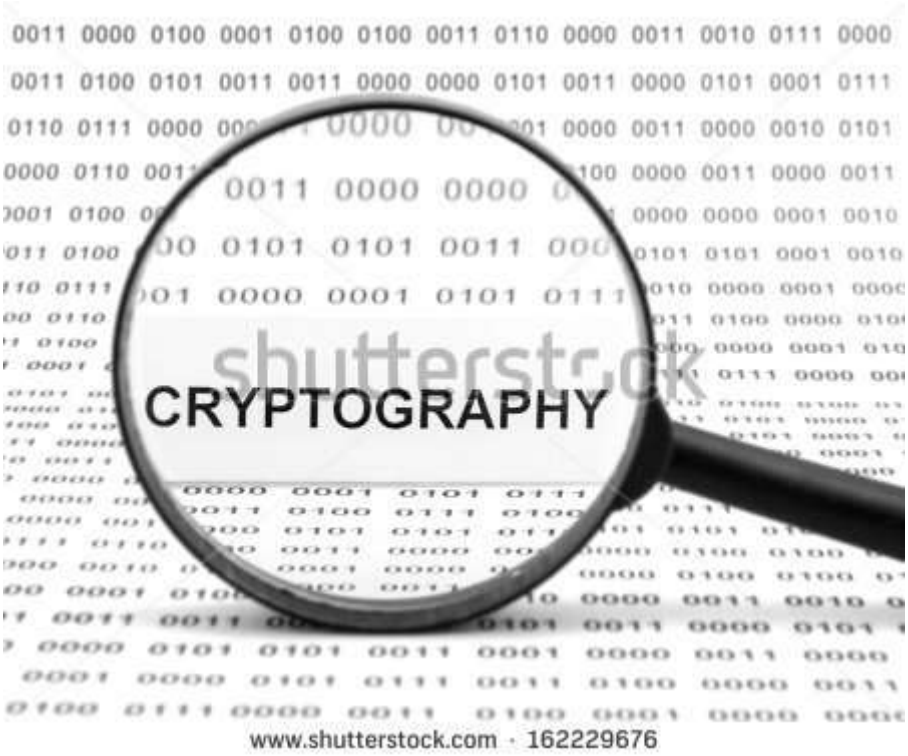
Κρυπτογραφία - Cryptography



ΓΕΝΙΚΟ ΛΥΚΕΙΟ ΑΛΙΑΡΤΟΥ

ΕΡΕΥΝΗΤΙΚΗ ΕΡΓΑΣΙΑ

Β΄ ΤΕΤΡΑΜΗΝΟ

ΣΧΟΛΙΚΟ ΕΤΟΣ 2014-15

ΑΛΙΑΡΤΟΣ, ΜΑΪΟΣ 2015

Εργάστηκαν οι μαθητές της Α' τάξης του Γενικού Λυκείου Αλιάρτου

Σύνθεση ομάδων και εργασίες που έχουν αναλάβει:

<table>
<tr><th colspan="2">Ομάδες - θέματα</th><th>Ερωτήματα που θα διερευνήσει κάθε ομάδα</th></tr>
<tr><td colspan="3">Ομάδα 1η : κεφ. 1^ο: Εισαγωγή, Ιστορική Αναδρομή – Μια ματιά στο παρελθόν</td></tr>
<tr><td>1</td><td>Ζαχαρία Δήμητρα</td><td rowspan="3">1.1.Εισαγωγή:
1.1.1. Τι είναι η Κρυπτογραφία – ποιο το αντικείμενο της
1.2. Ιστορική αναδρομή:
1.2.1. Ιερογλυφικά , Γραμμική γραφή Α , Γραμμική Γραφή Β
1.2.2. Η κρυπτογραφία στους Ελληνο -Ρωμαϊκούς χρόνους (Σπαρτιατική Σκυτάλη, Ο κώδικας του Πολύβιου, Ρωμαϊκοί χρόνοι – Ο κώδικας του Καίσαρα)
1.2.3. Η κρυπτογραφία στο Μεσαίωνα (Γενικά, Το χειρόγραφο Βόϊνιτς, πρώτοι αλγόριθμοι, κώδικας Vigenere)
1.2.4. Η κρυπτογραφία την εποχή του ηλεκτρισμού – Κώδικας Μορς</td></tr>
<tr><td>2</td><td>Ζαχαρία Μαίρη</td></tr>
<tr><td>3</td><td>Κάμπαξη Μαργαρίτα</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3">Ομάδα 2η : κεφ. 2^ο: Η κρυπτογραφία στη Σύγχρονη εποχή</td></tr>
<tr><td>1</td><td>Κάλλης Θοδωρής</td><td rowspan="4">2.1. Κωδικοποίηση της πληροφορίας
2.1.1. Αναπαράσταση της πληροφορίας στον Η/Υ
2.1.2. Δυαδικό σύστημα,
2.1.3. Κώδικας ASCII,
2.1.4. κώδικας UNICODE
2.1.5. Ραβδωτός κώδικας
2.1.6. Μαγνητικές κάρτες
2.1.7. Ασφάλεια ηλεκτρονικών συναλλαγών

Παράρτημα : Η ορολογία της Κρυπτογραφίας (Το λεξικό της κρυπτογραφίας)</td></tr>
<tr><td>2</td><td>Κουτρομάνου Λουκία</td></tr>
<tr><td>3</td><td>Μπελεσάκου Φένια</td></tr>
<tr><td>4</td><td>Τσιώλη Θεοδώρα</td></tr>
<tr><td colspan="3"></td></tr>
</table>

Ομάδα 3η : κεφ. 3ο: Κρυπτογραφία και Η/Υ		
1	Κραβαρίτης Αλέξανδρος	**3.1.Βασικές έννοιες** **3.2. Η κρυπτογραφία από το 1950 έως σήμερα** 3.2.1. Συμμετρικά συστήματα κρυπτογραφίας 3.2.2. Ασύμμετρα συστήματα κρυπτογραφίας **3.3.Ψηφιακές Υπογραφές** **3.4. Το σύστημα μετάδοσης των θεμάτων στις πανελλαδικές εξετάσεις** (συνέντευξη με τον δ/ντη του σχολείου και τον χειριστή του συστήματος VBI)
2	Μαργώνη Αγγελική	
3	Χαλιμούρδα Κωνσταντίνα	
Ομάδα 4η: πρόλογος και κεφ. 4ο: Κρυπτογραφία και Τέχνη		
1	Κούλια Κωνσταντίνα	Πρόλογος –εισαγωγή όλης της εργασίας 4.1. Η κρυπτογραφία στον Κινηματογράφο 4.2. Η κρυπτογραφία στην Λογοτεχνία 4.3. Μηχανή Enigma 4.4. Δημιουργία ενός δικού μας κώδικα κρυπτογράφησης.
2	Κουτρομάνου Γεωργία	
3	Πρωτόπαππα Νεκταρία	
4	Τσιώλης Παναγιώτης	

Υπεύθυνη καθηγήτρια: ΧΑΛΙΜΟΥΡΔΑ ΑΓΓΕΛΙΚΗ –ΠΕ19- Πληροφορικός

ΠΕΡΙΛΗΨΗ

Ομάδα 1η: Σε αυτό το τετράμηνο το θέμα μας ήταν η κρυπτογραφία. Η ομάδα μας ανέλαβε να περιγράψει συνοπτικά το αντικείμενο της κρυπτογραφίας και τις εφαρμογές της και πιο αναλυτικά την ιστορική της πορεία από την εποχή των ιερογλυφικών μέχρι την εποχή του ηλεκτρισμού και τον κώδικα Μορς. Για να επιτευχθεί ο σκοπός της ερευνάς μας χωρίσαμε το θέμα μας σε επιμέρους ενότητες και κάθε άτομο της ομάδας μας ανέλαβε από μια υποενότητα. Στο τέλος συγκεντρώσαμε όλα μας τα στοιχεία, τα επεξεργαστήκαμε, τα ενώσαμε και κάναμε τις απαραίτητες διορθώσεις. Έτσι προέκυψε η παρακάτω εργασία.

Ομάδα 2η: Στο δεύτερο τετράμηνο στα πλαίσια του μαθήματος "Ερευνητική Εργασία" ασχοληθήκαμε με την κρυπτογραφία. Συγκεκριμένα, εμείς, η 2η ομάδα επιλέξαμε το υπόθεμα ¨Κρυπτογραφία στην σύγχρονη εποχή¨ το οποίο αποτελείται από την κωδικοποίηση της πληροφορίας στον Η/Υ και από την ορολογία της κρυπτογραφίας. Αρχικά ασχοληθήκαμε με την αναπαράσταση της πληροφορίας στον Η/Υ, το δυαδικό σύστημα και τους κώδικες ASCII και UNICODE. Τέλος ασχοληθήκαμε με την εύρεση και την καταγραφή των όρων της κρυπτογραφίας και προσπαθήσαμε να δημιουργήσουμε ένα λεξιλόγιο κρυπτογραφίας.

Ομάδα 3η: Σε αυτό το τετράμηνο η ομάδα μας ασχολήθηκε με την κρυπτογραφία και πιο συγκεκριμένα με τη σύγχρονη μορφή της και την σχέση της με τους ηλεκτρονικούς υπολογιστές και την σύγχρονη επικοινωνία. Περιγράψαμε τα κρυπτοσυστήματα (το σύνολο των διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης) και τις βασικές κατηγορίες - είδη αυτών. Αναλύσαμε τους όρους των υποσυστημάτων καθώς και τα στοιχεία που χρησιμοποιούνται για την επίτευξη της κρυπτογράφησης, επιδιώκοντας να κάνουμε πιο κατανοητό το εννοιολογικό της περιεχόμενο.

Επίσης παραθέσαμε παραδείγματα χρήσης κρυπτογραφίας στην καθημερινή μας ζωή όπως η χρήση ψηφιακής υπογραφής και το σύστημα πανελλαδικών εξετάσεων αλλά και η χρήση κινητών τηλεφώνων. Τέλος δημιουργήσαμε ένα κείμενο σε μορφή παιχνιδιού ώστε οι μαθητές μέσα από τη διασκέδαση να μπορέσουν να αφομοιώσουν τους βασικούς όρους της κρυπτογραφίας.

Ομάδα 4η: Από το συνολικό θέμα του τμήματος μας για αυτό το τετράμηνο, εμείς ως τέταρτη ομάδα αναλάβαμε το κεφάλαιο με θέμα κρυπτογραφία και τέχνη. Το κεφάλαιο μας το χωρίσαμε σε 4 επιμέρους θέματα. Συγκεκριμένα:

1. Η κρυπτογραφία στον Κινηματογράφο
2. Η κρυπτογραφία στην Λογοτεχνία

3. Μηχανή Enigma
4. Δημιουργία ενός δικού μας κώδικα κρυπτογράφησης.

Αρχικά ασχοληθήκαμε με την κρυπτογραφία στον κινηματογράφο εστιάζοντας στον κώδικα DA VINCI και σε μια από τις ταινίες του James Bond. Ακολούθησε η κρυπτογραφία στην Λογοτεχνία όπου αναφερθήκαμε στο βιβλίο "Η επιστροφή του Σέρλοκ Χόλμς" και στην ιστορία "DancingMen - οι Χορευτές", συγγεγραμμένο από τον Arthur Conan Doyle καθώς και στο βιβλίο του Dan Brown με τίτλο «Ψηφιακό Οχυρό». Στη συνέχεια βρήκαμε πληροφορίες για την μηχανή Enigma και την ζωή και το έργο του Άλαν Τιούρινγκ καθώς και για την σημαντική συνεισφορά του στην αποκρυπτογράφηση των μηνυμάτων των γερμανών κατά τον Β' Παγκόσμιο Πόλεμο. Τέλος, δημιουργήσαμε έναν δικό μας κώδικα κρυπτογράφησης μηνυμάτων, χρησιμοποιώντας τα emoticons.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. ΕΙΣΑΓΩΓΗ

Στο δεύτερο τετράμηνο του σχολικού έτους 2014-2015 στα πλαίσια του μαθήματος ερευνητική εργασία, το τμήμα μας αποφάσισε να ασχοληθεί με το θέμα της κρυπτογραφίας. Σκοποί και στόχοι του συγκεκριμένου θέματος ήταν:

- ✓ να διαπιστώσουμε την ανάγκη διασφάλισης της εγκυρότητας και αυθεντικότητας των πληροφοριών που διακινούνται καθημερινά
- ✓ να αναγνωρίσουμε τους κινδύνους από πιθανές διαρροές σημαντικών ή έμπιστων πληροφοριών
- ✓ να κατανοήσουμε τους πολλαπλούς τρόπους και μεθόδους αποκρυπτογράφησης
- ✓ να δημιουργήσουμε δικό μας κώδικα κρυπτογράφησης
- ✓ να καλλιεργήσουμε συνεργατικές δεξιότητες και να αναπτύξουμε πνεύμα συλλογικής δημιουργίας με την ανταλλαγή και σύνθεση διαφορετικών απόψεων.

Χωριστήκαμε σε τέσσερις ομάδες και κάθε ομάδα ανέλαβε ένα υπόθεμα. Κατά την διάρκεια της εργασίας μας καταγράψαμε την ιστορική εξέλιξη της κρυπτογραφίας από την αρχαιότητα έως σήμερα και προσπαθήσαμε να περιγράψουμε βασικούς ορισμούς που διέπουν τον κλάδο της κρυπτογραφίας. Επιπλέον, εξετάσαμε την συμβολή της κρυπτογραφίας στην σύγχρονη εποχή. Περιγράψαμε τον τρόπο που γίνεται η αναπαράσταση της πληροφορίας στον ηλεκτρονικό υπολογιστή (δυαδικό σύστημα, κώδικες όπως ο κώδικας ASCII και ο κώδικας UNICODE). Στην συνέχεια, αναζητήσαμε πληροφορίες για την κρυπτογραφία και τη σχέση της με τον ηλεκτρονικό υπολογιστή (κρυπτοσυστήματα, αλγόριθμοι κρυπτογράφησης, ψηφιακές υπογραφές κ.λπ.) και τα συστήματα επικοινωνίας και ανταλλαγής πληροφοριών. Επίσης, αναφερθήκαμε στην επιρροή της κρυπτογραφίας στον χώρο των τεχνών και δημιουργήσαμε έναν δικό μας κώδικα αποκρυπτογράφησης καταγράφοντας ένα αποκρυπτογραφημένο μήνυμα. Τέλος, για την καλύτερη δυνατή συνεργασία μεταξύ των μελών του τμήματος και της καθηγήτριας μας για την πραγματοποίηση της εργασίας, δημιουργήσαμε μία ηλεκτρονική τάξη στο edmodo όπου ανταλλάσαμε πληροφορίες όλες οι ομάδες της ερευνητικής εργασίας με την υπεύθυνη καθηγήτρια.

2. ΘΕΩΡΗΤΙΚΟ ΜΕΡΟΣ

ΚΕΦ. 1ο : Εισαγωγή, Ιστορική αναδρομή – Μια ματιά στο παρελθόν

1.1. Εισαγωγή

1.1.1. Ορισμός

Η λέξη **κρυπτογραφία** προέρχεται από τα συνθετικά «κρυπτός» + «γράφω» και είναι ένα διεπιστημονικό γνωστικό πεδίο που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Η κρυπτογραφία είναι ο ένας από τους δύο κλάδους της **κρυπτολογίας** (ο άλλος είναι η **κρυπτανάλυση**), η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Σήμερα η κρυπτολογία θεωρείται ένα διεπιστημονικό γνωστικό πεδίο, το οποίο μπορεί να μελετηθεί ως όψη των εφαρμοσμένων μαθηματικών, της θεωρητικής πληροφορικής ή της επιστήμης ηλεκτρονικού μηχανικού. Παρεμφερείς κλάδοι είναι αντιστοίχως, η στεγανογραφία και η στεγανοανάλυση.

Η σημασία της κρυπτολογίας είναι τεράστια στους τομείς της ασφάλειας υπολογιστικών συστημάτων και τηλεπικοινωνιών. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς ώστε δύο ή περισσότερα άκρα επικοινωνίας (π.χ άνθρωποι, προγράμματα υπολογιστών κλπ.) να ανταλλάξουν μηνύματα, χωρίς κανένας τρίτος να είναι ικανός να διαβάζει την περιεχόμενη πληροφορία εκτός από τα δύο κύρια άκρα.

Ιστορικά η κρυπτογραφία χρησιμοποιήθηκε για τη μετατροπή της πληροφορίας μηνυμάτων από μια κανονική, κατανοητή μορφή σε έναν «γρίφο», που χωρίς τη γνώση του κρυφού μετασχηματισμού θα παρέμενε ακατανόητος. Κύριο χαρακτηριστικό των παλαιότερων μορφών κρυπτογράφησης ήταν ότι η επεξεργασία γινόταν πάνω στην γλωσσική δομή του μηνύματος. Στις νεότερες μορφές η κρυπτογραφία κάνει χρήση του αριθμητικού ισοδύναμου (πίνακας αντιστοίχησης γραμμάτων με αριθμούς), ενώ η έμφαση έχει μεταφερθεί σε διάφορα πεδία των μαθηματικών (π.χ διακριτά μαθηματικά, θεωρία αριθμών, θεωρία πληροφορίας, στατιστική και συνδυαστική ανάλυση).

1.2. Ιστορική αναδρομή

1.2.1. Ιερογλυφικά , Γραμμική γραφή Α , Γραμμική Γραφή Β

- **ΙΕΡΟΓΛΥΦΙΚΑ**

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

Όπως προκύπτει από μια μικρή σφηνοειδή επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, οι πολιτισμοί που αναπτύχτηκαν στην Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία ήδη από το 1500 π.χ. Η επιγραφή αυτή περιγράφει μια μέθοδο κατασκευής σμάλτων για αγγειοπλαστική και θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο (με βάση τον Kahn). Επίσης, ως το αρχαιότερο βιβλίο κρυπτοκωδικών στο κόσμο, θεωρείται μια σφηνοειδής επιγραφή στα Σούσα της Περσίας, η οποία περιλαμβάνει τους αριθμούς 1-8 και από το 32-35, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καθένα σφηνοειδή σύμβολα.

Η μεγαλύτερη αποκρυπτογράφηση ήταν αυτή των αιγυπτιακών ιερογλυφικών τα οποία, επί αιώνες, παρέμεναν μυστήριο και οι αρχαιολόγοι μόνο εικασίες μπορούσαν να διατυπώσουν για την σημασία τους. Ωστόσο, χάρη σε μια κρυπτοαναλυτική εργασία, τα ιερογλυφικά εν τέλει αναλύθηκαν και εκ τότε οι αρχαιολόγοι είναι σε θέση να διαβάζουν ιστορικές επιγραφές. Τα αρχαιότερα ιερογλυφικά χρονολογούνται περίπου από το 3000 π.χ. Τα σύμβολα των ιερογλυφικών ήταν υπερβολικά πολύπλοκα για την καταγραφή των συναλλαγών εκείνης της εποχής. Έτσι, παράλληλα με αυτά, αναπτύχτηκε για καθημερινή χρήση η ιερατική γραφή, που ήταν μια συλλογή συμβόλων, τα οποία ήταν εύκολα τόσο στο γράψιμο όσο και στην ανάγνωση. Τον $17^{ο}$ αιώνα αναθερμάνθηκε το ενδιαφέρον για την αποκρυπτογράφηση των ιερογλυφικών, έτσι το 1652 ο Γερμανός Ιησουίτης Αθανάσιος Κίρχερ εξέδωσε ένα λεξικό ερμηνείας τους, με τίτλο «Oedipus Aegyptiacus». Με βάση αυτό προσπάθησε να ερμηνεύσει τις αιγυπτιακές γραφές, αλλά η προσπάθεια του αυτή ήταν κατά γενική ομολογία αποτυχημένη. Για παράδειγμα, το όνομα του Φαραώ Απριη, το ερμήνευσε σαν «τα ευεργετήματα του θεϊκού Οσιρι εξασφαλίζονται μέσω των ιερών τελετών της αλυσίδας των πνευμάτων, ώστε να επιδαψιλεύσουν τα δώρα του Νείλου». Παρόλα αυτά, η προσπάθεια του άνοιξε

το δρόμο προς την σωστή ερμηνεία των ιερογλυφικών, που προχώρησε χάρη στην ανακάλυψη της «στήλης της Ροζέτας». Ήταν μια πέτρινη στήλη που βρήκαν τα στρατεύματα του Ναπολέοντα στην Αίγυπτο και είχε χαραγμένο πάνω της το ίδιο κείμενο τρεις φορές. Μια με ιερογλυφικά, μια στα ελληνικά και μια στην ιερατική γραφή. Δυο μεγάλοι αποκρυπτογράφοι της εποχής, ο Γιανγκ και ο Σαμπολιόν, μοιράστηκαν την δόξα της ερμηνείας τους. Οι προϊστορικοί πληθυσμοί χρησιμοποίησαν τρεις γραφές μέχρι να επινοήσουν αλφάβητο γύρω στο 850 π.χ.

Εικόνα 1. Ιερογλυφικά

- **ΓΡΑΜΜΙΚΗ ΓΡΑΦΗ Α΄**

Η Γραμμική Α' είναι μια Μινωική γραφή που ανακαλύφθηκε στην Κρήτη από τον Άρθουρ Έβανς το 1900. Η γραφή αυτή θεωρείται πρόγονος της Γραμμικής Β, η οποία είναι Μυκηναϊκή.

Οι πρώτες επιγραφές με γραμμική γραφή ανακαλύφθηκαν από τον Sir Arthur Evans, τον πρώτο άγγλο αρχαιολόγο που ανάσκαψε συστηματικά την Κνωσό το 1900. Ο ίδιος ονόμασε αυτή τη γραφή γραμμική επειδή τα γράμματα της είναι γραμμές και όχι σφήνες όπως στην σφηνοειδή γραφή. Τα γράμματα της χαράζονται πάνω σε πήλινες πλάκες, οι οποίες κατόπιν ξεραίνονται σε φούρνους. Οι περισσότερες επιγραφές με Γραμμική Γραφή Α΄ είναι λογιστικές και περιέχουν συντομογραφίες των εμπορευσίμων προϊόντων και αριθμούς για υπόδειξη.

Ο Evans κατέγραψε 135 σύμβολα της. Παρά την πρόοδο όμως που έχει σημειωθεί ακόμη δεν έχει επιτευχθεί η αποκρυπτογράφηση της.

Χαρακτηριστικό παράδειγμα της Γραμμικής Α΄ αποτελεί ο δίσκος της Φαιστού:

Εικόνα 2. Ο δίσκος της Φαιστού

Ο Δίσκος της Φαιστού είναι ένα αρχαιολογικό εύρημα από τη Μινωική πόλη της Φαιστού στη νότια Κρήτη και χρονολογείται πιθανώς στον 17ο αιώνα π.Χ.. Αποτελεί ένα από τα γνωστότερα μυστήρια της αρχαιολογίας, αφού ο σκοπός της κατασκευής του και το νόημα των όσων αναγράφονται σε αυτόν παραμένουν άγνωστα.

