2ο Γενικό Λύκειο Καλαμαριάς

ΕΡΕΥΝΗΤΙΚΗ ΕΡΓΑΣΙΑ

ΣΤΕΓΑΝΟΓΡΑΦΙΑ - ΚΡΥΠΤΟΓΡΑΦΙΑ

ΑΠΟ ΤΗ ΛΑΚΕΔΑΙΜΟΝΙΚΗ (ΚΡΥΠΤΕΙΑ) ΣΚΥΤΑΛΗ

ΣΤΗΝ ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ

Επιβλέπων Καθηγητής : Γιώργος Νικολακάκης ΠΕ20
Α΄ Τετράμηνο Σχολικό Έτος 2011-2012

ΠΕΡΙΕΧΟΜΕΝΑ

ΙΣΤΟΡΙΚΕΣ ΑΝΑΦΟΡΕΣ

ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΣΥΓΧΡΟΝΗ ΤΕΧΝΟΛΟΓΙΑ

ΕΙΣΑΓΩΓΗ

Το θέμα αυτής της ερευνητικής εργασίας επιλέχτηκε με σκοπό οι μαθητές :

- ✓ να διαπιστώσουν την ανάγκη διασφάλισης της εγκυρότητας και αυθεντικότητας των πληροφοριών που διακινούνται καθημερινά
- ✓ να αναγνωρίζουν τον κίνδυνο διαρροής και καταγραφής πληροφοριών στις ηλεκτρονικές επικοινωνίες
- ✓ να κατανοήσουν τα βασικά είδη και τις μεθόδους κρυπτογράφησης / στεγανογράφησης
- ✓ να κατασκευάσουν/κατανοήσουν ένα απλό σύστημα κωδικοποίησης / αποκωδικοποίησης
- ✓ να καλλιεργήσουν συνεργατικές δεξιότητες και να αναπτύξουν πνεύμα συλλογικής δημιουργίας με την ανταλλαγή και σύνθεση διαφορετικών απόψεων

Κατά τη διάρκεια της ερευνητικής εργασίας οι μαθητές αρχικά δημιούργησαν μια ιστορική αναδρομή από την αρχαιότητα έως και σήμερα, για να διερευνήσουν τους τρόπους και τις μεθόδους κρυπτογράφησης/στεγανογράφησης που χρησιμοποιήθηκαν κατά καιρούς αλλά και να κατανοήσουν την ανάγκη που υπήρχε και συνεχίζει να υπάρχει, σε πολύ μεγαλύτερο βαθμό σήμερα, για την ασφαλή διακίνηση των πληροφοριών μέσω ιστορικών αναφορών.

Στη συνέχεια διερευνήθηκαν συγκεκριμένοι τρόποι κρυπτογράφησης στη σύγχρονη εποχή, οι οποίοι βρίσκουν εφαρμογές στην καθημερινότητα (π.χ. Κώδικες σήμανσης προϊόντων – Bar Code, QR Code, Μαγνητικές κάρτες κ.α.).

Οι ομάδες εργασίας χρησιμοποίησαν διαμορφωμένο ιστοχώρο από τα wikispaces για την καταγραφή (ανέβασμα), τη διόρθωση ή και συμπλήρωση των επιμέρους εργασιών, την ανταλλαγή πληροφοριών και την επικοινωνία μεταξύ αυτών και του συντονιστή.

Επιπλέον, πέρα από το διερευνητικό ρόλο της εργασίας, κατά τη διάρκεια της ερευνητικής εργασίας πραγματοποιήθηκαν κάποια εκπαιδευτικά παιχνίδια-δραστηριότητες σχετικά με την κρυπτογραφία και την ασφαλή επικοινωνία . Συγκεκριμένα πραγματοποιήθηκαν με τη συμμετοχή όλων των μαθητών τα παρακάτω παιχνίδια που αναφέρονται στο "Computer Science Unplugged" Bell, Witten, and Fellows, 1998 :

- Απόκρυψη πληροφορίας (Information Hiding)
- Πρωτόκολλα κρυπτογραφίας (Cryptographic protocols)
- Κρυπτογράφηση με δημόσιο κλειδί (Public key encryption)
- Έλεγχος και διόρθωση σφαλμάτων πληροφορίας (Error Detection)

Η τελευταία δραστηριότητα (παιχνίδι) αναφέρεται στο Παράρτημα στο τέλος της εργασίας

