοντικά'- να καταθέσει ένα αντίγραφο του ιδιωτικού κλειδιού του σε κάποια υπηρεσία κοινής αποδοχής η οποία θα το δίνει στις κρατικές υπηρεσίες και την αστυνομία κατόπιν δικαστικής εντολής.

2) Παραλλαγή αυτής είναι η ιδέα που ανέπτυξε η ερευνητική ομάδα του καθηγητή Silvio Micali στο MIT. Σύμφωνα με αυτή, το ιδιωτικό κλειδί του κάθε χρήστη θα 'σπάει' κατά τη δημιουργία του σε τρία μέρη με το καθένα να στέλνεται και να κρατείται σε κάποιο πρόσωπο ή οργανισμό κοινής αποδοχής, π.χ. σε κάποιον δικαστή. Με την έκδοση μίας δικαστικής εντολής, οι τρεις φύλακες του κλειδιού θα παραδίδουν ο καθένας το κομμάτι του στην σχετική κρατική υπηρεσία.

**Ερωτήματα που θα πρέπει να απαντηθούν:**

1) Πώς μπορεί κάποιος να γνωρίζει ότι το πρόσωπο κοινής αποδοχής θα διαχειριστεί έντιμα το κλειδί του; Δεδομένου ότι ένα μήνυμα δε μπορεί να αποκρυπτογραφηθεί αν δεν είναι γνωστά και τα τρία μέρη του ιδιωτικού κλειδιού.

2)Πώς θα γνωρίζει κάποιος υπό ποιες ακριβώς συνθήκες αποκτούν οι κυβερνητικές υπηρεσίες πρόσβαση στο ιδιωτικό κλειδί του; Η δικαστική εντολή είναι κάτι τυπικό. Μόνο η απόλυτη διαφάνεια μπορεί να εξασφαλίσει τον απλό χρήστη και κάτι τέτοιο δεν υπάρχει και ούτε μπορεί να υπάρξει σε καμία κυβερνητική υπηρεσία σε κανένα μέρος του κόσμου.

**Ποιες χώρες έχουν εφαρμόσει ελέγχους και ποιους**

**R** Η Γαλλία έχει νομοθετικά προσδιορισμένη πολιτική πάνω στο θέμα.

**R** Η Βρετανία, επέβαλε τον έλεγχο μέσω του key-escrow, αλλά μετά την άνοδο των εργατικών του Tony Blair, ο νόμος αυτός καταργήθηκε.

**R** Στις Η.Π.Α. επανειλημμένες φορές, κατατέθηκαν νομοσχέδια, στην συνέχεια ψηφίστηκαν και μετά καταργήθηκαν.

**R** Μόνο η Ιαπωνία έχει καθιερώσει πολιτική προστασίας της ιδιωτικής ζωής και των εμπιστευτικών δεδομένων, αδιαφορώντας για το κόστος στην εγκληματικότητα.

**Επισήμανση:**

Πρέπει να σημειωθεί το γεγονός ότι η κρυπτογράφηση εμποδίζει την εγκληματική δραστηριότητα. Η ζημιά που έχει προκύψει από το ηλεκτρονικό έγκλημα παγκοσμίως ήδη ανέρχεται σε δισεκατομμύρια δολάρια (βιομηχανική κατασκοπεία, απάτες με πιστωτικές κάρτες και λογαριασμούς κινητής τηλεφωνίας, πειρατεία στη συνδρομητική τηλεόραση, στα CD και στο λογισμικό για προσωπικούς υπολογιστές). Συνεπώς υπάρχουν σημαντικά οικονομικά και νομικά οφέλη από την ελεύθερη διακίνηση αλγόριθμων ισχυρής κρυπτογράφησης.

# ΒΙΒΛΙΟΓΡΑΦΙΑ:


**1.** Βουκάλης, Δ., Εφαρμοσμένη κρυπτογραφία, Σύγχρονη εκδοτική, Έκδοση Α, Αθήνα, 2007.

**2.** Βλαχοπούλου,Κ., E-marketing, Rosili, Έκδοση Β, Αθήνα, 2003.

**3.** Κάτος,Β.Α,Στεφανίδης,Γ.Χ, Τεχνικές κρυπτογραφίας& κρυπτανάλυσης, Ζυγός , Έκδοση Α, Θεσσαλονίκη, 2003.

**4.** Λεκάτης,Γ., Κλαδάκης,Ν. ,Ασφάλεια δικτύων και συστημάτων, Παπασωτηρίου, Έκδοση Α, Αθήνα, 2001.

**5.** Μαρκασιώτης,Ι., Δίκτυα υπολογιστών, Γκούρδας Β., Έκδοση Β, Αθήνα, 2006.

**6.** Μάρκελλος, Κ., Μαρκέλλου,Π., Ρήγκου, Μ., Συρμακέσης,Σ., Τσακαλίδης,Α., Ε-Επιχειρηματικότητα από την ιδέα στην υλοποίηση, Ελληνικά γράμματα, Έκδοση Γ , Αθήνα, 2007.