- **ΓΡΑΜΜΙΚΗ ΓΡΑΦΗ Β΄**

Γνωρίζουμε πως η πρώτη γραφή που έγραφαν την γλώσσα τους, ήταν μια μορφή της προελληνικής γραφής που την ονομάζουμε Γραμμική Β. Οι επιγραφές που χρονολογούνται περίπου στον 13^{ο} αιώνα και βρέθηκαν στη Πύλο, στις Μυκήνες και την Κνωσό είναι οι παλαιότερες και είναι γραμμένες με αυτό το προελληνικό αλφάβητο.

Εικόνα 3. Γραμμική γραφή Β

Οι άνθρωποι εκείνης της εποχής έπλαθαν πηλό σε σχήμα κυλίνδρου, τον τοποθετούσαν σε λεία επιφάνεια και την πίεζαν μέχρι να γίνει επίπεδη, επιμήκης και συμπαγής πινακίδα, σαφώς διαφοροποιημένη σε δυο επιφάνειες: μια επίπεδη λειασμένη, που επρόκειτο να αποτελέσει την κύρια γραφική επιφάνεια και μια κυρτή, που συνήθως έμενε άγραφη. Συστηματικά, με την γραφή αυτή, με την οποία είχε πραγματικό πάθος, ασχολήθηκε ο Άγγλος αρχιτέκτονας και αρχαιολόγος Μαικλ Βεντρις ο οποίος ήταν ο πρώτος που κατάλαβε ότι επρόκειτο για κάποιο είδος ελληνικής γραφής.

Εικόνα 4. Γραμμική γραφή Β

Μέσα από ιστορικές αναφορές που έχουν διασωθεί μέχρι σήμερα παρουσιάζονται παρά πολλά μηνύματα. Μερικά μηνύματα έπρεπε πάντα να σταλούν με την μεγίστη ασφάλεια. Γι' αυτό χρησιμοποιήθηκαν διάφορες μέθοδοι ώστε τα μηνύματα να μπορούν να διαβαστούν μόνο απ' τον παραλήπτη και να είναι ακατανόητα σε βαθμό που να γίνονται άχρηστα για οποιονδήποτε άλλο. Μερικές μέθοδοι από αυτές δείχνουν πολύ απλοϊκές σήμερα, αλλά κάποιες άλλες δεν έχουν αποκρυπτογραφηθεί ακόμα.

1.2.2. Η κρυπτογραφία στους Ελληνορωμαϊκούς χρόνους

(Σπαρτιατική Σκυτάλη, Ο κώδικας τουΠολύβιου, Ρωμαϊκοί χρόνοι - Ο κώδικας του Καίσαρα)

- **ΣΠΑΡΤΙΑΤΙΚΗ ΣΚΥΤΑΛΗ**

Η σπαρτιατική σκυτάλη ήταν ένας διάσημος και ευφυής τρόπος επικοινωνίας που χρησιμοποιούσαν οι Σπαρτιάτες για να μην γίνονται αντιληπτοί από τους εχθρούς τους. Η τεχνικήαυτή χρησιμοποιήθηκε κυρίως για πολεμικούς σκοπούς.

Ηπρώτη σπαρτιατική σκυτάλη εμφανίστηκε τον 5ο αιώνα π.Χ.

Στην αρχαία Σπάρτη για την αποστολή στρατιωτικών μηνυμάτων το μήνυμα γραφόταν σ΄ένα κύλινδρο που γύρω του είχε τυλιχτεί μια στενή λωρίδα δέρματος σε διαδοχικές σειρές. Αυτή ήταν η περιβόητη σκυτάλη. Ο κύλινδρος αφαιρούνταν και έμενε η λωρίδα που μπορούσε να ξαναδιαβαστεί μόνο αν τυλιγόταν με τον ίδιο τρόπο πάνω σε ολόιδιας διαμέτρου κύλινδρο. Κάθε άλλη διαφορετική διάμετρος κυλίνδρου έδινε ακατανόητα μηνύματα. Πολλές φορές γραφόταν σε συνδυασμό με καθρέπτη, ώστε να απαιτείται καθρέπτης και στην ανάγνωση. Άλλη απλούστερη μέθοδος ήταν η αντιστροφή συλλαβών όπως «δημοκρατία» που θα φαινόταν σαν «ηδομαρκίτα».

Εικόνα 5. Η Σπαρτιατική Σκυτάλη

➢ Ο ΚΩΔΙΚΑΣ ΤΟΥ ΠΟΛΥΒΙΟΥ

Ο Πολύβιος (203 π.Χ. - 120 π.Χ.) ήταν Έλληνας ιστορικός διάσημος για το βιβλίο του "Οι Ιστορίες ή η Άνοδος της Ρωμαϊκής Αυτοκρατορίας", το οποίο καλύπτει λεπτομερώς την περίοδο από το 200 ως 146 π.Χ. Είναι επίσης γνωστός για τις πολιτικές του απόψεις σχετικά με την εξισορρόπηση των εξουσιών, απόψεις οι οποίες πολύ αργότερα χρησιμοποιήθηκαν κατά τη σύνταξη του Συντάγματος των Ηνωμένων Πολιτειών.

Στον Πολύβιο αποδίδεται ένα χρήσιμο εργαλείο στην τηλεγραφία, το οποίο επιτρέπει στην κωδικοποιημένη αποστολή γραμμάτων με την χρήση ενός αριθμητικού συστήματος. Στην ιδέα αυτή επίσης στηρίζονται η κρυπτογραφία και η στενογραφία. Το εργαλείο αυτό είναι γνωστό ως το «Τετράγωνο του Πολύβιου». Πρόκειται για ένα τετράγωνο 5Χ5, διαιρεμένο σε 25 μικρότερα ίσα τετραγωνάκια, όπου τοποθετούνται με τη σειρά οι χαρακτήρες της αλφαβήτου, από αριστερά προς τα δεξιά και από τα πάνω προς τα κάτω . Στη συνέχεια, οι σειρές και οι στήλες αριθμούνται οριζοντίως και καθέτως, συνήθως με τους αριθμούς από 1 έως 5. Έτσι, το κάθε ζεύγος 2 αριθμών αντιστοιχεί σε ένα συγκεκριμένο γράμμα και με τον τρόπο αυτό μπορεί να συνταχθεί κρυπτογραφικά ολόκληρη επιστολή.

Το τετράγωνο του Πολυβίου ή αλλιώς*Σκακιέρα του Πολυβίου* είναι ένας τρόπος που εφευρέθηκε από τον Πολύβιο και χρησιμοποιήθηκε από τους Αρχαίους Έλληνες για την κωδικοποίηση των μηνυμάτων που αντάλλασσαν φυλάκια μεταξύ τους. Ο λόγος που ο Πολύβιος δημιούργησε αυτόν τον πίνακα δεν ήταν άλλος παρά να δημιουργήσει μια μέθοδο που θα μπορούσε με απλό σχετικά τρόπο να μεταδώσει πληροφορίες μεταξύ απομακρυσμένων σημείων ιδιαίτερα αν τα σημεία αυτά είχαν οπτική επαφή. Η μορφή που είχε ο πίνακας για την Ελληνική γλώσσα είναι ο παρακάτω:

	1	2	3	4	5
1	Α	Β	Γ	Δ	Ε
2	Ζ	Η	Θ	Ι	Κ
3	Λ	Μ	Ν	Ξ	Ο
4	Π	Ρ	Σ	Τ	Υ
5	Φ	Χ	Ψ	Ω	

Εικόνα 6. Το τετράγωνο του Πολύβιου

Το αυθεντικό Τετράγωνο του Πολυβίου βασίστηκε στην ελληνική αλφάβητο (για αυτό το λόγο δεν είναι συμπληρωμένο και το κελί 55), ωστόσο η ίδια μεθοδολογία μπορεί να εφαρμοσθεί με

την ίδια επιτυχία για κάθε αλφάβητο. Έτσι οι Ιάπωνες από το 1500 έως το 1910 έκαναν χρήση του Τετραγώνου του Πολυβίου, τροποποιημένο ώστε να καλύπτει τα 48 γράμματα την Ιαπωνικής (πίνακας 7Χ7). Αντίστοιχα το μέγεθος του πίνακα μπορεί να τροποποιηθεί σε 6 επί 6 δίνοντας τη δυνατότητα να κωδικοποιηθεί η Κυριλλική αλφάβητος (που περιλαμβάνει από 33 έως 37 γράμματα).

Ο τρόπος λειτουργίας του πίνακα είναι απλός: κάθε γράμμα αναπαριστάται από τις συντεταγμένες του στον πίνακα. Έτσι ανάλογα με τη γλώσσα και το μέγεθος του πίνακα που έχουμε επιλέξει κωδικοποιούνται τα γράμματα και ακολούθως οι λέξεις. Έτσι για την αγγλική λέξη ¨BAT¨ με βάση τον πρώτο πίνακα (διαστάσεων 5 Χ 5) η αντιστοίχηση είναι ¨12 11 44¨ ενώ με το δεύτερο πίνακα (διαστάσεων 6 Χ 6) γίνεται ¨12 11 42¨. Η ελληνική λέξη ¨ΝΙΚΗ¨ μετασχηματίζεται στη σειρά ¨33 24 25 22¨.

- **Ο ΚΩΔΙΚΑΣ ΤΟΥ ΚΑΙΣΑΡΑ**

Στους Ελληνορωμαϊκούς χρόνους η πρώτη μέθοδος υποκατάστασης γραμμάτων για στρατιωτικούς σκοπούς εμφανίστηκε στους γαλατικούς πολέμους. Ο Ιούλιος Καίσαρας έγραφε στον Κικέρωνα και σε άλλους φίλους του, αντικαθιστώντας τα γράμματα του κειμένου, με γράμματα, που βρίσκονται 3 θέσεις μετά στο Λατινικό αλφάβητο. Έτσι, σήμερα το σύστημα κρυπτογράφησης που στηρίζεται στην αντικατάσταση των γραμμάτων του αλφάβητου με άλλα που βρίσκονται σε καθορισμένο αριθμό θέσης πριν ή μετά λέγεται κρυπτοσύστημα αντικατάστασης του Καίσαρα.

Για παράδειγμα η φράση VENI, VIDI, VICI κρυπτογραφείται σε YHQL, YLGL, YLFL.

Εικόνα 7. Ο κώδικας του Καίσαρα

Ο Καίσαρας χρησιμοποίησε και άλλα πιο πολύπλοκα συστήματα κρυπτογράφησης, για τα οποία έγραψε ένα βιβλίο ο Valerius Probus, το οποίο δυστυχώς δεν διασώθηκε, αλλά αν και χαμένο, θεωρείται το πρώτο βιβλίο κρυπτολογίας. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες.

1.2.3. Η κρυπτογραφία στο Μεσαίωνα (Το χειρόγραφο Βόϊνιτς, πρώτοι αλγόριθμοι, κώδικας Vigenere)

- **ΤΟ ΧΕΙΡΟΓΡΑΦΟ ΒΟΪΝΤΣ**

Το χειρόγραφο Βόϊνιτς πήρε το όνομά του από αυτόν που το ανακάλυψε το 1912 σε ένα ιταλικό μοναστήρι και είναι ίσως το πιο μυστηριώδες βιβλίο στην ιστορία του κόσμου. Πρόκειται για ένα βιβλίο γραμμένο σε μια ακατανόητη γλώσσα, με ακαταλαβίστικο περιεχόμενο και μυστηριώδεις εικονογραφήσεις. Οι επιστήμονες εκτιμούν ότι γράφτηκε πριν από αιώνες (400 έως 800 χρόνια περίπου) από κάποιον άγνωστο συγγραφέα που χρησιμοποίησε έναν άγνωστο κώδικα γραφής.

Από τις σελίδες του, το μόνο που μπορεί να καταλάβει κανείς είναι ότι χρησίμευε ως φαρμακολόγιο, καθώς φαίνεται να περιγράφει θέματα μεσαιωνικής και πρώιμης ιατρικής, αλλά και ως αστρονομικός και κοσμολογικός χάρτης. Αυτά όμως που ξενίζουν ακόμα περισσότερο από την γλώσσα γραφής, είναι οι εικόνες άγνωστων φυτών, κοσμολογικά διαγράμματα και παράξενες απεικονίσεις γυμνών γυναικών μέσα σε ένα πράσινο υγρό.

Εικόνα 8. Το χειρόγραφο Βόινιτς

Δεκάδες κρυπταναλυτές, μελετητές και επιστήμονες επιχείρησαν να το μεταφράσουν αλλά χωρίς αποτέλεσμα. Πολλοί έφτασαν στο συμπέρασμα ότι στην ουσία πρόκειται για μια καλοστημένη φάρσα, ότι τα κρυπτογραφημένα λόγια είναι μια δίχως νόημα εναλλαγή τυχαίων χαρακτήρων και ότι οι ανορθόδοξες εικόνες ανήκουν αποκλειστικά στην σφαίρα της φαντασίας. Σήμερα βρίσκεται στη Βιβλιοθήκη Σπανίων Χειρογράφων Beinecke του πανεπιστημίου Γέιλ, με το κωδικό όνομα MS408 και κανένας δεν κατάφερε μέχρι τώρα να αποκρυπτογραφήσει ούτε μια λέξη.

➢ ΚΡΥΠΤΟΓΡΑΦΙΑ - ΠΡΩΤΟΙ ΑΛΓΟΡΙΘΜΟΙ

Ο σημαντικότερος εκπρόσωπος των Αράβων κρυπτολόγων είναι ο πανεπιστήμων του 9^{ου} αιώνα Αλ Κιντί. Έγραψε πάνω από 290 βιβλία Μαθηματικών, Γλωσσολογίας, Αστρολογίας, Ιατρικής και Μουσικής.

Η Ευρωπαϊκή κρυπτογραφία έχει τις ρίζες της στο μεσαίωνα, ξεκίνησε από τα Παπικά κράτη και άλλες Ιταλικές πόλεις - κράτη. Από τα πρώτα συστήματα κρυπτογραφίας, ήταν εκείνο κατά το οποίο, αντικαθιστούσαν τα φωνήεντα, αφήνοντας τα σύμφωνα όπως έχουν

Ένα από τα πρώτα έγγραφα της εποχής με οδηγίες για τηνκρυπτογράφηση εγγράφων, χρονολογείται γύρω στο 1379 και είναι ένας συνδυασμός κρυπτοσυστημάτων από τον Gabriele de Lavinde της Πάρμας, που υπηρετούσε τον Πάπα Κλεμέντιο τον 7ο. Αυτό το έγγραφο, που τώρα βρίσκεται στα αρχεία του Βατικανού, περιέχει ένα σύνολο κλειδιών για 24 παραλήπτες και χρησιμοποιεί σύμβολα όπως γράμματα, αριθμούς και μερικούς κώδικες δύο γραμμάτων που συμβόλιζαν λέξεις και ονόματα.

Τα πρώτα συνοπτικά λεξιλόγια (nomenclators), σιγά-σιγά αναπτύχθηκαν και χρησιμοποιήθηκαν για αρκετούς αιώνες στις διπλωματικές συνομιλίες σε όλες σχεδόν τις Ευρωπαϊκές κυβερνήσεις. Για παράδειγμα, το Equatorie of the Planetris (1390), του Geoffrey Chaucer, περιέχει κείμενα κρυπτογραφημένα. Το1470, ο Leon Battista Alberti, εξέδωσε το "Tratta ti in cifra", στο οποίο περιέχονται περιγραφές ενός κρυπτογραφικού δίσκου, με τον οποίο μπορούσαν να κρυπτογραφήσουν μικρά κείμενα. Οι περισσότεροι, παρ' όλα αυτά, θεώρησαν τον Johannes Trithemius, ιερέα στην Spanheim της Γερμανίας, πατέρα της σύγχρονης κρυπτογραφίας. Ο Trithemius, το 1510, έγραψε την "Polygraphia", την πρώτη εκδιδόμενη εργασία για την κρυπτογραφία. Για πρώτη φορά παρουσίασε την ιδέα ενός τετραγώνου, στο οποίο η αλφαβήτα, μεταφερόταν σε ένα προκαθορισμένο αριθμό διαστημάτων. Κάθε σειρά στην αλφαβήτα, στη συνέχεια, χρησιμοποιούταν για να κρυπτογραφήσει ένα προκαθορισμένο αριθμό διαστημάτων. Για

παράδειγμα, το πρώτο γράμμα κρυπτογραφούταν με το πρώτο αλφάβητο, το δεύτερο γράμμα με το δεύτερο κοκ. τότε η λέξη Secret θα γινόταν: S(S+0) F(E+1) E(C+2) U(R+3)I(E+4) Y(T+5) δηλαδή SFEUIY.

Αργότερα, το 1605, ο Francis Bacon, παρουσιάζει το Κρυπτοσύστημα του, το οποίο βασιζόταν στη δημιουργία συνδυασμών των γραμμάτων a και b ανά 5, που ο καθένας τους σήμαινε ένα γράμμα της αλφαβήτου. Ο συγκεκριμένος κώδικας, παρουσιάζει για πρώτη φορά την αρχή ότι ο κώδικας με δύο σύμβολα μπορεί να χρησιμοποιηθεί για τη μεταφορά πληροφοριών.

Το 1860, μεγάλοι κώδικες χρησιμοποιήθηκαν για τις διπλωματικές αποστολές. Τα κρυπτογραφικά συστήματα επικρατούσαν στις στρατιωτικές επικοινωνίες, εκτός από τις επικοινωνίες μεταξύ των υψηλά ιστάμενων, εξαιτίας της δυσκολίας στην προστασία των βιβλίων με τα κρυπτοσυστήματα στο πεδίο της μάχης. Στην πρώιμη ιστορία των Ηνωμένων Πολιτειών, οι κώδικες ήταν δημοφιλείς. Κατά τη διάρκεια του Εμφυλίου, ο στρατός των Βορείων πρώτος χρησιμοποίησε κρυπτοσυστήματα στα οποία μία λέξη κλειδί έδειχνε τον τρόπο με τον οποίο θα έπρεπε να διαβαστούν οι στήλες στο κείμενο ή άλλα κρυπτοσυστήματα στα οποία υπήρχε αντικατάσταση κειμένου από άλλες λέξεις ή κώδικα. Από την άλλη πλευρά ο στρατός των Νοτίων χρησιμοποιούσε το Κρυπτοσύστημα Vigenère και κατά περίπτωση αντικαταστάσεις μόνο γραμμάτων.

- **ΚΩΔΙΚΑΣ VIGENERE**

Ένας αλγόριθμος κρυπτογράφησης λέγεται συμμετρικός όταν γνωρίζουμε το κλειδί κρυπτογράφησης k και είναι υπολογιστικά «εύκολο» να προσδιορίσουμε το κλειδί αποκρυπτογράφησης k΄ που είναι αντίστροφο. Στις περισσότερες περιπτώσεις τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης είναι τα ίδια. Αυτοί οι αλγόριθμοι (συμμετρικοί) χρειάζονται την συμφωνία μεταξύ του αποστολέα και του παραλήπτη για το κλειδί που θα χρησιμοποιηθεί, για να μπορέσουν να επικοινωνήσουν με ασφάλεια. Η ασφάλεια των αλγόριθμων βασίζεται στην μυστικότητα αυτού του κλειδιού. Για όσο καιρό επιθυμούμε η επικοινωνία να παραμείνει μυστική, για τον ίδιο καιρό πρέπει και το κλειδί να παραμείνει μυστικό. Οι συμμετρικοί αλγόριθμοι μπορούν να διαιρεθούν σε δυο υποκατηγορίες:

α) οι αλγόριθμοι δέσμης, οι οποίοι λειτουργούν πάνω σε στοιχειά δεδομένων και

β) οι αλγόριθμοι ροής οι οποίοι λειτουργούν από bit προς bit

Η κρυπτογράφηση Vigenere είναι μια μέθοδος κρυπτογράφησης αλφαβητικού κειμένου με την χρήση μιας σειράς διαφορετικών αλγόριθμων κρυπτογράφησης του Καίσαρα με βάση τα γράμματα μιας λέξης-κλειδιού. Είναι μια απλή μορφή πολυαλφαβητικης υποκατάστασης.

Ο κώδικας Vigenere έχει εφευρεθεί εκ νέου πολλές φορές. Η μέθοδος αρχικά περιγράφεται από τον Giovan Battista Bellaso το 1553 στο βιβλίο του La cifra del.Sig.-Giovan Battista Bellaso.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Εικόνα 9. Το τετράγωνο Vigenere ή πίνακας Vigenere, επίσης γνωστό και ως rectatabula, μπορεί να χρησιμοποιηθεί για κρυπτογράφηση και αποκρυπτογράφηση

- **ΠΟΛΥΑΛΦΑΒΗΤΙΚΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΤΕΤΡΑΓΩΝΟΥ VIGENERE**.

Στα πολυαλφαβητικά κρυπτοσυστήματα κάθε γράμμα του μηνύματος αντικαθίσταται με ένα σύμβολο κάθε φορά από διαφορετικό αλφάβητο. Κάθε γράμμα του μηνύματος αντικαθίσταται με ένα σύμβολο κάθε φορά από διαφορετικό αλφάβητο. Ορίζεται ένας πίνακας αντιστοίχησης 1-1 από το αλφάβητο της γλώσσας σε πολλά διαφορετικά αλφάβητα ανακατεμένα η μη φυσικά αλφάβητα τα οποία αλφάβητα αλλάζουν κάθε φορά ανάλογα με τα γράμματα της κλείδας. Το τετράγωνο Vigenere περιέχει ουσιαστικά μια λίστα μετατοπισμένων αλφαβήτων της κάθε γλώσσας.

Παράδειγμα:

Επιλέγουμε σαν λέξη κλειδί την AVALANCHE και την γράφουμε επαναληπτικά πάνω από το κείμενο του μηνύματος. Το πρώτο γράμμα του μηνύματος είναι το L πηγαίνουμε στην στήλη που ο δείκτης είναι το L και στην γραμμή που δείχνει το γράμμα κλειδιού A στον πίνακα Vigenere

το στοιχείο που δείχνουν είναι το γράμμα L όπου είναι το παραγόμενο κρυπτόγραμμα. Η διαδικασία επαναλαμβάνεται για τα επόμενα γράμματα του μηνύματος. Η αντιστροφή διαδικασία οδηγεί στην αποκρυπτογράφηση.

Κωδική λέξη: AVALANCHEAVALANCHE

Έστω το μήνυμα: LANDINGINBLUECOAST

Το παραγόμενο κρυπτοκείμενο είναι:LVNOIAIPRBGUPCBCZX

Υπάρχουν δυο τύποι μεικτών αλφάβητων

- Κλείδα και ακολουθία
- Κλείδα και αναδιάταξη

Στην μέθοδο κλείδα και ακολουθία γράφουμε την κλείδα αφαιρώντας τα επαναλαμβανόμενα γράμματα και μετά συμπληρώνουμε τα υπόλοιπα γράμματα του αλφάβητου. Ενώ στην μέθοδο κλείδα και αναδιάταξη γράφουμε την κλείδα χωρίς επαναλαμβανόμενα γράμματα και γράφουμε από κάτω τα υπόλοιπα γράμματα σε γραμμές κάτω από τα αρχικά και διαβάζουμε τις στήλες που δημιουργούνται και τις τοποθετούμε στην στήλη κλειδιών. Οι μέθοδοι αυτές αύξησαν την πολυπλοκότητα του κρυπτοσυστήματος. Το μέγεθος τάξης κλειδιού είναι πολύ μεγάλο.