ΙΣΤΟΡΙΚΕΣ ΑΝΑΦΟΡΕΣ

1. ΙΕΡΟΓΛΥΦΙΚΑ – ΓΡΑΜΜΙΚΗ ΓΡΑΦΗ Α – ΓΡΑΜΜΙΚΗ ΓΡΑΦΗ Β

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

1.1. ΙΕΡΟΓΛΥΦΙΚΑ

Περιεχόμενα

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

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

Η μεγαλύτερη αποκρυπτογράφηση ήταν αυτή των αιγυπτιακών ιερογλυφικών τα οποία, επί αιώνες, παρέμεναν μυστήριο και οι αρχαιολόγοι μόνο εικασίες μπορούσαν να διατυπώσουν για τη σημασία τους. Ωστόσο, χάρη σε μία κρυπταναλυτική εργασία, τα ιερογλυφικά εν τέλει αναλύθηκαν και έκτοτε οι αρχαιολόγοι είναι σε θέση να διαβάζουν ιστορικές επιγραφές. Τα αρχαιότερα ιερογλυφικά χρονολογούνται περίπου από το 3000 π.Χ. Τα σύμβολα των ιερογλυφικών ήταν υπερβολικά πολύπλοκα για την καταγραφή των συναλλαγών εκείνης της εποχής. Έτσι, παράλληλα με αυτά, αναπτύχθηκε για καθημερινή χρήση η ιερατική γραφή, που ήταν μία συλλογή συμβόλων, τα οποία ήταν εύκολα τόσο στο γράψιμο όσο και στην ανάγνωση. Τον 17ο αιώνα αναθερμάνθηκε το ενδιαφέρον για την αποκρυπτογράφηση των ιερογλυφικών,

έτσι το 1652 ο Γερμανός Ιησουΐτης Αθανάσιος Κίρχερ εξέδωσε ένα λεξικό ερμηνείας τους, με τίτλο «*Oedipus Aegyptiacus*». Με βάση αυτό προσπάθησε να ερμηνεύσει τις αιγυπτιακές γραφές, αλλά η προσπάθεια του αυτή ήταν κατά γενική ομολογία αποτυχημένη. Για παράδειγμα, το όνομα του Φαραώ Απρίη, το ερμήνευσε σαν «τα ευεργετήματα του θεϊκού Όσιρι εξασφαλίζονται μέσω των ιερών τελετών της αλυσίδας των πνευμάτων, ώστε να επιδαψιλεύσουν τα δώρα του Νείλου». Παρόλα αυτά, η προσπάθεια του άνοιξε τον δρόμο προς 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 στα ιερατική γραφή. Δύο μεγάλοι αποκρυπτογράφοι της εποχής, ο Γιάνγκ και ο Σαμπολιόν, μοιράστηκαν την δόξα της ερμηνείας τους. Οι προϊστορικοί πληθυσμοί χρησιμοποίησαν τρεις γραφές μέχρι να επινοήσουν αλφάβητο, γύρω στο 850 π.Χ.

ΑΡΙΘΜΟΙ ΙΕΡΟΓΛΥΦΙΚΩΝ

 . .1. . . .  . .10. . .  . .100.

..  . .1000

 . .10,000. . . . .  . .100,000. . .

. . . . .  . .1,000,000

12,425 Birds

Ο αριθμός

π.χ.: 

= 1,246,323

ΙΕΡΟΓΛΥΦΙΚΑ ΙΔΕΟΓΡΑΜΜΑΤΑ & ΣΥΝΑΜΑ ΚΑΘΟΡΙΣΤΙΚΑ ΣΥΜΒΟΛΑ

 . . . . .  . . . . . 

Man, male. . . . . .Woman, female. . . . . People.

 . . . . .  . . . . . 

Official, authority. . . . . King. . . . . .Force, effort

 . . . . .  . . . . . 

Child, young. . . . . Enemy. . . . . Praise

 . . . . .  . . . . . 

Lie down, death, bury. . . . . God. . . . . .Exalted person, the dead

 . . . . .  . . . . . 

Village, town. . . . . Desert, foreign land. . . . . Animal.



Bird. . . . . .Enemy . . . . . .Fish



Water, liquid. . . . . .Road. . . . . .Sky, above



Sun, light, time. . . . . .Stone. . . . . .Star.

1.1.1. Στήλη Ροζέτας (The Rosetta Stone)

Η ανάγνωσή των ιερογλυφικών έγινε για πρώτη φορά από το Σαμπολιόν το 1822. Ο Σαμπολιόν(Jean-Francois Champollion, 1790-1832) βοηθήθηκε σ' αυτό από τη στήλη της Ροζέτας, η οποία περιείχε το αυτό κείμενο και στα ελληνικά και στα Αιγυπτιακά (ιερογλυφικά και δημοτική). Επί μ. Αλεξάνδρου και πριν η ελληνική γλώσσα ήταν διεθνής (Ελληνιστική περίοδος 323 π.Χ. - 31 π.Χ.) και πολλές πινακίδες τότε είχαν γραφεί δίγλωσσα, όπως π.χ. η στήλη της Ροζέτας με ελληνικά και αιγυπτιακά, η επιγραφή Ράμπαδ στο 'Αλεπ με ελληνικά, συριακά, και αραβικά, η επιγραφή Αρράνστο Αουράν με ελληνικά και αραβικά... κ.α.