**7.** Νάστου,Π., Σπυράκης,Π., Σταματίου,Γ., Σύγχρονη κρυπτογραφία, Ελληνικά γράμματα, Έκδοση Β, Αθήνα,2003.

**8.** Παπαδημητρίου,Γ., Πομπόρτσης,Α., Ασφάλεια δικτύων υπολογιστών, Τζιόλα, Θεσσαλονίκη, Έκδοση Β, 2003.

**9.** Παπαχριστοφής,Κ., Σύγχρονα δίκτυα τηλεπικοινωνιών, Εκδόσεις νέων τεχνολογιών, Έκδοση Α, Αθήνα, 2001.

**10.** Πολλάλης, Γ.,Γιαννακόπουλος, Δ.,Ηλεκτρονικό επιχειρείν, Σταμούλη Α.Ε., Έκδοση Α, Αθήνα, 2007.

**11.** Πουλάκης,Δ.,Κρυπτογραφία,Ζήτη, Έκδοση Α, Θεσσαλονίκη, 2004.


# ΞΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ:


**12.** Douglas, E., Comer, Δίκτυα και διαδίκτυα υπολογιστών και εφαρμογές τους στο Internet, Κλειδάριθμος, Έκδοση Γ, Αθήνα, 2002.

**13.** Preston, G., E-auctions: Τα πάντα για τις δημοπρασίες στο διαδίκτυο, Compupress A.E., Έκδοση Α, Αθήνα, 2001.

**14.** Stalings, W., Βασικές αρχές ασφάλειας δικτύων, Κλειδάριθμος, Αθήνα, Έκδοση Γ, 2008.

**15.** Strebe, M., Ασφάλεια δικτύων, Γκιούρδας Μ. ,Αθήνα, Έκδοση Β, 2005.

**16.** Tanenbaun, A., Δίκτυα &διαδίκτυα υπολογιστών, Κλειδάριθμος, Αθήνα, Έκδοση Β, 2007.

**17.** Comer, Douglas, E., Δίκτυα και διαδίκτυα υπολογιστών, Κλειδάριθμος, Αθήνα Έκδοση Α, 2007.

## ΙΣΤΟΣΕΛΙΔΕΣ:

**18.** http:// www.ionio.gr

**19.** http://el.wikipedia.org/wiki

**20.** http:// www.efarmoges.gr

**21.** http://www.gsmforum.gr

**22.** http://www.be24.gr/markets/index.do

**23.** http://www.islab.demokritos.gr

**24.** http://www.abaxb2b.com

**25.** http://www.geocities.com

**26.** http://www.acm.org/crossroads/xrds11-3/sat.html

**27.** http://www.physics4u.gr

**28.** http://www.papadi.gr

**29.** http://www.securityinsider.gr

**30.** http://www.hte.com.cy

**31.** http:// www.ase.gr

**32.** http: //www.tech-faq.com

**33.** http://www.greekretail.gr

**34.** http: //www.reporter.gr

**35.** http:// www.abaxb2b.com

**36.** http://eclass.teilam.gr

**37.** http://www.go-online.gr

**38.** http:// nemis.cti.gr/ebusiness/distance_course.htm

**39.** http://www.kybernografoi.gr

**40.** http://pelopas.uop.gr

**41.** http://voip.sch.gr/

**42.** http://www.defencenet.gr

**43.** http://www.intracom.gr

**44.** http://www.securitymanager.gr

**45.** http://www.secure-phone.gr

**46.** http://www.aera.gr

**47.** http://users.forthnet.gr

**48.** http://www.uom.gr

**49.** http://noc.auth.gr

**50.** http://www.medialab.ntua.gr

**51.** http://www.cs.uoi.gr

**52.** http://www.cnc.uom.gr