Έστω κείμενο P και κρυπτοκείμενο C, όπου τα κείμενα εκφράζονται με το αριθμητικό τους ισοδύναμο και επιλογή γλώσσας η αγγλική (26 σύμβολα) και επιλογή κλειδιού που ορίζει το αλφάβητο που θα χρησιμοποιηθεί κάθε φορά.

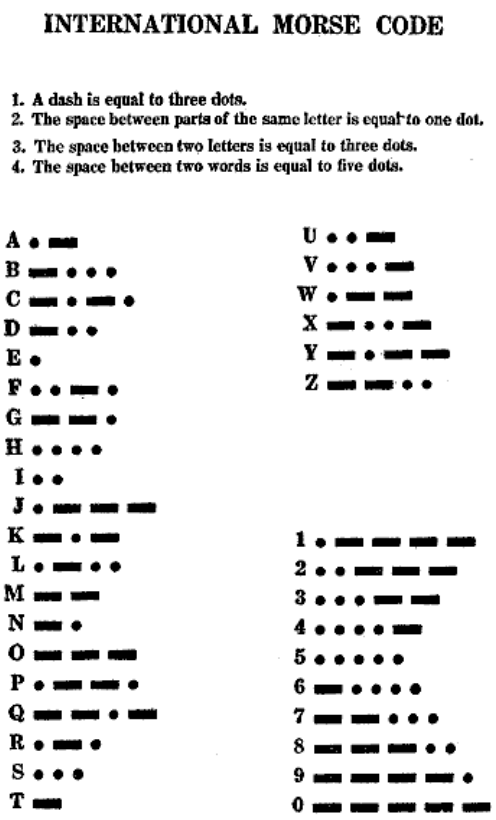
Η ασφάλεια του κρυπταλγορίθμου βασίζεται στην διάχυση των στατιστικών δεδομένων της γλώσσας. Η κατανομή γραμμάτων του κρυπτοκειμένου πλέον δεν παρουσιάζει μέγιστα και ελάχιστα, αλλά τείνει να γίνει επίπεδη. Το γράμμα Ε στην αγγλική γλώσσα διαμοιράζεται σε n διαφορετικά αλφάβητα δηλαδή κωδικοποιείται με n διαφορετικά γράμματα. Άρα η συχνότητα του καταμερίζεται σε n διαφορετικά γράμματα. Όπου n είναι οι χαρακτήρες του κλειδιού.

1.2.4. Η κρυπτογραφία την εποχή του ηλεκτρισμού – Κώδικας Μορς

Ο κώδικας Μορς (Morse code) είναι μια μέθοδος για μετάδοση πληροφορίας. Συγκεκριμένα, τα γράμματα των λέξεων και οι αριθμοί, αντιστοιχίζονται με σειρές από τελείες ή παύλες χρησιμοποιώντας ένα προσυμφωνημένο πίνακα αντιστοιχίας γραμμάτων – συμβόλων. Έπειτα, το κάθε γράμμα μπορεί να μεταδοθεί με ηχητικά ή φωτεινά σήματα.

Ο κώδικας Morse επινοήθηκε από τον Σάμιουελ Μόρς (Samuel Morse) το έτος 1830 και χρησιμοποιήθηκε για πρώτη φορά στις ενσύρματες τηλεγραφικές επικοινωνίες ξηράς. Μετά τα πρώτα πειράματα του Μαρκόνι για τις ασύρματες εκπομπές, έγινε ο βασικός τρόπος μετάδοσης των πληροφοριών μέσω ασυρμάτου.

Ο κώδικας Μορς είναι ο μόνος ψηφιακός κώδικας που μπορεί να ληφθεί ακουστικά από ανθρώπους, πράγμα που τον κάνει κατάλληλο για αυτόματη αποστολή σύντομων ψηφιακών μηνυμάτων σε φωνητικά κανάλια. Σήμερα χρησιμοποιείται μόνο σε εξειδικευμένες εφαρμογές όπως οι ραδιοφάροι.



Εικόνα 10. Διεθνής κώδικας Μορς

Ιστορικά, ο κώδικας Morse χρησιμοποιήθηκε από πολλές υπηρεσίες ραδιοεκπομπών, όπως εμπορική τηλεγραφία, ναυτιλιακές επικοινωνίες, αεροναυτιλία, στρατιωτικές επικοινωνίες και φυσικά από τους ραδιοερασιτέχνες, από τους οποίους συνεχίζει να χρησιμοποιείται μέχρι σήμερα, έχοντας φανατικούς φίλους στις τάξεις τους. Πρόκειται για το γνωστό τύπο εκπομπής CW (= continuous wave, συνεχές κύμα) κατά τον οποίο ο ραδιοερασιτέχνης δεν συνομιλεί με φωνή αλλά μέσω ενός ειδικού διακόπτη (χειριστήριο) στέλνει βραχείς ή μακρείς ήχους (τελείες ή παύλες) μέσω του ασυρμάτου του. Η ταχύτητα μετάδοσης μετράται σε «Λέξεις ανά Λεπτό» (Words per Minute, W.P.M) ή «Χαρακτήρες ανά Λεπτό».

Πλέον, μετά από αποφάσεις διεθνών φορέων του ραδιοερασιτεχνισμού, η γνώση του κώδικα δεν είναι απαραίτητο προσόν για τη χορήγηση της ραδιοερασιτεχνικής άδειας εκπομπής. Όμως για τα πλήρη δικαιώματα εκπομπής σε όλες τις ζώνες και ειδικά στα βραχέα κύματα (HF), στις περισσότερες χώρες η γνώση του κώδικα είναι υποχρεωτική.

ΚΕΦ.2ο : Η κρυπτογραφία στη Σύγχρονη εποχή

Κωδικοποίηση της πληροφορίας

2.1.1. Αναπαράσταση της πληροφορίας στον Η/Υ

Η αποθήκευση και επεξεργασία των δεδομένων στους ηλεκτρονικούς υπολογιστές γίνεται ψηφιακά. Ο Ηλεκτρονικός Υπολογιστής όμως διαχειρίζεται κυρίως ηλεκτρικά σήματα. Τα ηλεκτρικά σήματα αυτά, κυρίως για λόγους οικονομίας, μπορούν να εκφράζουν μόνο δύο καταστάσεις. Στα διάφορα τμήματα και κυκλώματα του υπολογιστή οι δύο αυτές καταστάσεις μπορεί να εκφράζονται από:

- Χαμηλή ή υψηλή τάση (0 και 1)
- Δύο διαφορετικής έντασης μαγνητικά πεδία (0 και 1)
- Ύπαρξη και ανυπαρξία οπτικής δέσμης (0 και 1)

Έτσι προκύπτει η ανάγκη τα δεδομένα που επεξεργάζεται ο υπολογιστής να κωδικοποιούνται με τη χρήση μόνο δύο στοιχείων, μια δυαδική μορφή.

2.1.2. Δυαδικό σύστημα

Το δυαδικό σύστημα αρίθμησης αναπαριστά αριθμητικές τιμές χρησιμοποιώντας δύο σύμβολα, το 0 και το 1. Πιο συγκεκριμένα, το δυαδικό είναι ένα θεσιακό σύστημα με βάση το δύο (αντίστοιχα μπορούμε να πούμε για το δεκαδικό αριθμητικό σύστημα που έχει βάση το 10). Κάθε ψηφίο ανήκει σε μία τάξη μεγέθους μεγαλύτερη κατά ένα από αυτήν του ψηφίου στα δεξιά του. Έτσι, κάθε ψηφίο ενός δυαδικού αριθμού από δεξιά προς τ' αριστερά δηλώνει μονάδες, δυάδες, τετράδες, οκτάδες κ.ο.κ (αντίστοιχα για το δεκαδικό αριθμητικό σύστημα έχουμε μονάδες, δεκάδες. εκατοντάδες κλπ).

- **Παράδειγμα μετατροπής από δεκαδικό σε δυαδικό σύστημα**

Ξεκινάμε στο δεκαδικό αριθμό μια σειρά από ακέραιες διαιρέσεις με το δύο και σταματάμε την διαδικασία όταν το πηλίκο γίνει μηδέν. Ας δούμε για παράδειγμα το 41 πως μετατρέπεται στο δυαδικό αριθμητικό σύστημα:

41 : 2	=	20 + **1** /2		
20 : 2	=	10 + **0** /2		
10 : 2	=	5 + **0** /2	⇨	**101001** - δυαδική μορφή του 41
5 : 2	=	2 + **1** /2		

2 : 2	=	1 + **0** / 2
1 : 2	=	0 + **1** / 2

Εικόνα 11. Παράδειγμα μετατροπής δεκαδικού αριθμού σε δυαδική μορφή

- **Μετατροπή από δυαδικό σε δεκαδικό σύστημα**

Για παράδειγμα ο δυαδικός αριθμός 101001

$$1 * 2^5 + 0 * 2^4 + 1 * 2^3 + 0 * 2^2 + 0 * 2^1 + 1 * 2^0 = 32+0+8+0+0+1= \mathbf{41}$$

Εικόνα 12. Παράδειγμα μετατροπής δεκαδικού αριθμού σε δυαδική μορφή

2.1.3. Κώδικας ASCII

Ο κώδικας ASCII είναι μια αμερικάνικη μορφή κώδικα που εξυπηρετεί την ανταλλαγή πληροφοριών. Συγκεκριμένα είναι ένα κωδικοποιημένο σύστημα χαρακτήρων του λατινικού αλφαβήτου όπως αυτό χρησιμοποιείται σήμερα στην αγγλική γλώσσα και σε άλλες δυτικοευρωπαϊκές γλώσσες .

USASCII code chart

b_7 b_6 b_5 →	0 0 0	0 0 1	0 1 0	0 1 1	1 0 0	1 0 1	1 1 0	1 1 1
b_4 b_3 b_2 b_1 ↓ Row	0	1	2	3	4	5	6	7
0 0 0 0	0	NUL	DLE	SP	0	@	P	`	p
0 0 0 1	1	SOH	DC1	!	1	A	Q	a	q
0 0 1 0	2	STX	DC2	"	2	B	R	b	r
0 0 1 1	3	ETX	DC3	#	3	C	S	c	s
0 1 0 0	4	EOT	DC4	$	4	D	T	d	t
0 1 0 1	5	ENQ	NAK	%	5	E	U	e	u
0 1 1 0	6	ACK	SYN	&	6	F	V	f	v
0 1 1 1	7	BEL	ETB	'	7	G	W	g	w
1 0 0 0	8	BS	CAN	(	8	H	X	h	x
1 0 0 1	9	HT	EM	)	9	I	Y	i	y
1 0 1 0	10	LF	SUB	*	:	J	Z	j	z
1 0 1 1	11	VT	ESC	+	;	K	[	k	{
1 1 0 0	12	FF	FS	,	<	L	\	l	|
1 1 0 1	13	CR	GS	-	=	M	]	m	}
1 1 1 0	14	SO	RS	.	>	N	^	n	~
1 1 1 1	15	SI	US	/	?	O	_	o	DEL

Εικόνα 12. Ο κώδικας ASCII

Ο κώδικας αυτός χρησιμοποιήθηκε για την απεικόνιση κειμένων στους υπολογιστές και σε διάφορα άλλα συστήματα όπως τηλεπικοινωνίες, που έχουν την δυνατότητα να δουλεύουν με κείμενα.

- **Ιστορική αναδρομή**

Ο ASCII αναπτύχθηκε με βάση τους τηλεγραφικούς κώδικες. Η πρώτη εμπορική χρήση του ήταν ως κώδικας ενός τηλέτυπου 7 bit της Bell. Συγκεκριμένα αναπτύχθηκε υπό την καθοδήγηση της επιτροπής του αμερικανικού οργανισμού τυποποίησης, γνωστή ως X3.

Ο οργανισμός τυποποίησης εξελίχθηκε σε ινστιτούτο τυποποίησης των Ηνωμένων Πολιτειών της Αμερικής και τελικώς σε Αμερικανικό Εθνικό Ινστιτούτο Τυποποίησης.

Η υποεπιτροπή X3.2 σχεδίασε τον ASCII με βάση παλιότερα συστήματα κωδικοποίησης τηλέτυπων. Όπως και άλλες κωδικοποιήσεις χαρακτήρων, ο ASCII καθορίζει μία αντιστοιχία μεταξύ ψηφιακών μοτίβων και σύμβολα - χαρακτήρων (γραφήματα και χαρακτήρες έλεγχου). Αυτό επιτρέπει σε ψηφιακές συσκευές να επικοινωνούν μεταξύ τους και να επεξεργάζονται, να αποθηκεύουν και να μεταδίδουν πληροφορίες σχετικές με χαρακτήρες, όπως η γραπτή γλώσσα. Πριν την ανάπτυξη του ASCII, οι κώδικες που ήταν σε χρήση περιλάμβαναν 26 αλφαβητικούς χαρακτήρες, 10 αριθμητικά ψηφία, και από 11 έως 25 ειδικά γραφικά σύμβολα, καθώς και χαρακτήρες ελέγχου

Η επιτροπή συζήτησε την πιθανότητα λειτουργίας πλήκτρου αλλαγής (shift, όπως στην κωδικοποίηση Baudot), η οποία θα επέτρεπε παραπάνω από 64 κωδικούς να αναπαρασταθούν με έξι bit. Σε ένα κωδικό με shift κάποιοι κωδικοί χαρακτήρων καθορίζουν εναλλαγή ανάμεσα σε κάποιες επιλογές για τους επόμενους κωδικούς χαρακτήρων. Αυτό επιτρέπει συμπαγή κωδικοποίηση, αλλά είναι λιγότερο αξιόπιστο για μετάδοση δεδομένων. Ένα σφάλμα στην μετάδοση του κωδικού με shift μπορεί να κάνει ένα μεγάλο τμήμα της μετάδοσης ακατάληπτο. Η επιτροπή τυποποίησης αποφάσισε κατά του shift και έτσι για τον ASCII απαιτούνταν κωδικοποίηση τουλάχιστον επτά bit.

Η επιτροπή εξέτασε την πιθανότητα κωδικοποίησης 8-bit, καθώς οκτώ bit θα επέτρεπαν αποδοτική κωδικοποίηση με μοτίβα τεσσάρων bit ψηφίων με δυαδικά κωδικοποιημένους δεκαδικούς (binary coded decimal). Αυτό ωστόσο θα απαιτούσε όλες οι μεταδόσεις δεδομένων να γίνονται με οκτώ bit, όταν επτά θα ήταν αρκετά. Η επιτροπή ψήφισε να χρησιμοποιηθεί κωδικοποίηση επτά bit ώστε να ελαχιστοποιηθεί το κόστος της μετάδοσης δεδομένων. Καθώς η

διάτρητη ταινία εκείνη την εποχή μπορούσε να καταγράψει οκτώ bit σε μία θέση, επέτρεπε την χρήση bit ισοτιμίας για έλεγχο σφαλμάτων αν αυτό ήταν επιθυμητό. Συσκευές με δυφιοοκτάδες (octet, ομαδοποίηση 8 bit) ως μητρικό τύπο δεδομένων που δεν χρησιμοποιούσαν έλεγχο ισοτιμίας συνήθως έθεταν το όγδοο bit στο 0.

Η κωδικοποίηση διατάχθηκε έτσι ώστε οι περισσότεροι κωδικοί ελέγχου να είναι μαζί, και όλοι οι γραφικοί κωδικοί μαζί. Οι πρώτες δύο στήλες (32 θέσεις) δεσμεύθηκαν για χαρακτήρες ελέγχου. Ο χαρακτήρας κενού (space) τοποθετήθηκε πριν από τους γραφικούς χαρακτήρες έτσι ώστε να γίνουν ευκολότεροι οι αλγόριθμοι ταξινόμησης, έτσι κατέλαβε την θέση 20. Η επιτροπή αποφάσισε ότι ήταν σημαντικό να υποστηρίζονται κεφαλαιογράμματα αλφάβητα 64 χαρακτήρων, και έτσι επέλεξε να δομήσει έτσι τον ASCII ώστε να μπορεί εύκολα να μετατραπεί σε σύνολο 64 γραφικών χαρακτήρων. Τα μικρά γράμματα έτσι δεν ανακατεύτηκαν με τα κεφαλαία. Οι ειδικοί και αριθμητικοί κωδικοί τοποθετήθηκαν πριν από τα γράμματα ώστε να υπάρχει ευελιξία, ενώ το γράμμα 'A' τοποθετήθηκε στη θέση 0x41 ώστε να ταιριάζει με το προσχέδιο του αντίστοιχου Βρετανικού προτύπου. Τα ψηφία 0-9 διατάχθηκαν έτσι ώστε να αντιστοιχούν σε τιμές με ψηφιακό πρόθεμα 011, κάνοντας έτσι εύκολη την αποκωδικοποίηση στο δεκαδικό.

Ο κώδικας ASCII περιλαμβάνει:

- 33 μη εκτυπώσιμους χαρακτήρες ελέγχου που χρησιμοποιούνται για έλεγχο
- 94 εκτυπώσιμους χαρακτήρες

Το κενό θεωρείται αόρατο γραφικό

- **ASCIIART**

Στην σύγχρονη κοινωνία , η τεχνολογία εξελίσσεται διαρκώς και χρησιμοποιεί νέα μέσα και συλλογές για να εντυπωσιάσει τον αναγνώστη.

Συγκεκριμένα, το facebook συμπεριλαμβάνει μία σειρά χαρακτήρων τα οποία η τέχνη ASCII μας έχει προσφέρει. Υπάρχουν περισσότερα από 1000 προσωπεία στα κοινωνικά δίκτυα, που οι χρήστες μπορούν να τα χρησιμοποιούν για να εκφράσουν τα συναισθήματα τους και να κάνουν ζωντανή τη συνομιλία τους. Έτσι η συλλογή αυτή βοηθάει στην ενίσχυση της διασκέδασης και επίτευξης της επικοινωνίας.

Emoticon Image	Meaning	Key
	Smile	:) :-) :] =)
	Confused	o.O O.o
	Unsure	:/ :-/ :\ :-\\
	Grumpy	>:(>:-(
	Upset	>:O >:-O >:o >:-o
	Sad	:-(:(:[=(
	Cry	:'(
	Tongue	:-P :P :-p :p =P
	Devil	3:) 3:-)
	Curly Lips	:3
	Angel	O:) O:-)
	Kiss	:-* :*
	Robot	:|]
	Grin	:-D :D =D
	Gasp	:-O :O :-o :o
	Chris Putnam	:putnam:
	Wink	;-) ;)
	Heart	<3
	Glasses	8-) 8) B-) B)
	Kiki	^_^
	Penguin	<(")
	Squint	-_-
	42	:42:
	Sunglasses	8-| 8| B-| B|
	Packman	:v
	Shark	(^^^)
	Like	(Y)

Εικόνα 13. Πίνακας αντιστοίχησης emoticons

2.1.4. Κώδικας Unicode

Ο κώδικας UNICODE είναι ένας διεθνής κώδικας που χρησιμοποιείται για την παράσταση των χαρακτήρων στους υπολογιστές. Επειδή ο αριθμός των χαρακτήρων που μπορούμε να παραστήσουμε με το κώδικα ASCII και τους άλλους κώδικες των 8 bit είναι περιορισμένος - το πολύ 256 συνδυασμοί – ήταν επιτακτική η ανάγκη να δημιουργηθεί ένας κώδικας ο οποίος θα έδινε την δυνατότητα για την παράσταση των γραμμάτων όλων των γλωσσών .

Έτσι σχηματίστηκε ο κώδικας UNICODE στον όποιο χρησιμοποιούνται 16 bit για την παράσταση των χαρακτήρων οπότε μπορούν να παρασταθούν 65.536 διαφορετικοί χαρακτήρες .

Με το κώδικα αυτό είναι δυνατόν να παρασταθούν οι χαρακτήρες που χρησιμοποιούνται σε όλα τα αλφάβητα του κόσμου –Λατινικό, Ελληνικό, Εβραϊκό, Κυριλλικό και Αραβικό και άλλα – ακόμη και τα ιδεογράμματα που χρησιμοποιούνται στην Κορεάτικη, Κινέζικη και την Ιαπωνική γλώσσα. Το πρότυπο UNICODE περιλαμβάνει ακόμη διάφορα διακριτικά σύμβολα, βέλη ,σημεία στίξης κ.α . Δίνει επίσης την δυνατότητα να παρασταθούν τονούμενα γράμματα.

- **ΧΡΗΣΗ UNICODE**

Λειτουργικά συστήματα

Παρά τα τεχνικά προβλήματα, τους περιορισμούς και την κριτική στη πορεία, το Unicode έχει επικρατήσει ως το κυρίαρχο σχήμα κωδικοποίησης χαρακτήρων. Ξεκινώντας από τα Windows NT και σε όλες τις μεταγενέστερες εκδόσεις των Windows γίνεται εκτεταμένη χρήση του σχήματος κωδικοποίησης UTF-16 για εσωτερική αναπαράσταση κειμένου. UNIX λειτουργικά συστήματα όπως GNU/Linux, Plan 9 από BellLabs, BSD και Mac OS X έχουν υιοθετήσει το σχήμα UTF-8, ως τη βάση για την αναπαράσταση πολυγλωσσικού κειμένου.