Η στήλη της Ροζέτας

1.2. ΓΡΑΜΜΙΚΗ ΓΡΑΦΗ Α

Περιεχόμενα

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 πρώτος άγγλο αρχαιολόγο που ανάσκαψε συστηματικά την Κνωσό το 1900. Ο ίδιος ονόμασε αυτή την 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΄(περίπου 1.500) 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 επιτευχτεί η αποκρυπτογράφηση της.

Ωστόσο χαρακτηριστικό παράδειγμα της Γραμμικής Α΄ αποτελεί ο δίσκος της Φαιστού:

Ο Δίσκος της Φαιστού είναι ένα αρχαιολογικό εύρημα από την 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. Ο δίσκος έχει κεντρίσει τη φαντασία πολλών αρχαιολόγων, επαγγελματιών και μη, και έχουν γίνει αρκετές προσπάθειες αποκρυπτογράφησής του. Έχουν προταθεί πάρα πολλές ερμηνείες του κειμένου του, όπως ότι πρόκειται για προσευχή, για τη διήγηση μίας ιστορίας η για ημερολόγιο κ.α.. Παρόλα αυτά η επιστημονική κοινότητα δεν έχει αποδεχθεί καμία από τις προτεινόμενες αποκρυπτογραφήσεις και ο δίσκος παραμένει ένα άλυτο μυστήριο.

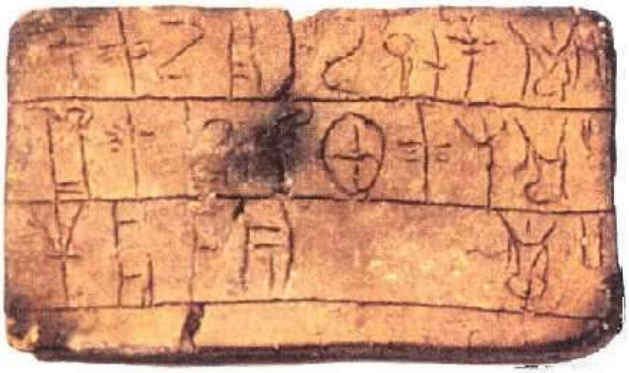
1.3. ΓΡΑΜΜΙΚΗ ΓΡΑΦΗ Β

Περιεχόμενα

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

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 δύο επιφάνειες: μία επίπεδη λειασμένη, που επρόκειτο να αποτελέσει την κύρια γραφική επιφάνεια και μία κυρτή, που συνήθως έμενε άγραφη. Συστηματικά, με την γραφή αυτή, με την οποία είχε πραγματικό πάθος, ασχολήθηκε ο Άγγλος αρχιτέκτονας και αρχαιολόγος Μάικλ Βέντρις ο οποίος ήταν ο πρώτος που κατάλαβε ότι επρόκειτο για κάποιο είδος ελληνικής γραφής.

Μέσα από ιστορικές αναφορές που έχουν διασωθεί μέχρι σήμερα παρουσιάζονται πάρα πολλά μηνύματα. Μερικά μηνύματα έπρεπε πάντα να σταλούν με την μέγιστη 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 απ' αυτές δείχνουν πολύ απλοϊκές σήμερα, αλλά κάποιες άλλες δεν έχουν αποκρυπτογραφηθεί ακόμα.



Πήλινη πινακίδα γραμμένη σε Γραμμική Β γραφή. Βρέθηκε στις Μυκήνες. 13ο αι. π.Χ.

2. Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΤΟΥΣ ΕΛΛΗΝΟΡΩΜΑΪΚΟΥΣ ΧΡΟΝΟΥΣ

2.1. ΣΠΑΡΤΙΑΤΙΚΗ ΣΚΥΤΑΛΗ

Περιεχόμενα

Στην αρχαία Σπάρτη για την αποστολή απόρρητων στρατιωτικών μηνυμάτων, το μήνυμα γραφόταν σ' ένα κύλινδρο που γύρω του είχε τυλιχτεί μία στενή λωρίδα δέρματος σε διαδοχικές σειρές. Αυτή ήταν η περιβόητη σκυτάλη. Ο κύλινδρος αφαιρούνταν κι 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».