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	NUL 0000	STX 0001	SOT 0002	ETX 0003	EOT 0004	ENQ 0005	ACK 0006	BEL 0007	BS 0008	HT 0009	LF 000A	VT 000B	FF 000C	CR 000D	SO 000E	SI 000F
10	DLE 0010	DC1 0011	DC2 0012	DC3 0013	DC4 0014	NAK 0015	SYN 0016	ETB 0017	CAN 0018	EM 0019	SUB 001A	ESC 001B	FS 001C	GS 001D	RS 001E	US 001F
20	SP 0020	! 0021	" 0022	# 0023	$ 0024	% 0025	& 0026	' 0027	(0028	) 0029	* 002A	+ 002B	, 002C	− 002D	. 002E	/ 002F
30	0 0030	1 0031	2 0032	3 0033	4 0034	5 0035	6 0036	7 0037	8 0038	9 0039	: 003A	; 003B	< 003C	= 003D	> 003E	? 003F
40	@ 0040	A 0041	B 0042	C 0043	D 0044	E 0045	F 0046	G 0047	H 0048	I 0049	J 004A	K 004B	L 004C	M 004D	N 004E	O 004F
50	P 0050	Q 0051	R 0052	S 0053	T 0054	U 0055	V 0056	W 0057	X 0058	Y 0059	Z 005A	[005B	\ 005C	] 005D	^ 005E	_ 005F
60	` 0060	a 0061	b 0062	c 0063	d 0064	e 0065	f 0066	g 0067	h 0068	i 0069	j 006A	k 006B	l 006C	m 006D	n 006E	o 006F
70	p 0070	q 0071	r 0072	s 0073	t 0074	u 0075	v 0076	w 0077	x 0078	y 0079	z 007A	{ 007B	| 007C	} 007D	~ 007E	DEL 007F
80	Ç 00C7	ü 00FC	é 00E9	â 00E2	ä 00E4	à 00E0	å 00E5	ç 00E7	ê 00EA	ë 00EB	è 00E8	ï 00EF	î 00EE	ì 00EC	Ä 00C4	Å 00C5
90	É 00C9	æ 00E6	Æ 00C6	ô 00F4	ö 00F6	ò 00F2	û 00FB	ù 00F9	ÿ 00FF	Ö 00D6	Ü 00DC	ø 00F8	£ 00A3	Ø 00D8	× 00D7	ƒ 0192
A0	á 00E1	í 00ED	ó 00F3	ú 00FA	ñ 00F1	Ñ 00D1	ª 00AA	º 00BA	¿ 00BF	® 00AE	¬ 00AC	½ 00BD	¼ 00BC	¡ 00A1	« 00AB	» 00BB
B0	░ 2591	▒ 2592	▓ 2593	| 2502	┤ 2524	Á 00C1	Â 00C2	À 00C0	© 00A9	╣ 2563	║ 2551	╗ 2557	╝ 255D	¢ 00A2	¥ 00A5	┐ 2510
C0	└ 2514	┴ 2534	┬ 252C	├ 251C	─ 2500	┼ 253C	ã 00E3	Ã 00C3	╚ 255A	╔ 2554	╩ 2569	╦ 2566	╠ 2560	═ 2550	╬ 256C	¤ 00A4
D0	ð 00F0	Ð 00D0	Ê 00CA	Ë 00CB	È 00C8	ı 0131	Í 00CD	Î 00CE	Ï 00CF	┘ 2518	┌ 250C	▉ 2588	▄ 2584	¦ 00A6	Ì 00CC	▀ 2580
E0	Ó 00D3	ß 00DF	Ô 00D4	Ò 00D2	õ 00F5	Õ 00D5	µ 00B5	þ 00FE	Þ 00DE	Ú 00DA	Û 00DB	Ù 00D9	ý 00FD	Ý 00DD	¯ 00AF	´ 00B4
F0	00AD	± 00B1	‗ 2017	¾ 00BE	¶ 00B6	§ 00A7	÷ 00F7	¸ 00B8	° 00B0	¨ 00A8	· 00B7	¹ 00B9	³ 00B3	² 00B2	■ 25A0	NBSP 00A0

Εικόνα 14. Ο κώδικας Unicode

Ηλεκτρονική αλληλογραφία

Το πρότυπο MIME (Multipurpose Internet Mail Extensions) ορίζει δύο διαφορετικούς μηχανισμούς για κωδικοποίηση όχι-ASCII χαρακτήρων στα μηνύματα ηλεκτρονικής αλληλογραφίας, e-mails, ανάλογα με το αν οι χαρακτήρες είναι στις επικεφαλίδες του μηνύματος όπως πχ η επικεφαλίδα "Θέμα:" ή βρίσκονται στο κύριος κείμενο του ηλεκτρονικού μηνύματος. Και στις δυο περιπτώσεις, προσδιορίζεται το αρχικό σύνολο χαρακτήρων καθώς και η κωδικοποίηση μεταφοράς. Για ηλεκτρονική αλληλογραφία με Unicode χαρακτήρες προτείνονται το σχήμα κωδικοποίησης UTF-8 και η κωδικοποίηση μεταφοράς Base64. Οι λεπτομέρειες των δύο

μηχανισμών καθορίζονται στο πρότυπο MIME και γενικά είναι κρυμμένοι από τον απλό χρήστη λογισμικού ηλεκτρονικής αλληλογραφίας.

Η υιοθέτηση του Unicode στην Ηλεκτρονική αλληλογραφία είναι πολύ αργή. Τα περισσότερα κείμενα στην ανατολική Ασία κωδικοποιούνται ακόμα σε τοπικές κωδικοποιήσεις όπως η Shift-JIS, και πολλά δημοφιλή προγράμματα ηλεκτρονικής αλληλογραφίας ακόμα και αν έχουν κάποια unicode υποστήριξη εντούτοις δεν μπορούν να χειριστούν Unicode δεδομένα σωστά. Η κατάσταση αυτή δεν προβλέπεται να αλλάξει στο προσεχές μέλλον.

Διαδίκτυο

Οι καινούργιοι πλοηγοί διαδικτύου μπορούν και απεικονίζουν σωστά ιστοσελίδες με Unicode χαρακτήρες εφόσον έχει εγκατασταθεί η ανάλογη γραμματοσειρά.

Παρόλο που συντακτικοί κανόνες μπορεί να επηρεάζουν τη σειρά με την οποία οι χαρακτήρες επιτρέπεται να εμφανίζονται και η γλώσσα HTML 4.0 αλλά και η XML 1.0 εξ ορισμού υποστηρίζουν έγγραφα που αποτελούνται από χαρακτήρες από όλο το εύρος των κωδικών σημείων του Unicode εξαιρουμένων μόνο κάποιων χαρακτήρων ελέγχου τα μόνιμα μη-διαθέσιμα κώδικα σημεία D800-DFFF, οποιοδήποτε κωδικό σημείο που τελειώνει σε FFFE ή FFFF και οποιοδήποτε κωδικό σημείο πάνω από 10FFFF. Αυτοί οι χαρακτήρες παρουσιάζονται είτε απευθείας ως μπάιτς σύμφωνα με την κωδικοποίηση του εγγράφου, εφόσον υποστηρίζονται από την κωδικοποίηση μπορούν να γραφτούν ως αριθμητικές αναφορές χαρακτήρων βασισμένες στο κωδικό σημείο του Unicode χαρακτήρα, εφόσον η κωδικοποίηση που χρησιμοποιεί το έγγραφο επιτρέπει τα ψηφία και τα σύμβολα που χρειάζονται για να γράψουμε τις αναφορές (κάτι που συμβαίνει με όλες τις κωδικοποιήσεις που έχουν υιοθετηθεί στο διαδίκτυο) Για παράδειγμα οι αναφορές : Δ Й קম あ叶葉넟 (ή η ίδια τιμή στο δεκαεξαδικό με πρόθεμα &#x) εμφανίζεται στον πλοηγό ως Δ, Й, ק, م, ম, あ, 叶, 葉 και εφόσον έχεις την κατάλληλη γραμματοσειρά, αυτά τα σύμβολα φαίνονται σαν Greekcapitalletter "Delta", Cyrilliccapitalletter "Short I", Arabicletter "Meem", Hebrewletter "Qof", Thainumeral 7, JapaneseHiragana "A", simplifiedChinese "Leaf", traditionalChinese "Leaf", andKoreanHangulsyllable "Nyaelh", αντίστοιχα.

Γραμματοσειρές

Ελεύθερες και εμπορεύσιμες γραμματοσειρές που βασίζονται στο Unicode πρότυπο είναι κοινές, με πρώτες τις TrueType και τώρα τις OpenType γραμματοσειρές που υποστηρίζουν και οι δύο Unicode απεικονίζοντας κωδικά σημεία σε συγκεκριμένες εμφανίσεις χαρακτήρων.

Υπάρχουν χιλιάδες γραμματοσειρές στην αγορά, αλλά λιγότερες από δώδεκα προσπαθούν να υποστηρίξουν την πλειοψηφία του συνόλου χαρακτήρων του προτύπου Unicode. Αντίθετα οι βασισμένες στο Unicode γραμματοσειρές συνήθως υποστηρίζουν μόνο βασικό ASCII και κάποια συγκεκριμένα αλφάβητα. Αυτό γίνεται κυρίως για λόγους οικονομίας των δημιουργών γραμματοσειρών και απόδοσης των προγραμμάτων που μπορεί να γονατίσουν καθώς η απόδοση γραμματοσειρών είναι μια διαδικασία που καταναλώνει πολλούς πόρους ενός υπολογιστή

2.1.5. Ραβδωτός κωδικός

Ο ραβδωτός κωδικός αναπαριστά πληροφορίες οι οποίες αναγνωρίζονται από μηχανές και βρίσκεται αναγραμμένος σε μια επιφάνεια ενός προϊόντος. Ο στόχος του ραβδωτού κωδικού είναι να προσδιορίζει συγκεκριμένα προϊόντα ενός ανθρώπου η μιας τοποθεσίας. Ο πιο συνηθισμένος ραβδωτός κωδικός είναι ο EAN ο οποίος αποτελείται από 13 ψηφία. Γενικότερα υπάρχουν 250 είδη ραβδωτών κωδικών .

Οι πληροφορίες που εμφανίζονται στο γραμμωτό κωδικό είναι μορφοποιημένες σε μια μικρή εικόνα με γραμμές και διαστήματα. Όμως, στην πραγματικότητα ο ένας ραβδωτός κωδικός είναι δυαδικός. Είναι μια αλληλουχία από 0 και 1, και η αλληλουχία αυτή δημιουργεί ένα κείμενο το οποίο μεταφράζεται σε πολλές γλώσσες.

Για να αναγνωριστούν οι ραβδωτοί κωδικοί είναι απαραίτητη η χρήση οπτικών σαρωτών καθώς και διάφοροι τύποι τεχνολογίας. Οι πιο συνηθισμένες είναι τα λέιζερ και οι κάμερες.

ΒΗΜΑΤΑ ΓΙΑ ΑΝΑΓΝΩΡΣΗ

1. Ο σαρωτής μεταφράζει τον κωδικό σε γλώσσες Η/Υ
2. Οι σαρωτές αποκωδικοποιούν την μεταβλητή ανάκληση και την μετατρέπουν σε αριθμούς και γράμματα (ταυτίζεται ως πρώτο περιεχόμενο τους με χαρακτήρες που κωδικοποίησαν τον κώδικα)

Εικόνα 15. Παράδειγμα Barcode

2.1.6. Κώδικας Quikresponse

Ο κώδικας QR είναι ένας γραμμωτός κωδικός (barcode) δύο διαστάσεων, που δημιουργήθηκε από την ιαπωνική εταιρεία Denso-Wave το 1994. Το "QR" προέρχεται από τα αρχικά των λέξεων "Quick Response" (Γρήγορη Ανταπόκριση), γιατί οι δημιουργοί του είχαν ως κύριο σκοπό τα δεδομένα, που περιέχονται στον κώδικα, να αποκωδικοποιούνται με μεγάλη ταχύτητα. Ο Κώδικας QR είναι πολύ διαδεδομένος στην Ιαπωνία, όπου αποτελεί το πιο δημοφιλές είδος κώδικα δύο διαστάσεων.

ΣΚΟΠΟΣ: Τα δεδομένα ,που προέρχονται από το κώδικα ,να αποκωδικοποιούνται ταχύτατα .
ΑΠΟΤΕΛΕΙΤΑΙ: Από μαύρες ενότητες πάνω σε ένα τετράγωνο μοτίβο σε λευκό φόντο .
ΠΕΡΙΕΧΕΙ: Πληροφορίες στην κάθετη και στην οριζόντια κατεύθυνση .Επίσης ,το barcode περιέχει δεδομένα σε οριζόντια κατεύθυνση . Συνεπώς QR περιέχει περισσότερο όγκο από το barcode .
ΧΡΗΣΗ :Χρησιμοποιείται σε ένα ευρύτερο πλαίσιο, σε εμπορικές εφαρμογές .
ΠΑΡΑΔΕΙΓΜΑ :

Εικόνα 16. Παράδειγμα χρήσης

Μέσα σε ένα κώδικα QR μπορεί να αποθηκευτεί, π.χ., ένας σύνδεσμος προς μια ιστοσελίδα. Ο χρήστης σαρώνει με το κινητό του τηλέφωνο τον κώδικα QR και πλοηγείται αυτόματα στην ιστοσελίδα. Αυτή η πράξη της σύνδεσης από το φυσικό κόσμο είναι γνωστή ως hardlink ή υπερσύνδεση με φυσικό κόσμο. Οι χρήστες μπορούν, επίσης, να δημιουργήσουν και να εκτυπώσουν τους δικούς τους κώδικες QR με χρήση διάφορων ελεύθερων λογισμικών παραγωγής κώδικα QR που υπάρχουν στο δίκτυο. Μέσα μπορούν να αποθηκεύσουν όποιο μήνυμα θέλουν.

2.1.7. Μαγνητικές κάρτες

Οι μαγνητικές κάρτες ενσωματώνουν μαγνητική ταινία στην πίσω όψη τους, η οποία περιέχει τρία μαγνητικά κανάλια (track) στα οποία μπορούμε να αποθηκεύσουμε πληροφορίες του κατόχου της. Οι μαγνητικές ταινίες χωρίζονται σε αρκετούς τύπους μαγνήτισης, LOCO, MECO, HICO, αλλά πρακτικά οι δύο μόνο χρησιμοποιούνται.

Χαμηλής μαγνήτισης LOCO (Low coercivity 300oe)

Αυτές τις χρησιμοποιούμε όταν χρειαζόμαστε συχνή επανεγγραφή της κάρτας και η χρήση της προορίζεται για μικρό χρονικό διάστημα.

Υψηλής μαγνήτισης HICO (High coercivity 2750oe)

Αυτές τις χρησιμοποιούμε όταν χρειαζόμαστε ισχυρό μαγνητισμό της κάρτας και η χρήση τους προορίζεται για μεγάλο χρονικό διάστημα γιατί απομαγνητίζονται δύσκολα.

Τα πλεονεκτήματα από την χρήση μαγνητικών καρτών είναι πολλά. Ορισμένα από αυτά είναι η ελαχιστοποίηση της χρήσης φυσικού χαρτιού σε χρηματικές συναλλαγές και η αυτοματοποίηση διαφόρων συναλλαγών

2.1.8. Ασφάλεια ηλεκτρονικών συναλλαγών

Είναι ο όρος που χρησιμοποίει για να αναφερθεί κάποιος σε ένα διαδικτυακό τόπο μέσου του οποίου πραγματοποιούνται πωλήσεις. Για όλες τις υπηρεσίες οι χρήστες πρέπει να δημιουργήσουν ένα προσωπικό προφίλ χρήστη και στην συνέχεια τους δίνεται η δυνατότητα πρόσβασης της υπηρεσίας

Σήμερα οι δύο τύποι αξιόπιστων τεχνολογιών που είναι διαθέσιμα για ηλεκτρονικές αγορές είναι το SSL (Secure Socket Layer) & το SET (Secure Electronic Transaction). Η τεχνολογία set αναπτύχθηκε για την εξακρίβωση ταυτότητας μεταξύ εμπόρων και καταναλωτών. Παρέχει εμπιστευτικότητα των πληροφοριών αλλά και πιστοποίηση ότι ο έμπορος μπορεί να δεχτεί συναλλαγές με πιστωτική κάρτα. Το set δημιουργήθηκε από την visa και την mastercard .

2.1.9. 3D –SECURE

Το 3d-secure βασίζεται σε xml και χρησιμοποιείται ως ένα επίπεδο ασφάλειας για online συναλλαγές με πιστωτικές κάρτες για την εξακρίβωση της νόμιμης κατοχής τους.

Ήταν αρχικά αναπτυγμένο από το Arcotsystem και αναπτύχθηκε από τη visa με τη πρόθεση να βελτιωθεί η ασφάλεια των πληρωμών στο Ίντερνετ. Υπηρεσίες βασισμένες στο πρωτόκολλο έχουν επίσης υιοθετεί από τη mastercard και από την ICB. Η American express πρόσθεσε το 3D – SECURE στις 8 Νοεμβρίου του 2010 σε επιλεγμένες αγορές καθώς συνεχίζει να προσθέτει επιπλέον αγορές. Η ανάλυση του πρωτόκολλου έχει δείξει ότι έχει πολλά θέματα ασφάλειας που αφορούν τους πελάτες, συμπεριλαμβανομένων προβλημάτων phising (ηλεκτρονικό ψάρεμα - υποκλοπή ταυτότητας) και μετατόπιση της ευθύνης σε περίπτωση δόλιων ή ύποπτων πληρωμών.

Δημιουργήθηκε από την visa για την βελτίωση της ασφάλειας των πληρωμών στο διαδίκτυο. Το 3d secure δεν πρέπει να συγχέεται με τον κωδικό ασφάλειας της κάρτας ο οποίος είναι ένας μικρός αριθμητικός κώδικας τυπωμένος πάνω σε κάρτα.

ΚΕΦ. 3ο: Κρυπτογραφία και Ηλεκτρονικοί Υπολογιστές

3.1. Βασικές έννοιες

3.1.1 Ορισμός κρυπτογραφίας

Με τον όρο κρυπτογραφία, αναφερόμαστε στη μελέτη μαθηματικών τεχνικών που στοχεύουν στην εξασφάλιση θεμάτων που άπτονται της ασφάλειας μετάδοσης πληροφοριών. Αρχικά, η Κρυπτογραφία αποτέλεσε την τεχνική της απόκρυψης του περιεχομένου ενός μηνύματος, από μη εξουσιοδοτημένες οντότητες. Στις μέρες μας η Κρυπτογραφία έχει αναχθεί σε επιστήμη, με τις εφαρμογές τις διαρκώς να πληθαίνουν.

Στη διεθνή βιβλιογραφία προτείνονται διάφοροι ορισμοί της κρυπτογραφίας. Ο πιο διαδεδομένος αναφέρεται στο πρόβλημα της μυστικής επικοινωνίας:

3.1.2 Στόχοι κρυπτογραφίας

Η κρυπτογραφία εξαιτίας της περίτεχνης μορφής της χαρακτηρίζεται από πληθώρα στόχων οι οποίοι επικεντρώνονται κυρίως στην αυθεντικότητα των εμπλεκόμενων ατόμων αλλά και στην άμεση και συγχρόνως πλήρης παράδοση των στοιχείων. Αναλυτικότερα:

- κύριο «μέλημα» της είναι η παράδοση των κρυπτογραφημένων πληροφοριών στους σωστούς / επιλεγμένους παραλήπτες
- στοχεύει στη φραγή παρεμβολής τρίτων προσώπων, δηλαδή επιδιώκει την άμεση και πλήρη παράδοση των στοιχείων χωρίς να έχουν υποστεί κάποια μορφή αλλοίωσης
- εξαιρετικά σημαντική είναι η πιστοποίηση της ταυτότητας του αποστολέα, δηλαδή του ατόμου που στέλνει τις προαναφερόμενες πληροφορίες

Για να πετύχει, όμως, τους προαναφερόμενους σκοπούς βασίζεται σε κάποιες περαιτέρω λειτουργίες οι οποίες είναι:

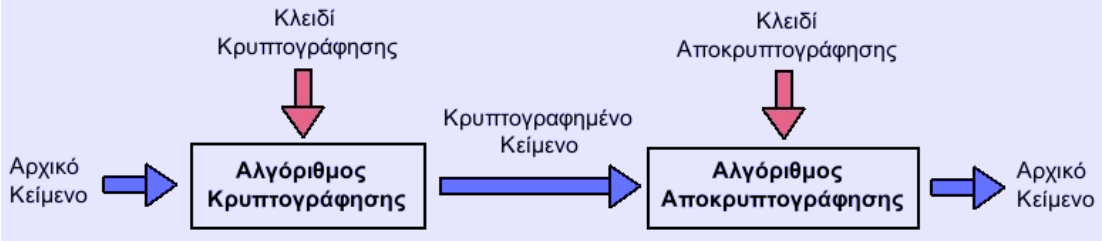
- **εμπιστευτικότητα**, δηλαδή η πληροφορία είναι προσβάσιμη μόνο από εξουσιοδοτημένα μέλη
- **ακεραιότητα**, δηλαδή η πληροφορία μπορεί να αλλοιωθεί από εξουσιοδοτημένα μέλη όπου η αλλοίωση καταγράφεται από το αρχείο
- **μη απάρνηση**, δηλαδή ο αποστολέας δεν μπορεί να απαρνηθεί την αυθεντικότητα της

- **πιστοποίηση**, δηλαδή ο παραλήπτης μπορεί να εξακριβώσει την ταυτότητα του αποστολέα καθώς και την πηγή της πληροφορίας

Κάποια άλλα θέματα που συναρτώνται με την ασφάλεια είναι

- **εξουσιοδότηση**: αφορά την εκχώρηση δικαιωμάτων από τον ιδιοκτήτη στον χρήστη
- **εξασφάλιση**: αναφέρεται στην αίσθηση εμπιστοσύνης ότι κάποιος αντικειμενικός σκοπός ή απαίτηση επιτυγχάνεται
- **μη αποποίηση ευθύνης**: σύμφωνα με τον όρο αυτό, κανένα από τα συναλλασσόμενα μέρη δεν πρέπει να έχει τη δυνατότητα να αρνηθεί τη συμμετοχή του σε μια συναλλαγή

Η παρακάτω εικόνα είναι μια απλουστευμένη ανάλυση του κρυπτογραφικού συστήματος το οποίο δημιούργει τον αλγόριθμο κρυπτογράφησης και αποκρυπτογράφησης με τη βοήθεια των αντίστοιχων κλειδιών.



Εικόνα 17. Σύστημα κρυπτογράφησης και αποκρυπτογράφησης

3.1.3 Τομείς εφαρμογών κρυπτογραφίας

Η κρυπτογραφία δεν αποτελεί μόνο αναπόσπαστο κομμάτι της εθνικής άμυνας όπως είναι εύκολα κατανοητό, αλλά κομμάτι της καθημερινής μας ζωής που επεκτείνεται σχεδόν σε όλους τους τομείς της καθημερινότητας μας, όπως αυτοί παρατίθενται κατηγοριοποιημένοι παρακάτω:

- **οικονομικός**
  - ασφάλεια συναλλαγών σε τραπεζικά δίκτυα-ATM
  - ηλεκτρονική δημοπρασία
  - ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες,πληρωμές)
  - έξυπνες κάρτες

- **κοινωνικός**
  - κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ)
  - σταθερή τηλεφωνία (cryptophones)
  - ηλεκτρονικό χρηματοκιβώτιο
  - World Wide Web
  - ιδιωτικά δίκτυα
  - δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
  - ασύρματα δίκτυα (bluetooth)
  - τηλεδιάσκεψη-τηλεφωνία μέσω διαδικτύου (VOIP)

- **επαγγελματικός**
  - διασφάλιση εταιρικών πληροφοριών
  - σύστημα ιατρικών δεδομένων και άλλων βάσεων δεδομένων

- **ασφάλειας**
  - εθνικής
    - στρατιωτικά δίκτυα (τακτικά συστήματα επικοινωνιών μάχης)
    - διπλωματικά δίκτυα (τηλεγραφήματα)
  - περιουσίας
    - συστήματα συναγερμών

3.1.4 Βασικοί όροι σύγχρονης κρυπτογραφίας

1. **Αλγόριθμος κρυπτογράφησης (encryption):** μετατρέπει τα δεδομένα σε μη αναγνώσιμη μορφή αποσκοπώντας στη διασφάλιση της εμπιστευτικότητας των δεδομένων, προσφέρει ψηφιακό ισοδύναμο σφραγισμένου φακέλου
2. **Αλγόριθμος αποκρυπτογράφησης (decryption):** αντιστρέφει τη διαδικασία της κρυπτογράφησης μετατρέποντας τα κρυπτογραφημένα δεδομένα στην αρχική τους μορφή
3. **Κρυπτογραφικό κλειδί:** χρησιμοποιώντας ένα κλειδί, η σύγχρονη κρυπτογραφία, η οποία παραλληλίζεται με μια συμβολοσειρά η οποία μπορεί να χρησιμοποιηθεί εξίσου για την

κρυπτογράφηση όσο και για την αποκρυπτογράφηση, καθώς επίσης και για τη δημιουργία ή επαλήθευση ψηφιακής υπογραφής. Τέτοιου είδους κλειδιά χρησιμοποιούνται από συμμετρικούς ή μη συμμετρικούς (δημόσιου κλειδιού) κρυπτογραφικούς αλγορίθμους.