Άλλη μέθοδος χρησιμοποιούσε την ουροδόχου κύστη κάποιου ζώου που φουσκωνόταν και πάνω της γραφόταν με οριακά μικρά γράμματα το μήνυμα. Όταν ξεφουσκωνόταν το μήνυμα έδειχνε πια σαν λεκές. Κατά την αποστολή της συνήθως κρυβόταν καλά, π.χ. σε δοχείο με λάδι και ο παραλήπτης έπρεπε να την φουσκώσει και πάλι για να μπορέσει να διαβάσει το μήνυμα.

2.2. Ο ΚΩΔΙΚΑΣ ΤΟΥ ΠΟΛΥΒΙΟΣ

Περιεχόμενα

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 220 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 στην τηλεγραφία εργαλείο, το οποίο επιτρέπει την κωδικοποιημένη αποστολή γραμμάτων με τη χρήση ενός αριθμητικού συστήματος. Στην ιδέα αυτή επίσης στηρίζονται η κρυπτογραφία και η στενογραφία. Το εργαλείο αυτό είναι γνωστό ως το «Τετράγωνο του Πολυβίου». 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 (στο σύγχρονο λατινικό αλφάβητο των 26 χαρακτήρων, τα γράμματα «Ι» και «J» συνδυάζονται). Στη συνέχεια, οι σειρές και οι στήλες αριθμούνται οριζοντίως και καθέτως, συνήθως με τους αριθμούς από 1 έως 5. Έτσι, οι κάθε ζεύγος 2 αριθμών (συντεταγμένες) 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 συσκευή που εφευρέθηκε από τον Πολύβιο και χρησιμοποιήθηκε από τους Αρχαίους Έλληνες για τη κωδικοποίηση των μηνυμάτων που αντάλλασσαν φυλάκια (σκοπιές) μεταξύ τους. Ο λόγος που ο Πολύβιος δημιούργησε αυτό 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 (π.χ. δυο πεντάδες από πυρσούς, 2 πεντάδες από χρωματιστές σημαίες κλπ). 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	

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 (σχεδόν). Έτσι οι Ιάπωνες από το 1500 έως το 1910 έκαναν χρήση του Τετραγώνου του Πολυβίου, τροποποιημένο ώστε να καλύπτει τα 48 γράμματα της 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 ως 37 γράμματα).

Ο τρόπος λειτουργίας του πίνακα είναι απλός: κάθε γράμμα αναπαρίσταται από τις συντεταγμένες του στο 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 "ΒΑΤ" με βάση το 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".

2.1.1. Τηλεγραφία και Στεγανογραφία

Ο Πολύβιος δημιούργησε το Τετράγωνο σαν βοήθημα για την τηλεγραφία, δηλαδή τη μετάδοση γραπτών μηνυμάτων σε απόσταση- παρά ως μέσο κρυπτογράφησης. Πρότεινε την χρήση δύο πεντάδων πυρσών στα φυλάκια όπου με ένα απλό σχετικά σύστημα είτε ανεβάζοντας και κατεβάζοντας τους πυρσούς είτε με την χρήση ξύλινης μάσκας με οπές που μπορούσαν να καλύπτονται ώστε να εκτίθεται τελικά ο επιθυμητός αριθμός φωτεινών σημείων, θα μπορούσε να μεταδώσει το όποιο επείγον μήνυμα στη Πόλη ή τα υπόλοιπα φυλάκια σε σχεδόν μηδενικό χρόνο.

Ως κώδικας, λέγεται ότι το Τετράγωνο του Πολυβίου χρησιμοποιήθηκε από τους φυλακισμένους του Τσάρου της Ρωσίας που με χτυπήματα σε σωλήνες και τοίχους αντάλλασσαν μεταξύ τους μηνύματα, αλλά και πολύ αργότερα από τους Αμερικανούς αιχμαλώτους του πολέμου στο Βιετνάμ.

Ουσιαστικά η μετάδοση των μηνυμάτων μπορεί να γίνει με πληθώρα διαφορετικών μέσων όπως αναβόσβημα φώτων, πακέτα ήχων, ταμ-ταμ, σήματα καπνού κ.α. επιπλέον είναι πολύ εύκολο να απομνημονευθεί σε σχέση με πιο σύνθετα συστήματα κωδικοποίησης όπως π.χ. τα σήματα Μορς.

Ωστόσο είναι κατά τι λιγότερο αποδοτικός από πιο πολύπλοκους κώδικες. Η απλότητα στη κωδικοποίηση ευνοεί την χρήση του Τετραγώνου του Πολυβίου στη Στεγανογραφία, αφού οι τιμές από το 1 μέχρι το 5 μπορούν να αναπαρασταθούν με σειρά από κόμπους σε σχοινί, λωρίδες ή σχήματα σε ένα κιλτ, πυκνογραμμένα γράμματα πριν από μεγάλο κενό ή και άλλοι απλοί τρόποι απεικόνισης.