4. **Οικονομολογική κρυπτογραφία:** είναι η κρυπτογραφία που εμπλέκεται σε εφαρμογές οι οποίες συσχετίζονται με πιθανή οικονομική απώλεια εξαιτίας της υπονόμευσης στο σύστημα μηνυμάτων.

3.1.5: Διαδομένοι Τρόποι Κρυπτογράφησης και κοινοτυπίες

1. Alice and Bob

Τα ονόματα Alice and Bob αποτελούν μια συνήθη επιλογή ψευδωνύμων, η χρήση των οποίων είναι συμβολική καθώς συχνά ταυτίζεται το όνομα με την ιδιότητα. Όμοια, τα ονόματα:

- *Zoe:*Z: αποτελεί το εικοστό-έκτο και τελευταίο γράμμα της λατινικής αλφάβητου και συμβολίζει το τελικό πρόσωπο σε μια υπόθεση
- *Walter:* είναι αγγλικό λογοπαίγνιο το οποίο είναι ηχητικά παρεμφερή με τη λέξη warden που σημαίνει δεσμοφύλακας/αρχιφύλακας

2. **SSH (εναλλακτικά SecureShell):** είναι ένα ασφαλές πρωτόκολλο δικτύου μέσω του οποίου επιτυγχάνεται η μεταφορά πληροφοριών ανάμεσα στους δύο υπολογιστές διασφαλίζοντας διάφορες μεταφορές αρχείων.

3. **Greeklish:** αποκαλείται μια σύγχρονη μορφή γραφής η οποία χρησιμοποιεί το ελληνικό αλφάβητο γραμμένο με λατινικούς χαρακτήρες. Χρησιμοποιείται από την νεολαία τόσο για την αποφυγή σπατάλης χρόνου (καθώς δεν υφίστανται γραμματικοί και συντακτικοί κανόνες) αλλά και ως ένα είδος ημικρυπτογράφησης πληροφοριών που δεν είναι εύκολα κατανοητή από τους ενήλικες .Παρόμοια μορφή ιδεολογίας ασπάζεται και η στάση κατά την οποία ελληνικοί χαρακτήρες απεικονίζουν αγγλικές λέξεις. Δυστυχώς, όμως, αυτές οι μορφές κρυπτογράφησης αλλοιώνουν την ιδιοσυγκρασία της κάθε γλώσσας προκαλώντας μια λεξιλογικού τύπου σύγχυση και ασάφειες.

3.2. Κρυπτοσυστήματα

3.2.1 Ορισμός και ανάλυση κρυπτοσυστημάτων

Κρυπτοσύστημα είναι το σύνολο των διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης.

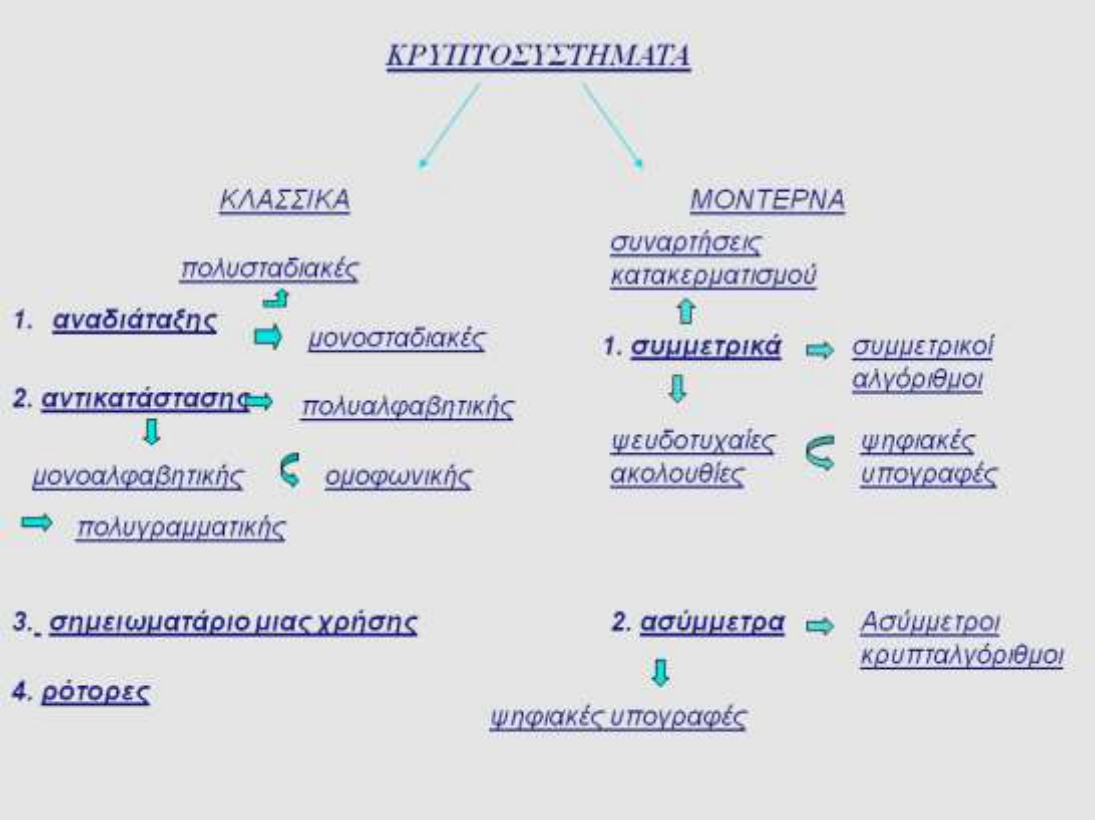
Τα κρυπτοσυστήματα χωρίζονται σε δύο κύριες κατηγορίες οι οποίες στη συνέχεια διαχωρίζονται σε υποκατηγορίες με βάση τη λειτουργία τους. Συγκεκριμένα, η πρώτη ομάδα χωρίζεται σε τέσσερις μικρότερες υποενότητες , δηλαδή σε συστήματα:

- **Αναδιάταξης -** τα οποία απαρτίζονται από τις πολυσταδιακές και τις μονοσταδιακές αναδιατάξεις
- **Αντικατάστασης -** που στη συνέχεια διαιρούνται σε τέσσερις μικρότερες κατηγορίες, στης:
  - αλφαβητικής αντικατάστασης
  - πολυαλφαβητικής αντικατάστασης
  - πολυγραμματικής αντικατάστασης
  - ομοφωνικής αντικατάστασης
- **Σημειωματάριο μιας χρήσης**
- **Ρότορες**

Ενώ η δεύτερη κατηγορία αποτελείται από δυο μεγάλες υποκατηγορίες:

- **τα συμμετρικά κρυπτοσυστήματα** που αποτελούνται από**:**
  - τους συμμετρικούς αλγορίθμους
  - τις ψευδοτυχαίες ακολουθίες
  - τις συναρτήσεις καταμερισμού
  - τις ψηφιακές υπογραφές
- **τα ασύμμετρα συστήματα**στα οποία κατατάσσονται:
  - οι ασύμμετροι αλγόριθμοι
  - οι ψηφιακές υπογραφές

Παρακάτω παρατίθεται ένα σχήμα για την καλύτερη κατανόηση των προαναφερόμενων υποσυστημάτων:



Εικόνα 18. Πίνακας κρυπτοσυστημάτων

3.2.2 Συμμετρικά και ασύμμετρα κρυπτοσυστήματα (αλγόριθμοι)

Αλγόριθμοι βασισμένοι σε κλειδιά

Οι αλγόριθμοι κρυπτογράφησης χρησιμοποιούν ένα ή περισσότερα κλειδία

Κατηγορίες αλγορίθμων ως προς το είδος του κλειδιού:

1. *Αλγόριθμοι συμμετρικού κλειδιού*: χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την κρυπτογράφηση
2. *Αλγόριθμοι ασύμμετρου κλειδιού:* χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση. Το κλειδί κρυπτογράφησης δε μπορεί να εξαχθεί από το κλειδί αποκρυπτογράφησης.

➢ Συμμετρικό κρυπτοσύστημα

είναι το σύστημα εκείνο που κατά τη διαδικασία της αποκρυπτογράφησης χρησιμοποιεί ένα κοινό κλειδί. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στη μυστικότητα του κλειδιού, η ανταλλαγή του οποίου γίνεται μέσα από ένα κανάλι επικοινωνίας ή μέσα από τη φυσική παρουσία των προσώπων (χαρακτηριστικό που καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων).

Συμμετρική κρυπτογράφηση και αλγόριθμοι

Στους συμμετρικούς αλγορίθμους το κλειδί κρυπτογράφησης μπορεί να υπολογιστεί από το κλειδί που χρησιμοποείται για την αποκρυπτογράφηση και το ανττίστροφο. Η ασφάλεια των αλγορίθμων βασίζεται στη μυστικότητα αυτού του κλειδιού. Για όσο καιρό και το κλειδί πρεπεί να παραμένει μυστικό.

Κρυπτογράφηση συμμετρικού κλειδιού

Ένα πρόβλημα που υπάρχει στους αλγορίθμους κρυπτογράφησης είναι η αδυναμία ανταλλαγής του κλειδιού με κάποιο ασφαλή τρόπο. Στη σύγχρονη ψηφιακή εποχή, ο αποστολέας και ο παραλήπτης του μηνύματος πολλές φορές δε γνωρίζονται, οπότε για τη μετάδοση του κλειδιού από τον έναν στον άλλον θα πρέπει να υπάρχει κάποιο ασφαλές κανάλι επικοινωνίας. Το διαδίκτυο δεν μπορεί να αποτελέσει τέτοιου είδους κανάλι, οπότε η χρήση της συμμετρικής κρυπτογράφησης σε εφαρμογές ηλεκτρονικού εμπορίου δεν υφίστανται.

Το βασικό πλεονέκτημα των αλγορίθμων συμμετρικού κλειδιού είναι ότι η διαδικασία της κρυπτογράφησης και απροκρυπτογράφησης είναι αρκετά γρήγορη και δεν καταναλώνει σημαντική υπολογιστική ισχύ.

1.Μηχανισμοί ασφαλείας

- Και τα δυο συναλλασσόμενα μέρη θα πρέπει να συμφωνήσουν για ένα κοινό μυστικό κλειδί και να εξασφαλισθεί η ασφαλής μετάδοση του
- Κάθε χρήστης θα πρέπει να έχει τόσα μυστικά όσα και τα μέλη με τα οποία συναλλάσσεται
- Δεν ικανοποιείται η απαίτηση για αυθεντικότητα, γιατί δεν μπορεί να αποδειχθεί η ταυτότητα των συναλλασσόμενων μελών. Από τη στιγμή που περισσότερα από ένα άτομα κατέχουν το κλειδί μπορούν εύκολα να κρυπτογραφήσουν το μήνυμα και να ισχυριστούν ότι το άλλο άτομο το έκανα. Συνεπώς, η μη αποποίηση της ευθύνης για την αποστολή ενός μηνύματος, καθίσταται και αύτη αδύνατη.

2. Παραδείγματα αλγορίθμων ιδιωτικού κλειδιού

- **Data Encryption Standard (DES) & Triple DES**:

1. Ο DES είναι κλειδί το οποίο είχε κάποτε προταθεί από την Αμερικάνικη κυβέρνηση, αλλά μετά από μια εικοσαετία περίπου επιτεύχθηκε η αποκρυπτογράφηση του από μια μηχανή και έκτοτε έχει «σπαστεί» πολλές φορές.
2. Το TripleDES είναι μια συνοπτική περιγραφή τριών DES στη σειρά στην οποία η αρχή του αποτελεί το πέρας του προηγούμενο DES (είσοδος-έξοδος)

- **Πρωτόκολλο SSL**

Το πρωτόκολλο SSL αναπτύχθηκε από την εταιρεία Netscape και δημιουργήθηκε προκειμένου να προστατεύει τη μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο . Η νέα έκδοση του πρωτοκόλλου κυκλοφόρησε από τη Netscape και αποτέλεσε τη βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου JLS , το οποίο πρόκειται να αντικαταστήσει το SSL. Τα δυο αυτά πρωτόκολλα χρησιμοποιούνται για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω διαδικτύου .

Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δυο συσκευών , θεσπίζοντας ,μια ασφαλή σύνδεση μεταξύ τους μέσω διαδικτύου . Το πρωτόκολλο αυτό είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης . Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου .

Τρόπος λειτουργίας

Το πρωτόκολλο SSL χρησιμοποιεί έναν συνδυασμό της κρυπτογράφησης δημοσίου και συμμετρικού κλειδιού. Η κρυπτογράφηση του συμμετρικού κλειδιού είναι πολύ πιο γρήγορη και αποδοτική σε σχέση με την κρυπτογράφηση του δημοσίου κλειδιού .

Παρόλα αυτά όμως η δεύτερη προσφέρει καλύτερες τεχνικές πιστοποίησης . Κάθε σύνδεση SSL ξεκινά πάντα με την ανταλλαγή μηνυμάτων από τον server και τον client έως ότου επιτευχθεί η ασφαλής σύνδεση , πράγμα που ονομάζεται χειραψία (handshake) .

Η χειραψία επιτρέπει στον server να αποδείξει την ταυτότητα του στον client χρησιμοποιώντας τεχνικές κρυπτογράφησης δημοσίου κλειδιού και στην συνέχεια επιτρέπει στον client και στον server να συνεργαστούν για την δημιουργία ενός συμμετρικού κλειδιού που θα χρησιμοποιηθεί στην γρήγορη κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που

ανταλλάσσονται μεταξύ τους. Προαιρετικά η χειραψία επιτρέπει στον client να αποδείξει την ταυτότητα στον server. Αναλυτικότερα η διαδικασία χειραψίας έχει ως εξής :

1. Αρχικά ο client στέλνει στον server την έκδοση του SSL που χρησιμοποιεί τον επιθυμητό αλγόριθμο κρυπτογράφησης, μερικά δεδομένα που έχουν παραχθεί τυχαία και οποιαδήποτε άλλη πληροφορία χρειάζεται ο server για να ξεκινήσει μια σύνδεση SSL .
2. Ο server απαντά στέλνοντας παρόμοιες πληροφορίες με προηγουμένως συμπεριλαμβανομένου όμως και του ψηφιακού πιστοποιητικού του , το οποίο τον πιστοποιεί στον client . Προαιρετικά μπορεί να ζητήσει και το ψηφιακό πιστοποιητικό του client .
3. Ο client λαμβάνει το ψηφιακό πιστοποιητικό του server και το χρησιμοποιεί για να τον πιστοποιήσει. Εάν η πιστοποίηση αυτή δεν καταστεί δυνατή , τότε ο χρήστης ενημερώνεται με ένα μήνυμα σφάλματος και η σύνδεση SSL ακυρώνεται . Εάν η πιστοποίηση του server γίνει χωρίς προβλήματα , τότε η διαδικασία της χειραψίας συνεχίζεται στο επόμενο βήμα .
4. Ο client συνεργάζεται με τον server και αποφασίζουν στον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιηθεί στην ασφαλή σύνδεση SSL. Επίσης ο client δημιουργεί το συμμετρικό κλειδί που θα χρησιμοποιηθεί στον αλγόριθμο κρυπτογράφησης και το στέλνει στο server κρυπτογραφημένο , χρησιμοποιώντας την τεχνική κρυπτογράφησης δημοσίου κλειδιού . Δηλαδή χρησιμοποιεί το δημόσιο κλειδί του server που αναγράφεται πάνω στο ψηφιακό του πιστοποιητικό για να κρυπτογραφήσει το συμμετρικό κλειδί και να του το στείλει . Στη συνέχεια ο server χρησιμοποιώντας το ιδιωτικό του κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα και να αποκτήσει το συμμετρικό κλειδί που θα χρησιμοποιηθεί για τη σύνδεση .
5. Ο client στέλνει ένα μήνυμα στον server ενημερώνοντας τον ότι είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση .
6. Ο server στέλνει ένα μήνυμα στον client ενημερώνοντας τον ότι και αυτός είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση

➢ Ασυμμετρικό κρυπτοσύστημα:

Ανακαλύφθηκε για να καλύψει τις αδυναμίες των συμμετρικών κρυπτοσυστημάτων άρα είναι μια νεότερη μορφή. Κύριο χαρακτηριστικό είναι η ύπαρξη δύο κλειδιών: ενός δημοσίου που είναι διαθέσιμο σε όλους και ένα ιδιωτικό το οποίο είναι μυστικό, τα οποία έχουν ακριβώς την ίδια αντίστροφη δράση καθώς ότι κρυπτογραφεί το ένα το αποκρυπτογραφεί το άλλο

RSA: Ο RSA αποτελεί ένα αλγόριθμο ασύμμετρου κλειδιού, μέσω της χρήσης του οποίου έχουμε τη δυνατότητα να κωδικοποιήσουμε μηνύματα όπως και να χρησιμοποιούμε τον ίδιο τον RSA ως μια ψηφιακή υπογραφή. Βασισμένο στη δύσκολη παραγοντοποίηση μεγάλων αριθμών, χρησιμοποιεί δύο κλειδιά: ένα δημόσιο κατά την κρυπτογράφηση και ένα ιδιωτικό κατά την αποκρυπτογράφηση.

3.3. Ψηφιακή Υπογραφή

Η ψηφιακή υπογραφή χρησιμοποιεί την κρυπτογραφία δημόσιου κλειδιού κατά την οποία ο χρήστης διαθέτει 2 κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Αναλυτικότερα το ένα κλειδί αξιοποιείται για την δημιουργία της ενώ το δεύτερο αντίστοιχα για την επαλήθευση της. Αναπτύσσει την αντιστρόφως ανάλογη σκέψη από αυτή της κρυπτογράφησης. Για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί ενώ για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα αντίστοιχα.

Αποτελείται από τρεις (3) αλγόριθμους.

1. **Δημιουργίας δημόσιου και ιδιωτικού κλειδιού**.

   Χρησιμοποιεί μια γεννήτρια τυχαίων αριθμών και με βάση αυτόν τον τυχαίο αριθμό δημιουργεί το δημόσιο αλλά και το ιδιωτικό κλειδί (από τα οποία, με το πρώτο δημιουργείται η ψηφιακή υπογραφή ενώ με το δεύτερο ελέγχεται η εγκυρότητά της.

2. **Προσθήκης ψηφιακής υπογραφής σε μηνύματα και έγγραφα.**

   Χρησιμοποιώντας το μήνυμα/έγγραφο κ το ιδιωτικό κλειδί (το οποίο ανήκει αποκλειστικά στον αποστολέα) , δημιουργεί την ψηφιακή υπογραφή.

3. **Ελέγχου ψηφιακής υπογραφής μηνύματος ή εγγράφου.**

   Χρησιμοποιείται το μήνυμα/έγγραφο αλλά αυτή τη φορά το δημόσιοι κλειδί (το οποίο είναι διαθέσιμο σε όλους) ελέγχει την αυθεντικότητά αλλά και την ακεραιότητα (ότι το μήνυμα δεν αλλοιώθηκε) του μηνύματος/εγγράφου

Παραδείγματα και χρήση ψηφιακής υπογραφής

Ο διευθυντής του σχολείου (υποχρεωτικά) αλλά και οι εκπαιδευτικοί (προαιρετικά) έχουν την δυνατότητα μέσα από τις υπηρεσίες του πανελλήνιου σχολικού δικτύου (ΠΣΔ)* να αποκτήσουν τη λεγόμενη ψηφιακή υπογραφή απαραίτητη προϋπόθεση για την οποία είναι ο διευθυντής ή οι

εκπαιδευτικοί αντίστοιχα να έχουν λογαριασμό στον αντίστοιχο φορέα που τους πιστοποιεί για την ιδιότητα τους ως εκπαιδευτικοί.

Η ψηφιακή υπογραφή, λοιπόν, χρησιμοποιείται και στα πλαίσια του σχολικού περιβάλλοντος. Χαρακτηριστικό παράδειγμα χρήσης της είναι η αξιοποίησης της κατά την υποβολή της απογραφής του ηλεκτρονικού εξοπλισμού της σχολικής μονάδας ώστε να πιστοποιηθεί η εγκυρότητα της αναφοράς που στάλθηκε από τον Διευθυντή του σχολείου στο Υπουργείο Παιδείας.

Συνοψίζοντας, η ψηφιακή υπογραφή αποτελεί μέρος συναλλαγών διάφορων φορέων μεταξύ τους κυρίως για την εγκυρότητα και την πιστοποίηση τους.

**Πανελλήνιο Σχολικό Δίκτυο: είναι ο πάροχος υπηρεσιών σύνδεσης με το διαδίκτυο για όλες τις σχολικές μονάδες , εκπαιδευτικούς αλλά και όλα τα εκπαιδευτικά ιδρύματα.*

3.4. Το σύστημα μετάδοσης των θεμάτων στις πανελλαδικές εξετάσεις …

Οι πανελλαδικές εξετάσεις είναι ένα σύστημα αξιολόγησης χιλιάδων μαθητών της Γ’ τάξης του Λυκείου σε όλη την Ελλάδα κάθε χρόνο που αφορά στην πρόσβαση τους στην τριτοβάθμια εκπαίδευση. Γι’ αυτό η αλλοίωση ή παραποίηση πληροφοριών ή θεμάτων είναι ανεπίτρεπτη. Στα πλαίσια του μαθήματος της ερευνητικής μας εργασίας με θέμα την «κρυπτογραφία» και κατόπιν υποδείξεως της καθηγήτριας μας, ζητήσαμε τη βοήθεια του διευθυντή του σχολείου μας, ώστε να ενημερωθούμε για το προαναφερόμενο σύστημα.

Το 1999, η εκπαιδευτική μεταρρύθμιση δημιούργησε την επιτακτική ανάγκη για ένα πανελλαδικά αδιάβλητο σύστημα εξέτασης των μαθητών στις σχολικές τους μονάδες. Το Υπουργείο Παιδείας, για την κάλυψη των καινούργιων αναγκών, αλλά και για την καλύτερη και άμεση ενημέρωση των περιφερειακών Διευθύνσεων Εκπαίδευσης, των Γραφείων, καθώς και των Σχολικών μονάδων, υιοθέτησε μια νέα μέθοδο μετάδοσης δεδομένων που είναι γνωστή ως "Μετάδοση VBI".

Η μέθοδος αυτή βασίζεται στο τηλεοπτικό σήμα και συγκεκριμένα στο μέρος του που ονομάζεται "Vertical Blanking Interval", δηλαδή κατακόρυφο διάστημα αμαύρωσης.

Η μετάδοση αυτού του τύπου είναι μονόδρομη από ένα σημείο προς πολλά (pointtomultipoint) με αρκετά υψηλή ταχύτητα και μηδενικό κόστος.

Το ΥΠΕΠΘ βελτίωσε το σύστημα αυτό προσθέτοντάς του Ενημέρωση Λήψης (Ffeedback) και το ολοκλήρωσε μετατρέποντάς το έτσι από σύστημα Εκπομπής (Broadcasting) σε υβριδικό - αλληλοδραστικό, ώστε να έχει πλέον την δυνατότητα αμφίδρομης επικοινωνίας.

Πως όμως πραγματοποιείται στην πραγματικότητα όλη η διαδικασία από το σχολείο; Οι υπεύθυνοι του συστήματος VBI πραγματοποιούν συντονισμένες δοκιμές της λειτουργίας του με το Υπουργείο αρκετές μέρες νωρίτερα από τη διεξαγωγή των εξετάσεων ώστε να πιστοποιηθεί η ακεραιότητα και σωστή λειτουργία του. Δύο καθηγητές ορίζονται χειριστές του συστήματος ένας από τους οποίους πρέπει υποχρεωτικά να είναι καθηγητής πληροφορικής ενώ για τον άλλον δεν αναφέρεται κάποιος περιορισμός. (απαραίτητη προϋπόθεση για την συμμέτοχη τους είναι να μην λαμβάνει μέρος κάποιος συγγενικό τους πρόσωπο στις πανελλαδικές εξετάσεις). Η διαδικασία αυτή επαναλαμβάνεται καθημερινά μέχρι το τέλος διεξαγωγής των εξετάσεων.

Το σύστημα με το οποίο είναι εξοπλισμένο το κάθε σχολείο – εξεταστικό κέντρο περιλαμβάνει: Ηλεκτρονικό υπολογιστή με εγκατεστημένο ειδικό λογισμικό λήψης και αποκωδικοποίησης, εκτυπωτή, αποκωδικοποιητή, μοναδικό κλειδί, δορυφορική κεραία λήψης καθώς και μόντεμ συνδεδεμένο με τηλεφωνική γραμμή για την περίπτωση που δεν λειτουργήσει το κύριο σύστημα μετάδοσης, για εναλλακτική λήψη.

Κατά την διάρκεια των εξετάσεων το σύστημα τίθεται σε λειτουργία αρκετές ώρες νωρίτερα από την ώρα έναρξης. Τα θέματα λαμβάνονται κρυπτογραφημένα και η αποκρυπτογράφηση τους γίνεται με ειδικό λογισμικό που έχει εγκατασταθεί λίγες μέρες νωρίτερα στον υπολογιστή που γίνεται η λήψη σε συνδυασμό με το κλειδί που έχει συνδεθεί στον ίδιο υπολογιστή. Μετά την λήψη σε καθορισμένη ώρα, των θεμάτων, την αποκρυπτογράφηση και τον έλεγχο της ορθής εκτύπωσης τα θέματα διανέμονται στους μαθητές και οι εξετάσεις ξεκινάνε.

Το σύστημα αυτό εξασφαλίζει την ακεραιότητα των δεδομένων και τη ‘δίκαιη’ διεξαγωγή των εξετάσεων.

ΚΕΦ. 4ο : Κρυπτογραφία και Τέχνη

4.1. Η Κρυπτογραφία στην Λογοτεχνία

Η κρυπτογραφία έχει συντελέσει σημαντικό ρόλο στην λογοτεχνία και γενικότερα στον χώρο τον τεχνών. Πολλοί συγγραφείς και σεναριογράφοι έχουν εμπνευστεί από την κρυπτογραφία και την έχουν συμπεριλάβει στα έργα τους. Πιο έντονα εμφανίζονται στα βιβλία μυστηρίου καθώς αυτή η μέθοδος ελκύει τους αναγνώστες σαν μια πρωτόγνωρη πρόκληση για αυτούς.

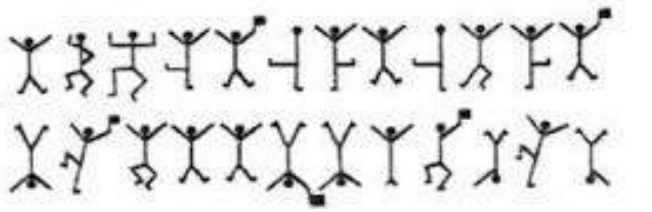
Συγκεκριμένα:

- **Dancing Men:**

Συγγεγραμμένο από τον ArthurConanDoyle, δημιουργού του πιο διάσημου ντετέκτιβ όλων των εποχών το βιβλίο «Η επιστροφή του Σέρλοκ Χόλμς» περιέχει μια πληθώρα αυτόνομων ιστοριών, μία εκ των οποίων είναι και η υπόθεση που τιτλοφορείται «DancingMen - οι Χορευτές» που εκδόθηκε το1903. Η ιστορία που διαδραματίζεται σε αυτή την υπόθεση έχει ως εξής:

Ο γαιοκτήμονας HiltonCubitt επισκέπτεται τον Σέρλοκ Χολμς και του δίνει ένα κομμάτι χαρτί με την εξής ακολουθία αριθμών - ραβδίων.

Οι μικροί άνδρες που χορεύουν βρίσκονται στην καρδιά ενός μυστηρίου πίσω από το οποίο φαίνεται να κρύβεται η νέα σύζυγος του HiltonCubitt,Elsie. Η νεαρή Elsie είναι Αμερικάνα, και πριν τον γάμο ζήτησε από τον σύζυγο της να μην ρωτήσει ποτέ για το παρελθόν της αν και του τόνισε ότι δεν υπήρχε τίποτα για το οποίο θα έπρεπε να ντρέπεται για αυτήν. Εκείνος σεβάστηκε την επιθυμία της αγαπημένης του.



Εικόνα 19. Dancing men

Το πρόβλημα εμφανίστηκε όταν η Elsie έλαβε μια επιστολή από τις Ηνωμένες Πολιτείες,από την οποία φρόντισε να απαλλαγεί, αφού την διάβασε, πετώντας την στην φωτιά. Τα σύμβολα άρχισαν να εμφανίζονται όλο και πιο συχνά, άλλοτε σε τοίχους και πόρτες σχεδιασμένα με κιμωλία, άλλοτε σε ένα χαρτί που είχε απομείνει στο ηλιακό ρολόι. Κάθε φορά η σύγχυση της ήταν εμφανής. Ο Cubitt απευθύνεται στον Holmes και εκείνος του ζητάει να συλλέξει όσο το

δυνατόν περισσότερα στοιχεία μπορεί. Η παρουσία των ανδρών που χορεύουν φτάνουν στα χέρια του Holmes και τότε ανακαλύπτει πως πρόκειται για κρυπτογράφημα. Έτσι, σπάει τον κωδικό με την ανάλυση συχνοτήτων. Το τελευταίο μήνυμα ήταν ιδιαίτερα ανησυχητικό.

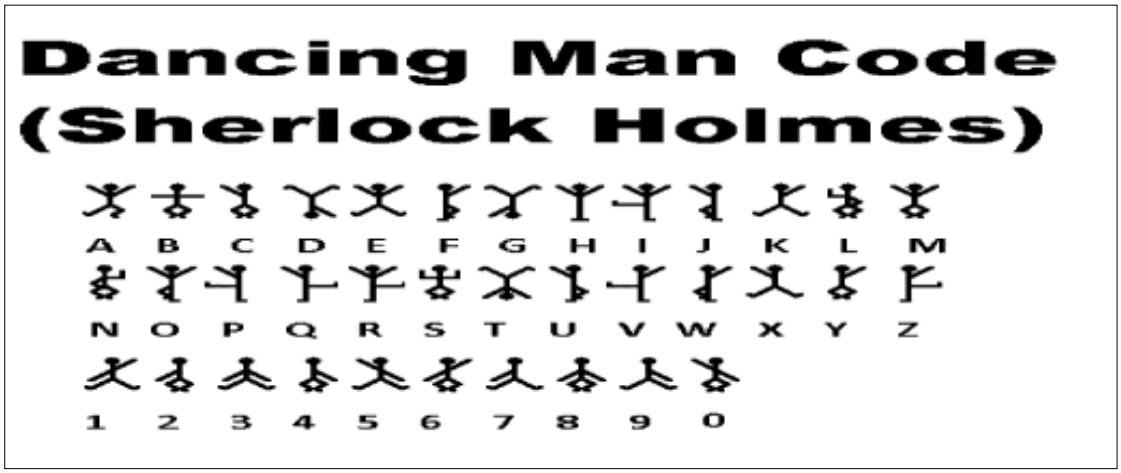
Ο Holmes πηγαίνει όσο πιο γρήγορα μπορεί στο Riddling Thorpe Manor και βρίσκει τον Cubitt νεκρό από σφαίρα στην καρδιά και την Elsie σοβαρά τραυματισμένη στο κεφάλι. Ο επιθεωρητής Martin πιστεύει ότι πρόκειται για δολοφονία-αυτοκτονία. Η Elsie είναι η κύρια ύποπτος για το θάνατο του άνδρα της. Ο Holmes, όμως, δεν το βλέπει έτσι. Γιατί υπάρχει μια τρύπα από σφαίρα στο περβάζι, δηλαδή συνολικά τρεις βολές, ενώ ο Cubbit και η σύζυγός του πυροβόλησαν μόνο μια φορά; Γιατί μόνο δύο θάλαμοι στο περίστροφο του Cubitt είναι άδειοι; Τι κάνει ένα μεγάλο ποσό χρημάτων μέσα στο δωμάτιο; Η ανακάλυψη ενός πατημένου παρτεριού που φαίνεται έξω από το παράθυρο, και ένα περίβλημα από κέλυφος επιβεβαιώνει τις υποψίες του Holmes - ένα τρίτο πρόσωπο είχε εμπλακεί, και είναι σίγουρα αυτός που έστελνε τα περίεργα μηνύματα με τους άνδρες που χορεύουν.

Ο Holmes γνωρίζοντας περισσότερα για την υπόθεση τα μεταφέρει στον Martin. Τυχαία διαλέγει το όνομα "Elrige" και ο βοηθός του Cubbit το αναγνωρίζει ως όνομα ενός αγρότη. Τότε ο Holmes γράφει ένα γράμμα χρησιμοποιώντας την μέθοδο των ανδρών που χορεύουν και στέλνει το αγόρι σε έναν ένοικο που ήταν εκεί, του οποίου το όνομα είχε επιλεχθεί πάλι τυχαία. Ο Holmes, βέβαια, ήξερε τα ονόματα τους, αφού είχε διαβάσει τον κώδικα τον ανδρών που χορεύουν. Αναμένοντας τα αποτελέσματα ο Holmes βρήκε την ευκαιρία να εξηγήσει στον Martin τον τρόπο με τον οποίο έσπασε των κώδικα των ανδρών που χορεύουν. Το τελευταίο μήνυμα, που οδήγησε τον Holmes στο τόπο του εγκλήματος, έλεγε "Elsie προετοιμάσου να γνωρίσεις τον Θεό σου".

Ο ένοικος κ. Abe Slaney, ένας άλλος Αμερικανός, ο οποίος αγνοεί ότι η Elsie είναι ετοιμοθάνατη και δεν μπορεί να επικοινωνήσει φτάνει στο Ridling Thorpe Manor λίγο αργότερα, προς μεγάλη έκπληξη όλων, εκτός του Holmes, ο οποίος είχε στείλει το μήνυμα μέσω των ανδρών που χορεύουν, θέλοντας να τον παγιδεύσει νομίζοντας πως το είχε στείλει η Elsie. Μόλις έρχεται λέει όλη την αλήθεια. Είναι πρώην εραστής από το Σικάγο και είχε έρθει στην Αγγλία για να ζητήσει από την Elsie να γυρίσει πίσω. Η Elsie απομακρύνθηκε από αυτόν επειδή ήταν εγκληματίας, όπως είχε ανακαλύψει ο Holmes μέσω των τηλεγραφικών ερευνών που είχε κάνει στις Η.Π.Α. Την συνάντησε κάποια στιγμή στο παράθυρο και η συνάντηση αυτή εξελίχθηκε βίαια με την εμφάνιση του Cubitt στο δωμάτιο. Ο Slaney έβγαλε το όπλο του και πυροβόλησε τον Cubitt, ο οποίος είχε ήδη πυροβολήσει προς το μέρος του. Ο Cubitt έπεσε νεκρός και ο Slaney τράπηκε σε φυγή. Προφανώς, η Elsie προσπάθησε να αυτοκτονήσει στην συνέχεια. Ο Slaney αναστατώθηκε πραγματικά όταν

πληροφορήθηκε ότι η Elsie προσπάθησε να αυτοκτονήσει. Η απειλητική φύση των μηνυμάτων "dancing men" εξηγείται από το γεγονός ότι ο Slaney έχασε την ψυχραιμία του στην πιθανή απροθυμία της Elsie να αφήσει τον άνδρα της. Τα χρήματα που βρέθηκαν στο δωμάτιο ήταν, προφανώς, η δωροδοκία του Slaney για να εξαφανιστεί από τις ζωές τους.

Ο αριθμός ραβδίων είναι ένας πολύ ακατέργαστος τύπος σχεδίου. Παριστάνεται με την χρήση ανθρώπινων μορφών ή και μορφών ζώων. Σε έναν αριθμό - ραβδί, το κεφάλι αντιπροσωπεύεται από τον κύκλο. Ο λαιμός, τα άκρα και ο κορμός σχηματίζεται από ενιαίες ευθείες γραμμές. Ο λαιμός και ο κορμός είναι διαφορετικά τμήματα μιας ευθείας γραμμής.



Εικόνα 20. Dancing men - Αντιστοιχία χορευτών και γραμμάτων

Οι αριθμοί ραβδίων είναι μια μορφή διανυσματικής τέχνης. Δημιουργούνται στους κινηματογράφους με τη βοήθεια του Macromedia. Η χρήση τους είναι συχνή καθώς είναι πολύ εύκολη η αναπαράστασή τους. Παρόλο που εμφανίζονται συχνά σε 2D περιβάλλον, ο τρισδιάστατος κόσμος προσπαθεί κάποιες φορές να τον μιμηθεί.

- **Ψηφιακό Οχυρό**

Το ψηφιακό οχυρό είναι ένα από τα καλύτερα και ρεαλιστικότερα τεχνολογικά θρίλερ που κυκλοφόρησε ποτέ. Γραμμένο από τον Dan Brown, τον πολυδιαβασμένο συγγραφέα παγκόσμια τα τελευταία χρόνια, θα κερδίσει κάθε είδους αναγνώστη με την πλοκή και την αιχμηρότητά του.

Η πλοκή: Η Εθνική Υπηρεσία Ασφάλειας των ΗΠΑ έχει στα χέρια της ένα υπερόπλο στο χώρο των επικοινωνιών: τον παντοδύναμο υπολογιστή TRANSLTR, ο οποίος παρακολουθεί όλο τον πλανήτη και μπορεί να αποκρυπτογραφήσει άμεσα οποιοδήποτε κωδικοποιημένο μήνυμα. Τα

προβλήματα ωστόσο ξεκινούν όταν ένας πρώην υπάλληλος της υπηρεσίας αντιτάσσεται στην πρακτική της να παρακολουθεί κάθε πολίτη και δημιουργεί έναν κώδικα απροσπέλαστο, ακόμη και από τον υπερυπολογιστή. Η Εθνική Υπηρεσία Ασφάλειας βρίσκεται σε ομηρία... Ο κώδικας έχει τέτοια δύναμη, που μπορεί να καταστρέψει όλο το δίκτυο αντικατασκοπίας. Τότε τη λύση καλείται να δώσει η γοητευτική Σούζαν Φλέτσερ, η ικανότερη κρυπτοναλύτρια που διαθέτει η υπηρεσία. Αυτό που ανακαλύπτει θα προκαλέσει τριγμούς σε όλη την ιεραρχία της εξουσίας και θα θέσει σε κίνδυνο ακόμη και την ζωή της. Αντιμέτωπη με δυνάμεις που την υπερβαίνουν, θα αγωνιστεί με μόνο όπλο το μυαλό της να σώσει τη χώρα από μια σκοτεινή συνωμοσία. (Εκδοτικός Οίκος Α. Α. ΛΙΒΑΝΗ ΑΘΗΝΑ 2005, Συγγραφέας DAN BROWN)

4.2. Η Κρυπτογραφία στον Κινηματογράφο

Δεν υπάρχει ανθρώπινη κοινωνία δίχως μυστικά, χωρίς συνωμοσίες ,πολέμους ή κρυφές ερωτικές σχέσεις. Η ιστορία των καλυμμένων μηνυμάτων και τη μυστικής γραφής έχει τις ρίζες της στους αρχαιότερους πολιτισμούς. Στο σύγχρονο κόσμο, τα πάντα γύρω μας είναι κρυπτογραφημένα. Εδώ και 4.000 χρόνια, οι κώδικες και τα κρυπτογράμματα παίζουν καθοριστικό ρόλο στην πολιτική, στον πόλεμο, στις δολοφονίες και στο έγκλημα. Το μυστικό και η δράση για την αποκάλυψή του κώδικα αιχμαλωτίζει τη φαντασία, και εξηγεί την εμφάνιση αποκρυπτογραφών σε κινηματογραφικές ταινίες. Όλοι μας έχουμε σίγουρα παρακολουθήσει κινηματογραφικές ταινίες ή τηλεοπτικές σειρές, όπου οι ήρωες επικοινωνούν μέσω κρυπτογραφημένων συνομιλιών.

4.2.1. Κώδικας DaVinci

Μία ταινία που χρησιμοποιούνται κρυπτογραφικά μηνύματα είναι και ο Κώδικας DaVinci. Όλη η υπόθεση του έργου εξελίσσεται αρχικά στο Παρίσι, όπου ένας φημισμένος καθηγητής, ειδικός των συμβόλων, καλείται ξαφνικά μία νύχτα στο Μουσείο του Λούβρου για να βοηθήσει με την εξιχνίαση του φόνου του εφόρου του Λούβρου. Ανακαλύπτει ότι μια μυστική οργάνωση εμπλέκεται στην δολοφονία του εφόρου. Υπό την απειλή της ιδίας του της ζωής και με τη βοήθεια μιας κρυπτολόγου, ο καθηγητής αποκαλύπτει μία σειρά από κρυμμένα στους πίνακες του Λεονάρντο ντα Βίντσι ίχνη που οδηγούν σε μία κλειστή κοινότητα αφοσιωμένη στην προστασία ενός μυστικού, κρυμμένο για 2000 χρόνια!

4.2.2. Μηχανή Enigma

Η μηχανή Αίνιγμα είναι μια μηχανή από μια οικογένεια συναφών ηλεκτρομηχανικών μηχανιών κρυπτογράφησης, η χρήση της οποίας είναι η κρυπτογράφηση και αποκρυπτογράφηση των μυστικών μηνυμάτων. Η εφεύρεση της τοποθετείται στα τέλη του Β΄ Παγκόσμιου Πολέμου από τον Γερμανό μηχανικό Arthur Scherbius. Τα πρώτα μοντέλα χρησιμοποιήθηκαν από τις αρχές της δεκαετίας του 1920 άλλα για εμπορικούς σκοπούς, άλλα από την κυβέρνηση και άλλα από στρατιωτικές υπηρεσίες άλλων χωρών – κυρίως από την ναζιστική Γερμανία πριν και κατά την διάρκεια του Παγκόσμιου Πολέμου. Στη συνέχεια δημιουργήθηκαν πολλά διαφορετικά μοντέλα της μηχανής αλλά τα Γερμανικά στρατιωτικά μοντέλα είναι τα πιο πολυσυζητημένα .

Τον Δεκέμβρη του 1932, το Πολωνικό Γραφείο Αποκρυπτογράφησης έσπασε πρώτο τους στρατιωτικούς αλγόριθμους κρυπτογράφησης Enigma της Γερμανίας. Πέντε εβδομάδες πριν από το ξέσπασμα του Β΄ Παγκόσμιου Πολέμου, στις 25 Ιουλίου του 1939, στη Βαρσοβία, που παρουσιάστηκαν στρατιωτική οι τεχνικές Enigma - αποκρυπτογράφησης και ο εξοπλισμός τους στη γαλλική και βρετανική στρατιωτική νοημοσύνη. Από το 1938 επιπλέον πολυπλοκότητα επανειλημμένα προσθέτονταν στις μηχανές καθιστώντας τις αρχικές τεχνικές αποκρυπτογράφησης μειωτικά επιτυχής. Παρ' όλα αυτά η πολωνική επανάσταση αποτέλεσε μια ζωτικής σημασίας βάση για την μετέπειτα βρετανική προσπάθεια. Κατά την διάρκεια του πολέμου οι Βρετανοί κρυπτογράφοι ήταν σε θέση να αποκρυπτογραφήσουν ένα τεράστιο αριθμό των μηνυμάτων που είχαν κρυπτογραφηθεί χρησιμοποιώντας το Enigma. Η νοημοσύνη που αποκτήθηκε από την πηγή αυτή με την κωδική ονομασία "Ultra" από τους Βρετανούς, ήταν μια σημαντική βοήθεια στην πολεμική προσπάθεια των Συμμάχων.

Εκτιμάτε πως η θέση της "Ultra" κατά την διάρκεια του πολέμου ήταν η αποκρυπτογράφηση των γερμανικών αλγόριθμων κρυπτογράφησης. Ο Winston Churchill υποστήριξε ότι χάρη στο Ultra νίκησαν τον πόλεμο.

➢ Alan Matheson Turing

Ο Άλαν Μάθισον Τούρινγκ γεννημένος στις 23 Ιουλίου του 1912 στο Πάντιγκτον του Λονδίνου ήταν Βρετανός μαθηματικός, καθηγητής της λογικής και κρυπτογράφος. Θεωρείται «πατέρας της επιστήμης υπολογιστών», χάρη στην πολύ μεγάλη συνεισφορά του στο γνωστικό πεδίο της θεωρίας υπολογισμού κατά τη δεκαετία του 1930, αλλά και της τεχνητής νοημοσύνης, χάρη στη λεγόμενη *δοκιμή Τούρινγκ* την οποία πρότεινε το 1950: έναν τρόπο να διαπιστωθεί πειραματικά αν μία μηχανή έχει αυθεντικές γνωστικές ικανότητες και μπορεί να σκεφτεί.

Η συνεισφορά του Τούρινγκ στον Β΄ Παγκόσμιο Πόλεμο δεν αναγνωρίστηκε λόγο του γεγονότος ότι η εργασία του ήταν απόρρητη. Υπήρξε κεντρικό πρόσωπο στο κέντρο της Βρετανικής Υπηρεσίας Αντικατασκοπείας καθώς ήταν προϊστάμενος στην ομάδα 8 , η όποια ασχολήθηκε με την αποκωδικοποίηση της γερμανικής κρυπτογραφικής συσκευής Enigma.

Εικόνα 21.