2.1.2. Κρυπτογραφία

Ο βαθμός ασφαλείας που παρέχει το Τετράγωνο του Πολυβίου είναι πολύ περιορισμένος, ακόμη και αν συνδυαστεί με αλγορίθμους αντικατάστασης και μεικτά αλφάβητα: τα ζεύγη των αριθμών προκύπτουν αν σε έναν πίνακα αντικατάστασης που το σύνολο των συμβόλων του είναι απλά ζεύγη αριθμών . Ο Πολύβιος τελικά εφηύρε ένα πραγματικά χρήσιμο εργαλείο για τη τηλεγραφία, που επέτρεψε την εύκολη μετάδοση γραμμάτων σε απόσταση μέσω μετασχηματισμού των γραμμάτων σε αριθμητικές απεικονίσεις. Η ίδια ιδέα είναι εφαρμόσιμη και στη κρυπτογραφία και τη στεγανογραφία.

2.3. ΡΩΜΑΙΚΟΙ ΧΡΟΝΟΙ – Ο ΚΩΔΙΚΑΣ ΤΟΥ ΚΑΙΣΑΡΑ

Περιεχόμενα

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

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

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.

3. Η ΚΡΥΠΤΟΓΡΑΦΙΑ - ΣΤΕΓΑΝΟΓΡΑΦΙΑ ΣΤΟΝ ΜΕΣΑΙΩΝΑ

3.1. ΓΕΝΙΚΑ

Περιεχόμενα

Στην διάρκεια του Μεσαίωνα, η κρυπτογραφία ήταν κάτι το απαγορευμένο και αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας, κάτι που συντέλεσε στην καθυστέρηση της ανάπτυξης της.

Τα μυστικά της κρυπτογραφίας φυλάσσονταν στα μοναστήρια ή στα μυστικά αρχεία των βασιλιάδων και λίγες μέθοδοι γίνονταν ευρέως γνωστές.

Κατά την αναγέννηση η κρυπτογραφίας έγινε χωριστή επιστήμη και ταυτόχρονα οι εφαρμοστές της αναζητούσαν μια γενική γλώσσα.

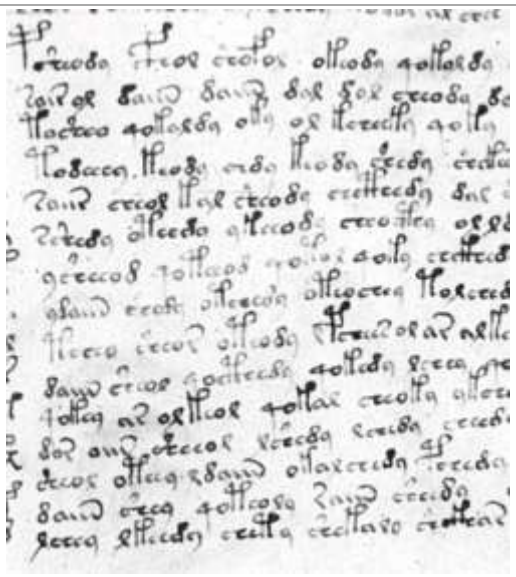
Οι αλχημιστές του μεσαίωνα συνήθιζαν να κρατούν ως επτασφράγιστα μυστικά τις λεπτομέρειες των τεχνικών τους και να κρατούν σημειώσεις με "κρυπτογραφικά" σύμβολα. Αυτό είχε ως αποτέλεσμα να ταυτιστούν με μυστικιστικές ομάδες και συντεχνίες με "ύποπτους σκοπούς". Αλλά και οι ίδιοι οι αλχημιστές, τις περισσότερες φορές σκόπιμα και για λόγους εντυπωσιασμού και βιοπορισμού, δεν επεδίωξαν να διαχωρίσουν την "τέχνη" τους από το υπερφυσικό, το μαγικό και τη δεισιδαιμονία.

Η εξέλιξη, τόσο της κρυπτογραφίας, όπως και των μαθηματικών, συνεχίζεται στον Αραβικό κόσμο. Οι Άραβες είναι οι πρώτοι που επινόησαν αλλά και χρησιμοποίησαν μεθόδους κρυπτανάλυσης. Το κυριότερο εργαλείο στην κρυπτανάλυση, η χρησιμοποίηση των συχνοτήτων των γραμμάτων κειμένου, σε συνδυασμό με τις συχνότητες εμφάνισης στα κείμενα των γραμμάτων της γλώσσας, επινοήθηκε από αυτούς γύρω στον 14ο αιώνα. Η κρυπτογραφία, λόγω των στρατιωτικών εξελίξεων, σημείωσε σημαντική ανάπτυξη στους επόμενους αιώνες.