Άλαν Μάθισον Τούρινγκ

Παιδική ηλικία και εφηβεία

Ο Τούρινγκ γεννήθηκε το 1912 στο Πάντιγκον του Λονδίνου. Από πολύ νωρίς αναδείχθηκε η μεγαλοφυΐα του. Παρουσίαζε μεγάλη οικειότητα με τους αριθμούς και τους γρίφους. Έλυσε προηγμένα προβλήματα του 1927 χωρίς να έχει μελετήσει το στοιχειώδη λογισμικό. Το 1928, σε ηλικία δέκα έξι ετών μελέτησε την εργασία του Άλμπερτ Αϊνστάιν και όχι μόνο την κατάλαβε αλλά και προεξέτεινε τα ερωτήματα του για τους νόμους του Νεύτωνα, σε ένα κείμενο που δεν δημοσιεύτηκε.

Κρυπτογραφική ανάλυση

Κατά την διάρκεια του Β' Παγκοσμίου Πολέμου ο Τούρινγκ ήταν σημαντικός συμμετέχων στις προσπάθειες του Μπλέτσλει Πάρκ για να καταφέρουν να αποκρυπτογραφήσουν τα γερμανικά μηνύματα. Η εργασία του έμεινε μυστική μέχρι την δεκαετία του ’70. Για να επιτευχθεί αυτό έπρεπε να δουλεύει συγκεκριμένες ώρες της ημέρας, ώστε να μην κινεί υποψίες. Συνέλαβε διάφορες μαθηματικές ιδέες με την αποκρυπτογράφηση μηνυμάτων των συσκευών ENIGMA και Lorenz SZ 40/42. Το 1940 μετακινήθηκε στην Ομάδα 8 όπου συνεργάστηκε με τον Dilly Knox . Οι Πολωνοί παρείχαν στους Άγγλους και στους Γάλλους πληροφορίες για το πώς δούλευε η μηχανή Enigma αποκτώντας πλεονέκτημα λόγω της πιο προσεγγισμένης δουλειάς τους. Ο Τούρινγκ συνειδητοποίησε ότι δεν ήταν απαραίτητο να εξεταστούν όλοι οι πιθανοί συνδυασμοί για να σπάσουν τους κωδικούς της μηχανής Enigma. Απέδειξε ότι ήταν δυνατό να εξετάσει τις σωστές τοποθεσίες των διακοπτών χωρίς να πρέπει να εξεταστούν οι τοποθεσίες του πίνακα συνδέσεων .

Ακόμα επιτεύχθηκε η κατασκευή της ηλεκτρομηχανικής μηχανής βόμβας, κατασκευασμένη από τον Τούρινγκ και τον Gordon Welchman.

Ο κωδικός enigma που χρησιμοποιούσαν στο ναυτικό του γερμανικού στόλου ήταν πολύ περίπλοκος και δύσκολος. Γι' αυτό ο Τούρινγκ κατάφερε να εφεύρει μια νέα συσκευή με νέα τεχνική, ονόματι Banburismus, για να βοηθήσει στο σπάσιμο της γερμανικής κρυπτογραφικής συσκευής Enigma.

Η ιστορία της μηχανής

Υπάρχουν αρκετά μοντέλα και παραλλαγές της μηχανής Enigma. Οι πρώτες μηχανές ήταν εμπορικά μοντέλα που χρονολογούνται από τις αρχές της δεκαετίας του 1920. Στα μέσα της δεκαετίας αυτής, διάφοροι κλάδοι του γερμανικού στρατού χρησιμοποίησαν αυτή τη μηχανή κάνοντας κάποιες αλλαγές. Επίσης πολλά άλλα έθνη προσάρμοσαν το σχέδιο Enigma για τις δικές τους μηχανές κρυπτογράφησης.

Η εμπορική Enigma: Στις 23 φεβρουαρίου 1918, ο Γερμανός μηχανικός Arthur Scherbius έκανε αίτηση για δίπλωμα για ένα μηχάνημα με τη χρήση κρυπτογράφησης και ρότορων, και με τον Richard E.Ritter, ίδρυσε την εταιρία Scherbius & Ritter. Πλησίασαν το γερμανικό ναυτικό και Υπουργείο Εξωτερικών με το σχεδιασμό τους, αλλά κανένας από τους δύο δεν ήταν ενδιαφερόμενος. Θα αναθέσουν τότε τα δικαιώματα ευρεσιτεχνίας στον Gewerkschaft Securitas, ο οποίος ίδρυσε το Chiffriermaschinen Aktien-Gesellschaft στις 9 Ιουλίου του 1923! Ο Scherbius και ο Ritter ήταν στο διοικητκό συμβούλιο. Η Chiffriermaschinen AG άρχισε να διαφημίζει μια λιανικής μηχανή-μοντέλο Enigma A – η οποία παρουσιάστηκε στο συνέδριο της Διεθνούς Ταχυδρομικής Ένωσης το 1923-1924. Η μηχανή ήταν βαριά και ογκώδη, ενσωματώνοντας μια γραφομηχανή. Μέτρησε 65 x 45 x 35 εκατοστά και ζύγιζε περίπου 50 κιλά.

Το 1925 Enigma μοντέλο Β εισήχθη και ήταν μια παρόμοια κατασκευή αν και τα δύο μοντέλα Α και Β είχαν το ίδιο όνομα ήταν αρκετά διαφορετικές σε σχέση με νεότερες εκδόσεις. Διέφεραν σε φυσικό μέγεθος και σχήμα, αλλά και κρυπτογραφικά υπό έννοια ότι έλειπε ο ανακλαστήρας.

Ο ανακλαστήρας είναι μία ιδέα που προτάθηκε από τον συνάδελφο του Will Scherbius Korn εισήχθη για πρώτη φορά στο Enigma C (1926) μοντέλο. Ο ανακλαστήρας είναι ένα βασικό χαρακτηριστικό των μηχανών Enigma.

Η στρατιωτική Enigma: Το Πολεμικό Ναυτικό ήταν το πρώτο υποκατάστημα του γερμανικού στρατού που θα υιοθετήσει την μηχανή. Αυτή η εκδόση, που ονομάζεται Funkschussel C, είχε τεθεί σε παραγωγή απο το 1925 και τέθηκε σε λειτουργία το 1926. Το πληκτρολόγιο περιείχε 29 γράμματα, τα οποία ήταν με αλφαβητική σειρά. Οι ρότορες είχαν 28 επαφές, με το γράμμα X ενσύρματο για να παρακάμψει τα στροφεία. Από 15 Ιουλίου του 1928, ο γερμανικός στρατός είχε καθιερώσει τη δική τους εκδοχή του Enigma G, αναθεωρήθηκε στο Enigma I μέχρι τον Ιούλιο του 1930. Η Enigma I χρησιμοποιήθηκε από τις γερμανικές στρατιωτικές υπηρεσίες και άλλους κυβερνητικούς οργανισμούς κατά την διάρκεια του Α Παγκοσμίου Πολέμου. Από το 1930 , ο στρατός είχε προτείνει ότι το Πολεμικό Ναυτικό θα υιοθετούσε την μηχανή τους . Το Ναυτικό συμφώνησε και το 1934 θα τεινόταν σε λειτουργία η έκδοση του Ναυτικού Enigma . Ενώ ο στρατός χρησιμοποιούσε μόνο τρείς ρότορες εκείνη την στιγμή , για μεγαλύτερη ασφάλεια το Πολεμικό Ναυτικό ορίζεται μια επιλογή τριών από μια πιθανή πέντε.

Τον Δεκέμβριο του 1938 , ο στρατός εξέδωσε δύο επιπλέον ρότορες ,έτσι οι τρείς ρότορες επιλέχθηκαν από ένα σύνολο πέντε. Μέχρι το 1939 , το Πολεμικό Ναυτικό πρόσθεσε άλλους τρείς ρότορες . Το 1935 η Πολεμική Αεροπορία εισήγαγε την I Enigma για επικοινωνίες. Κατά την διάρκεια του Παγκοσμίου Πολέμου αυτές οι μηχανές χρησιμοποιούνται για να ελέγχουν και να αναφέρουν τις θέσεις των υποβρυχίων στον Ατλαντικό και να περάσουν πληροφορίες σχετικά με βομβαρδισμούς , την μετακίνηση των στρατιωτικών μονάδων ,καθώς και η θέση και το φορτίο των στρατιωτικών πλοίων εφοδιασμού.

Πριν την χρήση του μηχανήματος Enigma, οι Βρετανοί ήταν ένα βήμα μπροστά από τους Γερμανούς καθώς και το υποβρύχιο ναυάγιο ταχύτερα από ότι θα μπορούσε να είναι. Άλλες χώρες χρησιμοπούν μηχανές Enigma. Οι ισπανοί χρησιμοποιούν επίσης μια εμπορική Enigma κατά τον Εμφύλιο Πολεμό τους. Βρετανοί κρυπτογράφοι κατάφεραν να σπάσουν αυτές τις μηχανές, οι οποίες δεν είχαν plugboard.

Περιγραφή λειτουργίας της μηχανής

Ηλεκτρονικές διαδρομές

Τα μηχανικά μέρη ενεργούν κατά τέτοιο τρόπο ώστε να σχηματίζουν ένα μεταβαλλόμενο ηλεκρικό κύκλωμα. Όταν πατηθεί ένα πλήκτρο, ένα κύκλωμα ολοκληρώνεται με ρεύμα που ρέει μέσω των διαφόρων συστατικών με την παρούσα διαμόρφωσή τους και τελικά ανάβει μια από τις

λάμπες, υποδεικνύοντας την επιστολή εξόδου. Οι επνειλημμένες αλλαγές της ηλεκτρικής διαδρομής μέσα από ένα scrambler Enigma, υλοποίησε πολυαλφαβητικές κρυπτογραφήσεις αντικατάστασης που παρείχε υψηλή ασφάλεια από την Enigma.

Στροφείς

Οι ρότορες αποτέλεσαν τη καρδιά μιας μηχανής Enigma .Κάθε στροφείο ήταν ένας δίσκος περίπου 10 cm και ήταν κατασκευασμένα απο σληρό ελαστικό με ελατήριο ορειχάλκινων πείρων. Στην άλλη πλευρά υπάρχει ένας αντίστοιχος αριθμός κυκλικών ηλεκτρικών επαφών . Οι ακίδες και οι επαφές αντιπροσωπεύουν το αλφάβητο .Μέσα στο σώμα του ρότορα, 26 σύρματα συνέδεαν κάθε ακίδα από τη μία πλευρά σε μια επαφή από την άλλη.

Ένα στροφείο θα εκτελέσει ένα απλό τύπο αποκρυπτογράφησης . Η πολυπλοκότητα της Enigma, και κρυπτογραφική ασφάλεια , προήλθε απο την χρήση πολλών δρομέων σε σειρά και την τακτική κίνηση των στροφειών υλοποιώντας μια πολυαλφαβητική κρυπτογράφηση .

Με αφορμή την ιστορίοα της μηχανής Enigma ,γυρίστηκε και η ταινία "The Imitation Game" (Το Παιχνίδι της Μίμησης) βασισμένη στην βιογραφία Alan Turing: The Enigma του Άντριου Χότζες. Πρωταγωνιστεί ο Μπένεντικτ Κάμπερμπατς.

4.3. Κρυπτογραφούμε ένα μήνυμα

ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΜΕ FACEBOOKEMOTICONS (πίνακας αντιστοίχισης γραμμάτων**)**

ΓΡΑΜΜΑΤΑ	ΚΩΔΙΚΟΠΟΙΗΣΗ
Α	

Β	
Γ	
Δ	
Ε	
Ζ	
Η	
Θ	
Ι	
Κ	
Λ	
Μ	
Ν	
Ξ	
Ο	
Π	
Ρ	
Σ	
Τ	
Υ	

Φ	
Χ	
Ψ	
Ω	

Παράδειγμα: Κρυπτογράφηση της λέξης ΚΡΥΠΤΟΓΡΑΦΙΑ

Αποκρυπτογράφηση:	Κ	Ρ	Υ	Π	Τ	Ο	Γ	Ρ	Α	Φ	Ι	Α
Κρυπτογράφηση:												

3. Βιβλιογραφία – Πηγές :

Βιβλία:

- Εφαρμογές Πληροφορικής Α' Λυκείου
- Η Καινοτομία των Ερευνητικών Εργασιών στο Λύκειο (Ηλίας Γ. Ματσαγγούρας)
- Edmodo - Ασφαλές Κοινωνικό Δίκτυο Μάθησης για Εκπαιδευτικούς
  Οδηγός Διαχειριστή
  Συγγραφική ομάδα: Τσόκανος Γ.
  Επιμέλεια: Α. Καπανιάρης
  Α.Σ.ΠΑΙ.Τ.Ε., Γενικό Τμήμα Παιδαγωγικών Μαθημάτων, Παράρτημα Βόλου
  Creative Commons Attribution-NonCommercial 3.0 Ελλάδα

Ιστοσελίδες:

- http://www.samos.aegean.gr/math/stamatiu/crypto_samos/
- https://www.academia.edu
- www.edmodo.com
- https://www.edmodo.com/?language=el
- http://internet-safety.sch.gr/
- http://blogs.sch.gr/internet-safety
- users.sch.gr/johncyp/documents/vbi/leitourgia_VBI.doc
- http://utopia.duth.gr/~vkatos/documents/the_book/ch1.pdf
- http://el.wikipedia.org/wiki/Unicode
- http://mathhmagic.blogspot.gr/2012/06/blog-post.html
- http://rumkin.com/tools/cipher/morse.php
- http://en.wikipedia.org/wiki/Cryptography
- https://www.youtube.com/watch?v=Kf9KjCKmDcU
- https://www.youtube.com/watch?v=EfxcG6HTK28
- http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-CryptoTerminology.html
- https://e.edim.co/59092009/μαθηματικά_και_κρυπτογραφία.pdf
- https://e.edim.co/59092009/συμμετρική_κρυπτογραφία.pdf
- https://e.edim.co/59092009/simeioseis_kryptografia.pdf
- https://e.edim.co/59092009/γενική_επισκόπηση_κρυπτογραφίας.pdf

4. Παράρτημα

4.1. Η ορολογία της Κρυπτογραφίας

Algorithm - Αναφέρεται στον αλγόριθμο κρυπτογράφησης, που είναι μια μαθηματική διαδικασία (μέθοδος) κρυπτογράφησης (κωδικοποίησης) και αποκρυπτογράφησης (αποκωδικοποίησης) μηνυμάτων και κειμένων, τα οποία μετατρέπονται σε μια μη αναγνώσιμη μορφή.

Asymmetric Encryption – Αποδίδεται στα ελληνικά ως Ασύμμετρη Κρυπτογράφηση και είναι ένα σύγχρονο σύστημα κρυπτογράφησης, το οποίο με τη χρήση δύο κλειδιών (δημόσιο και ιδιωτικό) επιτυγχάνει σχεδόν απόλυτη προστασία των ευαίσθητων (απόρρητων) πληροφοριών (δεδομένων).

Authentication - Αποδίδεται στα ελληνικά με τον όρο Ταυτοποίηση ή Πιστοποίηση και είναι η διαδικασία ή μέθοδος επιβεβαίωσης (εξακρίβωσης) με τη χρήση ψηφιακών ταυτοτήτων ή πιστοποιητικών της ταυτότητας ενός ατόμου ώστε να έχει δικαίωμα για πρόσβαση σε διάφορα συστήματα.

Authorization - Αποδίδεται στα ελληνικά με τον όρο Εξουσιοδότηση και είναι η διαδικασία σύμφωνα με την οποία γίνεται ο απαραίτητος έλεγχος από την τράπεζα του πελάτη (πληρωτή) ως προς το υπόλοιπο του λογαριασμού του, έτσι ώστε να εγκριθεί η εισαγωγή του σ' ένα δίκτυο και να δοθεί η σχετική εντολή πληρωμής στην τράπεζα του αποδέκτη.

BackDoor - Αποδίδεται στα ελληνικά με τον όρο Πίσω Πόρτα ή και Κερκόπορτα και αναφέρεται σε ορισμένες αδυναμίες των λειτουργικών συστημάτων των υπολογιστών, τις οποίες μπορούν να εκμεταλλευτούν κάποιο επίδοξοι hackers ή crackers και να προκαλέσουν ζημιά ή απλά να καταγράφουν (παρακολουθούν) τις κινήσεις και τις επιλογές μας στο Internet ή και να υποκλέπτουν μυστικούς κωδικούς εν αγνοία μας.

Certification Authority (CA/TTP) - Αποδίδεται στα ελληνικά μ' έναν από τους όρους Οργανισμός Πιστοποίησης ή Έμπιστη Τρίτη Οντότητα ή και Πάροχος Υπηρεσιών Πιστοποίησης και αναφέρεται στους Οργανισμούς ή Εταιρείες που έχουν το δικαίωμα (άδεια) να εκδίδουν ψηφιακές ταυτότητες και να εγγυώνται μ' αυτόν τον τρόπο τη διασφάλιση (απόρρητο) των επικοινωνιών.

Cipher - Όρος που αναφέρεται στην κρυπτογράφηση (κωδικοποίηση) μηνυμάτων. Είναι συνώνυμος με τους όρους Encryption και Encode.

CipherText - Αποδίδεται στα ελληνικά με τον όρο Κρυπτογράφημα και είναι το κρυπτογραφημένο (κωδικοποιημένο) αρχείο, κείμενο ή μήνυμα που στέλνει ο αποστολέας στον παραλήπτη. Το αρχικό (αυθεντικό), δηλ. το μη κρυπτογραφημένο μήνυμα, αποκαλείται PlainText.

Code - Αποδίδεται στα ελληνικά με τον όρο Κώδικας και αναφέρεται στη χρήση χαρακτήρων ή λέξεων για την αναπαράσταση άλλων λέξεων ή προτάσεων. Κλασικό παράδειγμα αποτελεί ο Κώδικας Morse, όπου με τον κατάλληλο συνδυασμό από τελείες και παύλες μπορούμε να παραστήσουμε όλα τα γράμματα και τα ψηφία αλλά και μερικές τυποποιημένες προτάσεις.

Cracker - Χρήστης ο οποίος εισβάλει σε σύστημα στο οποίο δεν έχει νόμιμη πρόσβαση, με σκοπό να παραποιήσει ή ακόμη και να καταστρέψει δεδομένα και πληροφορίες ή και να δημιουργήσει παράνομα αντίγραφα νόμιμων προγραμμάτων.

Cryptography - Αποδίδεται στα ελληνικά με τον όρο Κρυπτογραφία και είναι η προστασία των ευαίσθητων (απόρρητων) πληροφοριών (δεδομένων) με την μετατροπή τους από την απλή μορφή κειμένου, που αποκαλείται plaintext, σε μια μη αναγνώσιμη μορφή, που αποκαλείται ciphertext. Το κρυπτογραφημένο μήνυμα μπορεί να αποκρυπτογραφηθεί (decrypted) μόνο από τον κάτοχο ενός απόρρητου αλγορίθμου (encryption algorithm), που αποκαλείται κλειδί ή κλείδα (key).

Cryptoanalysis - Αποδίδεται στα ελληνικά με τον όρο Κρυπτανάλυση και αναφέρεται στην τέχνη της παραβίασης, δηλ. της αποκρυπτογράφησης, των κρυπτοσυστημάτων. Μπορεί να αναφέρεται επίσης και στην εύρεση λαθών ή και ελλείψεων κατά την εφαρμογή ενός αλγορίθμου κρυπτογράφησης.

Cryptology - Αποδίδεται στα ελληνικά με τον όρο Κρυπτολογία και αναφέρεται στη μελέτη (έρευνα) της κρυπτογραφίας και της κρυπτανάλυσης.

Cryptosystem - Αποδίδεται στα ελληνικά με τον όρο Σύστημα Κρύπτο και αναφέρεται στην όλη διαδικασία χρησιμοποίησης της κρυπτογραφίας, δηλ. στις μεθόδους κρυπτογράφησης και αποκρυπτογράφησης καθώς και στις μεθόδους διαπίστωσης της ταυτότητας του αποστολέα ενός μηνύματος.

DataEnrcyption - Αποδίδεται στα ελληνικά με τον όρο Κρυπτογράφηση Δεδομένων και αναφέρεται στη χρήση μαθηματικών εργαλείων για την καθιέρωση της εμπιστοσύνης ανάμεσα στον αποστολέα και τον παραλήπτη (αποδέκτη) ενός μηνύματος. Η κύρια χρήση της κρυπτογραφίας είναι αυτή της κωδικοποίησης της πληροφορίας με τέτοιο τρόπο ώστε η αποκωδικοποίηση της να είναι δυνατή μόνο από τον τελικό αποδέκτη του μηνύματος. Για να γίνει αυτό ο τελικός αποδέκτης του μηνύματος αναγνωρίζεται από ένα ειδικό identifier, ευρύτερα γνωστό ως κλειδί αποκωδικοποίησης. Οι δύο σημαντικότερες μορφές (μέθοδοι) κρυπτογράφησης δεδομένων είναι η Συμμετρική Κρυπτογράφηση και η Κρυπτογράφηση Δημόσιου Κλειδιού, στην οποία ο κάθε χρήστης έχει τη δυνατότητα να δημιουργήσει ένα ζεύγος κλειδιών, δηλ. ένα γνωστό ή δημόσιο κλειδί (public key) και ένα κρυφό κλειδί (secret key) ή ιδιωτικό κλειδί (private key). Το δημόσιο κλειδί μπορεί να το δημοσιοποιήσει (κοινοποιήσει) σ' όλον τον κόσμο. Στη συμμετρική κρυπτογραφία, υπάρχει μόνο ένα κλειδί το οποίο χρησιμοποιείται τόσο για την κωδικοποίηση όσο και για αποκωδικοποίηση του μηνύματος, το οποίο κλειδί πρέπει να παραμένει κρυφό σ' όλους εκτός από τον αποστολέα και τον αποδέκτη του μηνύματος, πράγμα βέβαια δύσκολο σήμερα με τις εκπληκτικές δυνατότητες των hackers και των crackers. Η κρυπτογραφία με χρήση δημόσιου κλειδιού χρησιμοποιεί ένα πιο ευέλικτο και πιο ασφαλή σχήμα πιστοποίησης για την αποκωδικοποίηση των δεδομένων και ως εκ τούτου έχει επικρατήσει (με δημοφιλέστερες μορφές δεδομένων το PKI και το PGP).

Decryption - Αποδίδεται στα ελληνικά με τον όρο Αποκρυπτογράφηση και είναι η μέθοδος (διαδικασία) επαναφοράς ενός μηνύματος, που έχει κρυπτογραφηθεί σε μη αναγνώσιμη μορφή (ciphertext), στην κανονική ή αρχική του του μορφή (plaintext). Η αποκρυπτογράφηση μπορεί να γίνει μ' ένα απόρρητο ή μ' ένα δημόσιο (publickey) ή και μ' έναν κωδικό πρόσβασης (password).

DataEncryption Standard (DES) - Αποδίδεται στα ελληνικά με τον όρο Πρότυπο Κρυπτογράφησης Πληροφοριών και είναι ένας είδος κρυπτογράφησης που δημιουργήθηκε από την κυβέρνηση των ΗΠΑ τη δεκαετία του 1970 ως ο επίσημος αλγόριθμος κρυπτογράφησης σε χρήση στις ΗΠΑ. Αναπτύχθηκε από την IBM υπό την αιγίδα της κυβέρνησης των ΗΠΑ. Αναπτύχθηκαν ανησυχίες ότι ίσως υπάρχουν κρυμμένες παγίδες στη λογική του αλγορίθμου που θα επέτρεπαν στην κυβέρνηση να σπάσει τον κωδικό μιας οποιασδήποτε επικοινωνίας. Το DES χρησιμοποιεί ένα κλειδί των 56 bit για να κάνει μια σειρά από μη γραμμικούς μετασχηματισμούς σ' έναν μπλοκ δεδομένων των 64 bit. Όμως, σήμερα με την ολοένα αυξανόμενη ταχύτητα του hardware και το χαμηλό του κόστος, είναι εφικτό να κατασκευασθεί ένα μηχάνημα που αν μπορεί να σπάισε ένα κλειδί των 56 bit σε μία μόνο ημέρα. Γι' αυτόν τον λόγο, έχει αναπτυχθεί το τριπλό-DES ή 3DES, το οποίο χρησιμοποιεί το 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.

Digital ID/Certificate - Αποδίδεται στα ελληνικά με τον όρο Ψηφιακή Ταυτότητα ή Ψηφιακή Βεβαίωση ή και Ψηφιακό Πιστοποιητικό και πρόκειται για μια κρυπτογραφημένη ταυτότητα που την εκδίδουν ειδικά εξουσιοδοτημένοι Οργανισμοί Παροχής Υπηρεσιών Πιστοποίησης, με την οποία επιβεβαιώνεται η γνησιότητα των στοιχείων του κατόχου, το ότι αυτός που στέλνει το μήνυμα είναι όντως αυτός που ισχυρίζεται ότι είναι και ότι δεν γίνεται ηλεκτρονική απάτη ή πλαστοπροσωπία. Μπορεί να την χρησιμοποιήσει ο κάτοχός της για να κάνει ασφαλείς ηλεκτρονικές συναλλαγές και επικοινωνία μέσω του Internet. Η ψηφιακή ταυτότητα περιλαμβάνει την ψηφιακή υπογραφή του κατόχου της(digitalsignature) και το δημόσιο κλειδί του (publickey). Το πρότυπο που χρησιμοποιείται κυρίως στα ψηφιακά πιστοποιητικά είναι το X.509.

Digital Signature - Αποδίδεται στα ελληνικά με τον όρο Ψηφιακή Υπογραφή και πρόκειται για ειδικό αρχείο το οποίο δημιουργείται από κείμενο που το υπογράφει και το κρυπτογραφεί (κωδικοποιεί) ο κάτοχός του. Ο παραλήπτης του μηνύματος θα πρέπει να κάνει αποκρυπτογράφηση του κειμένου, σύγκριση της ψηφιακής υπογραφής και πιστοποίηση (επιβεβαίωση) της ταυτότητας του αποστολέα του μηνύματος. Με την ψηφιακή υπογραφή μπορεί να γίνει η ηλεκτρονική πιστοποίηση (επιβεβαίωση) στοιχείων, όπως είναι η ταυτότητα ενός χρήστη, η ικανότητα πληρωμής ή και η γνησιότητα ενός ηλεκτρονικού εγγράφου.

Encryption - Αποδίδεται στα ελληνικά με τον όρο Κρυπτογράφηση και είναι η μέθοδος (διαδικασία) μετατροπής κάποιων πληροφοριών (δεδομένων) σε απόρρητο (μη αναγνώσιμο) κώδικα, που είναι γνωστό και ως κρυπτογράφημα (ciphertext). Αποτελεί την αποτελεσματικότερη μέθοδο για την επίτευξη της ασφάλειας στις επικοινωνίες. Για την ανάγνωση ενός κρυπτογραφημένου αρχείου είναι απαραίτητη η κατοχή του απόρρητου (ιδιωτικού) κλειδιού ή του κωδικού πρόσβασης, με τα οποία μπορεί να γίνει η αποκρυπτογράφηση των δεδομένων. Τα μη κρυπτογραφημένα δεδομένα ονομάζονται plaintext, ενώ τα κρυπτογραφημένα δεδομένα ονομάζονται ciphertext. Υπάρχουν δύο είδη κρυπτογράφησης : η Ασύμμετρη Κρυπτογράφηση, που είναι γνωστή και ως Κρυπτογράφηση Δημόσιου Κλειδιού και η Συμμετρική Κρυπτογράφηση.

Encryption Algorithm - Είναι ένας αλγόριθμος (μαθηματική μέθοδος) κρυπτογράφησης δεδομένων, με τη βοήθεια του οποίου μπορούμε να μετατρέψουμε κανονικό κείμενο (πληροφορία)

σε μη αναγνώσιμη μορφή (ciphertext). Για την επαναφορά των δεδομένων στην αρχική τους μορφή απαιτείται η ύπαρξη ειδικού κλειδιού.

Firewall - Ειδικό Πρόγραμμα (λογισμικό) ή και υλικό (hardware) που έχει τη δυνατότητα να ελέγχει ή και να απαγορεύει την απομακρυσμένη πρόσβαση σ' έναν υπολογιστή ή και να περιορίζει τις διαθέσιμες ιστοσελίδες σ' έναν προσωπικό υπολογιστή ή και σ' ένα δίκτυο υπολογιστών. Το firewall κάνει έλεγχο στα εισερχόμενα και εξερχόμενα δεδομένα από και προς τον υπολογιστή ή το δίκτυο από τη μια μεριά και το Interneταπό την άλλη.

Hacker - Χρήστης ο οποίος εισβάλει σε σύστημα στο οποίο δεν έχει νόμιμη πρόσβαση, αλλά μόνο για πειραματισμό και ευχάριστη απασχόληση καθώς και για να εντοπίσει και να υποδείξει κενά στα συστήματα ασφαλείας των υπολογιστικών συστημάτων. Διακρίνονται από τους λεγόμενους Crackers, οι οποίοι προκαλούν ζημιές ή κάνουν μη νόμιμες ενέργειες.

HTTPS (SecureHypertextTransferProtocol) - Ασφαλές πρωτόκολλο για την ανταλλαγή κρυπτογραφημένων ιστοσελίδων ανάμεσα στον Webserver και τον φυλλομετρητή (browser). Οι δικτυακοί τόποι που υποστηρίζουν το συγκεκριμένο πρωτόκολλο, στο πεδίο διευθύνσεων του φυλλομετρητή εμφανίζεται το https:// αντί του γνωστού http:// και στη γραμμή κατάστασης το σύμβολο μιας κλειδαριάς. Το πρωτόκολλο αυτό παρέχει ασφαλή διαχείριση των προσωπικών δεδομένων των χρηστών και χρησιμοποιείται συνήθως σε online συναλλαγές ή σε αποστολή στοιχείων πιστωτικής κάρτας κ.ά. Πρόκειται στην ουσία για μια ασφαλή μορφή του γνωστού πρωτοκόλλου μεταφοράς υπερκειμένου HTTP, ώστε να είναι εξασφαλισμένη η ανταλλαγή πληροφοριών ανάμεσα στον φυλλομετρητή και τον Web server.

Key - Αποδίδεται στα ελληνικά με τον όρο Κλειδί ή και Κλείδα και είναι μια συλλογή από δυαδικά ψηφία που είναι αποθηκευμένα σ' ένα αρχείο που χρησιμοποιείται για την κρυπτογράφηφη ή αποκρυπτογράφηση ενός μηνύματος.

KeyEscrow - Σε γενικές γραμμές, η διαδικασία keyescrow σημαίνει ότι ένα αντίγραφο του μυστικού κλειδιού που είναι απαραίτητο στην αποκρυπτογράφηση αποθηκεύεται (φυλάσσεται) από κάποιον τρίτο, που μπορεί να είναι ένας συμβολαιογράφος ή μια τράπεζα, και οι οποίοι το κρατούν σε ασφάλεια σε περίπτωση απώλειας του κλειδιού ή θανάτου του κατόχου του. Η χρήση του είναι κοινή και στις επιχειρήσεις, όπως όταν ένας υπάλληλος κατέχει κρυπτογραφημένο υλικό στον υπολογιστή της εταιρείας του και σε περίπτωση που συμβεί κάτι με τον υπάλληλο ή με τον υπολογιστή, η εταιρεία δεν θα μπορέσει να αποκρυπτογραφήσει τα μηνύματα. Γι' αυτόν τον λόγο, ένα αντίγραφο του μυστικού κλειδιού φυλάσσεται από έναν ή περισσότερους προϊσταμένους. Για να υπάρχει η εξασφάλιση ότι ένας προϊστάμενος δεν θα κάνει κατάχρηση της θέσης του, το κλειδί μπορεί να διαχωριστεί και να μοιρασθεί σε πολλά άτομα, οι οποίοι θα πρέπει να συνεργασθούν για την ανάκτηση του κλειδιού.

KnownPlainTextAttack - Είναι μια μέθοδος επίθεσης σ' ένα σύστημα κρυπτογράφησης όπου ο κρυπταναλυτής κατέχει αντίγραφα του plaintext και του αντίστοιχου κρυπτογραφημένου κειμένου. Με τα ασθενέστερα συστήματα κρυπτογράφησης, η μέθοδος αυτή μπορεί να βελτιώσει τις πιθανότητες σπασίματος του κωδικού και απόκτησης του plaintext των άλλων μηνυμάτων όπου το plaintext δεν είναι γνωστό.

OneTimePad (OTP) - Το onetimepad είναι το μόνο σχήμα κρυπτογράφησης (encryptionscheme) που μπορεί να αποδειχθεί ότι είναι απολύτως απαραβίαστο. Χρησιμοποιείται πολύ από τους κατασκόπους καθώς δεν απαιτεί κάποιον μηχανισμό (hardware) για να υλοποιηθεί και λόγω της απόλυτης ασφάλειας που παρέχει. Αυτός ο αλγόριθμος απαιτεί τη δημιουργία πολλών συνόλων από keyspads, όπου το κάθε pad αποτελείται από έναν αριθμό από τυχαίους χαρακτήρες κλειδιών. Eachpartyinvolvedreceivesmatchingsetsofpads. Ο κάθε χαρακτήρας κλειδιού στο pad χρησιμοποιείται για να κρυπτογραφήσει έναν μόνο χαρακτήρα plaintext και μετά δεν χρησιμοποιείται ποτέ ξανά. Ο λόγος που δεν χρησιμοποιείται ευρέως αυτό το σχήμα κρυπτογράφησης είναι ότι λόγω της πολυπλοκότητάς του δεν είναι κατάλληλο για τα σύγχρονα συστήματα επικοινωνιών που έχουν μεγάλες απαιτήσεις σε ταχύτητα. Ένα από τα διασημότερα links επικοινωνίας που χρησιμοποιούν αυτό το σχήμα είναι η κόκκινη γραμμή Ουάσινγκτον - Μόσχας.

Passphrase - Αποδίδεται στα ελληνικά με τον όρο Συνθηματική Λέξη ή και Κωδική Φράση και είναι ουσιαστικά το ίδιο πράγμα με το Password με τη διαφορά ότι είναι πιο περίπλοκο και συνεπώς πιο δύσκολο να εντοπισθεί.

Password - Αποδίδεται στα ελληνικά με τον όρο Συνθηματικό ή και Κωδικός Πρόσβασης και είναι μια μοναδική και απόρρητη λέξη κλειδί με την οποία σε συνδυασμό με το όνομα χρήστη (username) μπορούμε να αποδείξουμε την ταυτότητά μας όταν εισερχόμαστε σε περιορισμένης πρόσβασης σελίδες ή εφαρμογές ή σε πύλες (portals) ή και αλλού. Αποτελεί καλή τακτική να αλλάζουμε συχνά το password μας και να μην χρησιμοποιούμε κωδικούς που να μπορεί εύκολα να τους μαντέψει κάποιος αλλά περίεργους συνδυασμούς από γράμματα, ψηφία και σύμβολα.

PGP (PrettyGoodPrivacy) - Αποτελεί ένα από τα πιο δημοφιλή προγράμματα που χρησιμοποιούνται για την κρυπτογράφηση μηνυμάτων και την αποστολή τους μέσω του Internet. Χρησιμοποιεί την κρυπτογράφηση με συνδυασμό δημόσιου και ιδιωτικού κλειδιού (publickey - privatekey). Θεωρείται απόλυτα ασφαλές. Το δημόσιο κλειδί είναι γνωστό σ' όλους και μπορούμε να το κατεβάσουμε (download) από κάποια ιστοσελίδα, ενώ το ιδιωτικό κλειδί είναι αυστηρά προσωπικό για τον κάθε χρήστη. Ότι κωδικοποιείται με το ένα κλειδί μπορεί να αποκωδικοποιηθεί με το άλλο και αντίστροφα. Όμως, είναι εξαιρετικά δύσκολη, αν όχι αδύνατη, η εύρεση του ιδιωτικού κλειδιού όταν γνωρίζουμε το δημόσιο κλειδί ενός χρήστη. Όταν ένα μήνυμα κωδικοποιείται με το ιδιωτικό κλειδί ενός χρήστη, μπορεί να αποκωδικοποιηθεί από οποιονδήποτε τρίτο με το γνωστό δημόσιο κλειδί του ίδιου χρήστη, αλλά αυτό αποτελεί μια επιβεβαίωση της ταυτότητας του χρήστη. Επίσης, η κωδικοποίηση ενός μηνύματος με το δημόσιο κλειδί ενός χρήστη εξασφαλίζει το ότι μόνο ο συγκεκριμένος χρήστης θα μπορέσει να το αποκωδικοποιήσει.

PlainText - Είναι το αυθεντικό (αρχικό) αρχείο, κείμενο ή μήνυμα, το οποίο πρέπει να λάβει κανονικά ο παραλήπτης. Το κρυπτογραφημένο μήνυμα που αποστέλνεται αποκαλείται CipherText (Κρυπτογράφημα).

PrivateKey - Αποδίδεται στα ελληνικά με τον όρο Ιδιωτικό Κλειδί και είναι το μυστικό (κρυφό) κλειδί ενός κρυπτογραφικού συστήματος. Μπορεί να το χρησιμοποιεί ο κάτοχός του για να υπογράφει ηλεκτρονικά τα εξερχόμενα μηνύματά του καθώς και για να αποκρυπτογραφεί τα εισερχόμενα μηνύματά του.

PublicKey - Αποδίδεται στα ελληνικά με τον όρο Δημόσιο Κλειδί και είναι το κοινό κλειδί ενός κρυπτογραφικού συστήματος. Μπορεί να το χρησιμοποιεί ένας οποιοσδήποτε τρίτος για να κρυπτογραφεί τα εξερχόμενα μηνύματά του προς τον κάτοχο του αντίστοιχου ιδιωτικού κλειδιού καθώς και για να αποκρυπτογραφεί τα εισερχόμενα μηνύματα που έχουν κωδικοποιηθεί με το ιδιωτικό κλειδί του αποστολέα.

PublicKeyEncryption - Αποδίδεται στα ελληνικά με τον όρο Κρυπτογράφηση με Δημόσιο Κλειδί και πρόκειται για ένα σύστημα (τεχνική) κρυπτογράφησης που χρησιμοποιεί έναν συνδυασμό από ένα δημόσιο και ένα ιδιωτικό κλειδί για την κρυπτογράφηση των μηνυμάτων. Με τον τρόπο αυτό αποφεύγουμε την αποστολή του κλειδιού από τον αποστολέα στον παραλήπτη, κάτι που είναι πολύ επικίνδυνο για υποκλοπή. Η τεχνική αυτή κρυπτογράφησης λειτουργεί μ' έναν εμπιστευτικό κωδικό του νόμιμου χρήστη, που είναι το γνωστό ιδιωτικό κλειδί (privatekey), και μ' έναν δημόσιο κωδικό, που είναι το γνωστό δημόσιο κλειδί (publickey), και το οποίο διανέμεται (δίνεται) ελεύθερα μέσω του Internet ή και ως συνημμένο σ' ένα e-mail. Οι δύο αυτοί κωδικοί αποτελούν από κοινού ένα μοναδικό ζεύγος κλειδιού με το οποίο επιτυγχάνεται η αποκρυπτογράφηση των δεδομένων.

RSA - Μια μέθοδος κρυπτογράφησης δημόσιου κλειδιού που μπορεί να χρησιμοποιηθεί και για την κρυπτογράφηση μηνυμάτων και για τη δημιουργία ψηφιακών υπογραφών, δηλ. για την επιβεβαίωση της ταυτότητας του αποστολέα ενός μηνύματος. Το RSA είναι η μέθοδος κρυπτογράφησης δημοσίου κλειδιού που χρησιμοποιείται στο PGP. Τα αρχικά του RSA 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 γινόμενό τους, είναι υπολογιστικά δύσκολο να κάνουμε το αντίστροφο, δηλ. το να βρούμε τους δύο πρώτους παράγοντες ενός δεδομένου σύνθετου αριθμού. Είναι αυτή η φύση του RSA που επιτρέπει τη δημιουργία και την αποκάλυψη στον κόσμο ενός κλειδιού κρυπτογράφησης, ενώ από την άλλη μεριά δεν επιτρέπει την αποκρυπτογράφηση ενός μηνύματος.

SecretKeyEncryption - Αποδίδεται στα ελληνικά με τον όρο Κρυπτογράφηση με Κρυφό Κλειδί και πρόκειται για ένα σύστημα κρυπτογράφησης με το οποίο αποστέλλεται στον παραλήπτη το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ενός μηνύματος.

Secure Web Server - Ένας Web server που εργάζεται με πιστοποιητικά (πρωτόκολλα) ασφαλείας. Οι συνδέσεις που γίνονται μ' έναν τέτοιο Webserver είναι ασφαλείς και όλα τα μηνύματα (δεδομένα) που ανταλλάσσονται με τους πελάτες (clients) του είναι κρυπτογραφημένα.

SET (SecureElectronicTransaction) - Πρόκειται για ένα σύστημα ασφαλών τραπεζικών πληρωμών που έχει δημιουργηθεί από γνωστές εταιρείες πιστωτικών καρτών. Χρησιμοποιεί τη λεγόμενη Έμπιστη Τρίτη Οντότητα (ThirdTrustedParty) στις συναλλαγές εμπόρου-πελάτη, δηλ. μια ιδιωτική εταιρεία εμπιστοσύνης που παρεμβάλλεται ως τρίτος στις συνδιαλλαγές και εκδίδει τα ψηφιακά πιστοποιητικά ταυτότητας των συναλλασσομένων. Τα κρυπτογραφικά αυτά πρωτόκολλα σχεδιάστηκαν και αναπτύχθηκαν από κοινού από τις εταιρείες Visa, MasterCard, Netscape& Microsoft προκειμένου να παρέχουν ασφαλείς συναλλαγές με πιστωτικές κάρτες στο Διαδίκτυο για τους καταναλωτές (επλάτες) και τους πωλητές.

SSL (SecureSocketsLayer)- Πρόκειται για ένα σύστημα (πρωτόκολλο) κρυπτογράφησης που έχει δημιουργήσει η γνωστή εταιρεία Netscape, με σκοπό την ασφαλή σύνδεση (επικοινωνία) ενός

φυλλομετρητή με τον Web server. Τα δεδομένα που στέλνονται ανάμεσα στους δύο είναι κρυπτογραφημένα αλλά το σύστημα δεν εξασφαλίζει την ταυτότητα ούτε του αποστολέα ούτε του παραλήπτη. Είναι ειδικό πρωτόκολλο επικοινωνίας ανάμεσα σε browsers και servers και το οποίο κρυπτογραφεί κάθε online επικοινωνία. Το πρωτόκολλο αυτό διασφαλίζει συναλλαγές με διαφάνεια στους τελικούς χρήστες.

Steganography - Αποδίδεται στα ελληνικά με τον όρο Στεγανογραφία και είναι η διαδικασία απόκρυψης πληροφοριών μέσα σ' ένα άλλο πακέτο πληροφοριών και δεδομένων. Με τον τρόπο αυτό μπορούμε να αποκρύψουμε ένα αρχείο κειμένου μέσα σε κάποιο αρχείο εικόνας ή και ήχου, ώστε να μην γίνεται κατανοητό από τον παραλήπτη του αρχείου εικόνας ή ήχου.

SymmetricEncryption - Αποδίδεται στα ελληνικά με τον όρο Συμμετρική Κρυπτογράφηση και είναι μια από τις πρώτες μορφές κρυπτογραφίας που χρησιμοποιεί το ίδιο κλειδί τόσο για την κωδικοποίηση όσο και για την αποκωδικοποίηση του μηνύματος. Υπάρχει και ηΑσύμμετρη Κρυπτογράφηση (AsymmetricEncryption), η οποία χρησιμοποιεί δύο διαφορετικά κλειδιά (δημόσιο και ιδιωτικό).

SymmetricKey - Αποδίδεται στα ελληνικά με τον όρο Συμμετρικό Κλειδί και είναι η παλιά μέθοδος κρυπτογράφησης που χρησιμοποιεί το ίδιο κλειδί τόσο για την κωδικοποίηση όσο και για την αποκωδικοποίηση του μηνύματος. Δεν χρησιμοποιείται σήμερα καθώς δεν είναι ασφαλής μέθοδος επικοινωνίας.

TripleDES - Είναι μια μέθοδος βελτίωσης των δυνατοτήτων του αλγορίθμου DES, η οποία χρησιμοποιεί τον ίδιο αλγόριθμο τρεις φορές σε αλληλουχία με διαφορετικά κλειδιά, για μεγαλύτερη ασφάλεια.

UserIdentification - Αναφέρεται στην πιστοποίηση, δηλ. στον έλεγχο της ταυτότητας ή του δικαιώματος πρόσβασης σ' έναν δικτυακό τόπο, που γίνεται με το όνομα χρήστη και τον κωδικό πρόσβασης.

Username - Αποδίδεται στα ελληνικά με τον όρο Όνομα Χρήστη ή και Αναγνωριστικό και χρησιμοποιείται συνήθως σε συνδυασμό μ' έναν Κωδικό Πρόσβασης (Password) για την εισαγωγή σ' ένα σύστημα ή δίκτυο πολλαπλών χρηστών. Συνήθως ο χρήστης μπορεί να επιλέξει ο ίδιος το δικό του username (που πρέπει να είναι μοναδικό, στο πλαίσιο ενός δικτύου ή συστήματος) και το password, το οποίο δεν είναι απαραίτητο να είναι μοναδικό αλλά θα πρέπει να είναι απόρρητο και δύσκολο στο να μπορέσει να το εντοπίσει κάποιος.

Verisign - Μια από τις πιο γνωστές διεθνώς εταιρείες που λειτουργεί ως Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ) και εκδίδει ψηφιακές ταυτότητες (digitalID's) σε τρίτους (ιδιώτες ή και εταρείες). Οι εταιρείες αυτές αποκαλούνται και Έμπιστες Τρίτες Οντότητες (ΕΤΟ), δηλ.TrustedThirdParties (TTP), ή και Αρχές Πιστοποίησης (CA, CertificationAuthorities). Μια εταιρεία Παροχής Υπηρεσιών Πιστοποίησης μπορεί να εξουσιοδοτήσει άλλες εταιρείες σ' άλλες χώρες ή και σ' άλλες πόλεις για να κάνουν πιστοποίηση και να σχηματιστεί έτσι ένα δένδρο από τους Οργανισμούς Πιστοποίησης.