Ο Ιταλός *Giovanni Batista Porta*, το 1563, δημοσίευσε το περίφημο για την κρυπτογραφία βιβλίο «*De furtivis literarum notis*», με το οποίο έγιναν γνωστά τα πολυαλφαβητικά συστήματα κρυπτογράφησης και τα διγραφικά κρυπτογραφήματα. Σημαντικός εκπρόσωπος εκείνης της εποχής είναι και ο Γάλλος *Vigenere*, του οποίου ο πίνακας πολυαλφαβητικής αντικατάστασης, χρησιμοποιείται ακόμη και σήμερα. Μέσα από την αποκρυπτογράφηση της ακατάληπτης ερμητικής γλώσσας των αλχημιστών, οι ιστορικοί αρχίζουν να αντιλαμβάνονται όλο και περισσότερο την πνευματική σύνδεση που υπάρχει ανάμεσα στην αλχημική μέθοδο και σε άλλες όψεις της πολιτισμικής ιστορίας της Δύσης.

3.2. ΧΕΙΡΟΓΡΑΦΟ ΒΟΙΝΙΤΣ

Περιεχόμενα



Το χειρόγραφο Βόινιτς πήρε το όνομα 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.

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.

3.3. ΚΡΥΠΤΟΓΡΑΦΙΑ - ΟΙ ΠΡΩΤΟΙ ΑΛΓΟΡΙΘΜΟΙ

Περιεχόμενα

Ο σημαντικότερος εκπρόσωπος των Αράβων κρυπτολόγων είναι ο πανεπιστήμων του 9ου αιώνα Αλ Κιντί. έγραψε πάνω από 290 βιβλία Μαθηματικών – Γλωσσολογίας – Αστρολογίας– Ιατρικής και Μουσικής.

Η Ευρωπαϊκή κρυπτογραφία έχει τις ρίζες της το μεσαίωνα, που αναπτύχθηκε από τους Πάπα και τις Ιταλικές πόλεις κράτη, αλλά τα περισσότερα συστήματα βασίζονταν στην απλή αντικατάσταση γραμμάτων της αλφαβήτου (όπως στον αλγόριθμο του Καίσαρα). Οι πρώτοι αλγόριθμοι βασίζονταν στην αντικατάσταση των φωνηέντων. Το πρώτο Ευρωπαϊκό εγχειρίδιο κρυπτογραφίας (1379) ήταν μια συλλογή αλγορίθμων από τον Gabriele de Lavinde of Parma, για τον Πάπα. Το 1470 ο Leon Battista Alberti εξέδωσε το "Trattati in cifra", όπου περιγράφεται ο πρώτος δίσκος κρυπτογράφησης (τον οποίο είχε κατασκευάσει το 1460), χρησιμοποιώντας 15και την έννοια της χρήσης πολλαπλών αλφαβήτων. Επίσης στο βιβλίο αυτό περιέγραφε και τις αρχές της ανάλυσης συχνότητας των γραμμάτων.

Ο Φλωρεντινός Λέων Μπατίστα Αλμπέρτι (1404 μΧ.) στην κρυπτανάλυση ήταν ο πρώτος που σκέφθηκε ένα πολυαλφαβητικό σύστημα, δηλ. ένα σύστημα με περισσότερα από ένα κρυπτογραφικά αλφάβητα, γεγονός που κάνει την κρυπτανάλυση δυσκολότερη αφού δεν διατηρεί τις συχνότητες των γραμμάτων. Επίσης επινόησε και την πρώτη μετά τη σκυτάλη κρυπτογραφική μηχανή, τους λεγόμενους δίσκους του Alberti. Πήρε δύο χάλκινους δίσκους διαφορετικής διαμέτρου, τους έκανε ομόκεντρους και χάραξε ένα αλφάβητο στην περιφέρεια του κάθε δίσκου. Οι δύο δίσκοι μπορούν να περιστρέφονται ανεξάρτητα. Ο έξω δίσκος αναφέρεται στο α.κ. και οι αντίστοιχες θέσεις του μέσα δίσκου μας δίνουν το κ.κ.. Για περισσότερη δυσκολία ένα μέρος του μηνύματος κρυπτογραφείται σε μια θέση του εσωτερικού δίσκου και ένα άλλο μέρος σε άλλη θέση του δίσκου (πολυαλφαβητικό).

Το 1499 μΧ. ο Γερμανός abbas Johanes Trithemius έγραψε τη Στενογραφία, ένα βιβλίο επικοινωνίας με τα πνεύματα.

3.4. ΑΛΛΑ ΓΕΓΟΝΟΤΑ ΚΑΙ ΜΕΘΟΔΟΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Περιεχόμενα

Ο Sir Francis Bacon το 1563 περιέγραψε έναν αλγόριθμο που σήμερα φέρει το όνομά του. Ήταν ένας αλγόριθμος που χρησιμοποιούσε κωδικοποίηση 5 bits. Τον αλγόριθμο αυτό τον εξέλιξε σαν μια μέθοδο στεγανογραφίας, χρησιμοποιώντας μία

μεταβολή στη μορφή των χαρακτήρων μετέφερε κάθε bit της κωδικοποίησης. πίνακες αριθμών που δήθεν αντιπροσώπευαν κώδικες επικοινωνίας με τα πνεύματα.

Το αόρατο μελάνι ήταν μία ακόμα μέθοδος που χρησιμοποιούνταν αρκετά. Πάνω συνήθως από κάποιο άλλο κείμενο αδιάφορου περιεχομένου γραφόταν με χυμό λεμονιού αντί για μελάνι το κρυφό μήνυμα. Μετά μπορούσε να διαβαστεί στο φως κεριού μόνο από τον υποψιασμένο παραλήπτη.

Ακόμα και βρασμένα αυγά χρησιμοποιήθηκαν για την ασφαλή μεταφορά μηνυμάτων. Τον 16ο αιώνα στην Ιταλία ο Τζιοβάνι Πόρτα έγραφε με μελάνι φτιαγμένο από σκόρδο και ξύδι πάνω στο τσόφλι του αβγού. Το μελάνι απορροφούταν στο εσωτερικό και εξωτερικά δεν φαινόταν τίποτα. Το μήνυμα όμως παρέμενε αποτυπωμένο πάνω στο ασπράδι του βρασμένου αβγού.

Ο βραχμάνος λόγιος Βατσιγιάνα έγραψε τον 4ο μΧ. αιώνα το περίφημο «Κάμα Σούτρα».Τα «Κάμα Σούτρα» συνιστούν στις γυναίκες να μελετούν 64 τέχνες όπως, μαγειρική, ενδυματολογία, αρωματοποιία κλπ. Η 45η τέχνη του καταλόγου είναι η μιλεχίτα βικάλπα, δηλ., η τέχνη της μυστικής γραφής (σύσταση που αφορά την απόκρυψη των ερωτικών τους περιπετειών).

3.5. ΚΩΔΙΚΑΣ VIGENERE (ΚΩΔΙΚΑΣ ΜΕ ΣΥΜΜΕΤΡΙΚΟ ΚΛΕΙΔΙ) Περιεχόμενα

Ένας αλγόριθμος κρυπτογράφησης λέγεται συμμετρικός όταν γνωρίζουμε το κλειδί κρυπτογράφησης k και είναι υπολογιστικά «εύκολο» να προσδιορίσουμε το κλειδί αποκρυπτογράφησης k′, και αντίστροφα. 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 δύο υποκατηγορίες:

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

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

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

Ο κώδικας Vigenère 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.* Ωστόσο, το σχέδιο ήταν μη αποδεκτό ως Blaise de Vigenère τον 19ο αιώνα και πλέον ειναι ευρέως γνωστό ως "κώδικας Vigenère".

Αυτή η κρυπτογράφηση είναι γνωστή γιατί ενώ είναι εύκολο να την κατανοήσουν και να την εφαρμόσουν, εμφανίζεται συχνά σε αρχάριους ως αδιάσπαστη. Κατά συνέπεια, πολλοί άνθρωποι προσπάθησαν να εφαρμόσουν συστήματα κρυπτογράφησης που είναι ουσιαστικά Vigenère κώδικες, μόνο για να τα έχουν σπάσει.

	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

3.5.1. Πολύαλφαβητικά κρυπτοσυστήματα τετραγώνου Viginere

Στα πολυαλφαβητικά κρυπτοσυστήματα κάθε γράμμα του μηνύματος αντικαθίσταται με ένα σύμβολο κάθε φορά από διαφορετικό αλφάβητο. Κάθε γράμμα του μηνύματος αντικαθίσταται με διαφορετικό κάθε φορά σύμβολο. Ορίζεται ένας πίνακας αντιστοίχησης 1-1 (αμφιμονότιμη) από το αλφάβητο της γλώσσας σε πολλά διαφορετικά αλφάβητα ανακατεμένα ή μη φυσικά αλφάβητα τα οποία αλλάζουν κάθε φορά ανάλογα με τα γράμματα της κλείδας. Το τετράγωνο Viginere 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 Α στον πιν 2.4 το στοιχείο που δείχνουν είναι το γράμμα L όπου είναι το παραγόμενο κρυπτόγραμμα. Η διαδικασία επαναλαμβάνεται για τα επόμενα γράμματα του μηνύματος.. Η αντίστροφη διαδικασία οδηγεί στην αποκρυπτογράφηση.

Κωδική λέξη AVALANCHEAVALANCHE Έστω το μήνυμα : LANDINGINBLUECOAST
Το παραγόμενο κρυπτοκείμενο είναι : LVNOIAIPRBGUPCBCZX

Υπάρχουν δύο τύποι μικτών αλφαβήτων

- 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 αλφαβήτου. 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 κρυπτοαλγορίθμου 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 ν διαφορετικά γράμματα. Άρα η συχνότητα του καταμερίζεται σε ν διαφορετικά γράμματα. Όπου ν είναι οι χαρακτήρες του κλειδιού. Πιο επίπεδη κατανομή σε ένα κρυπτόγραμμα σημαίνει μεγάλο παράγοντα εργασία και οδηγεί σε μία πρώτη σχεδιαστική αρχή.

4. Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΜΕΤΑ ΤΟΝ ΗΛΕΚΤΡΙΣΜΟ

4.1. Ο ΚΩΔΙΚΑΣ MORSE

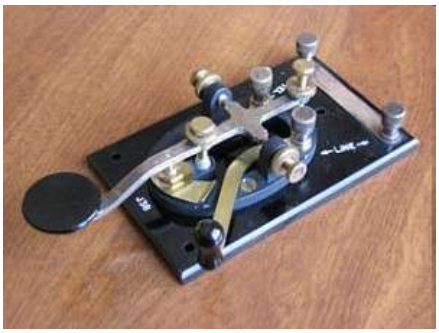
Περιεχόμενα

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.

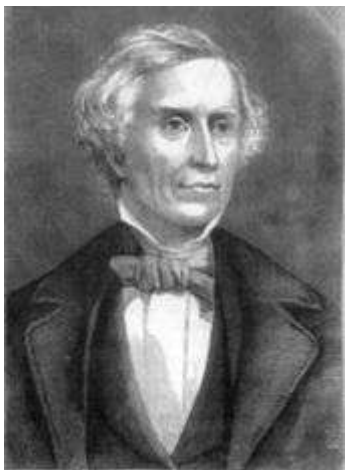
Ο κώδικας Morse επινοήθηκε από τον Σάμιουελ Μόρς (Samuel Morse) το έτος 1830 και χρησιμοποιήθηκε για πρώτη φορά στις ενσύρματες τηλεγραφικές επικοινωνίες ξηράς. Μετά τα πρώτα πειράματα του Μαρκόνι για τις ασύρματες εκπομπές, έγινε ο βασικός τρόπος μετάδοσης των πληροφοριών μέσω ασυρμάτου.

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.

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».



Χειριστήριο (key) Μόρς



Samuel Mors

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. Το καθιερωμένο ελληνικό μορσικό αλφάβητο έχει ως εξής:

Γράμμα	*Κωδικοποίηση σε Μορς*	*Μνημονικός Κανόνας*
Α	·–	*ΑΝ*
Β	–···	*ΒΑΟΥ*
Γ	––·	*ΓΡΙ*
Δ	–··	*ΔΙΑ*
Ε	·	*ΕΙΣΗ ΤΜΟΧ*
Ζ	––··	*ΤΖΙΑ*
Η	····	*ΕΙΣΗ ΤΜΟΧ*
Θ	–·–·	*ΘΕΜΑ*
Ι	··	*ΕΙΣΗ ΤΜΟΧ*
Κ	–·–	*ΚΟΚ*
Λ	·–··	*ΕΛΙΑ*
Μ	––	*ΕΙΣΗ ΤΜΟΧ*
Ν	–·	*ΝΑ*
Ξ	–··–	*ΞΟΥΤ*

Ο	−−−	*ΕΙΣΗ ΤΜΟΧ*
Π	·−−·	*ΑΡΠΑ*
Ρ	·−·	*ΑΡΑ*
Σ	···	*ΕΙΣΗ ΤΜΟΧ*
Τ	−	*ΕΙΣΗ ΤΜΟΧ*
Υ	−·−−	*ΛΥΝΞ*
Φ	··−·	*ΟΥΦΑ*
Χ	−−−−	*ΕΙΣΗ ΤΜΟΧ*
Ψ	−−·−	*ΧΛΕΨ*
Ω	·−−	*ΩΧΡ*

Ψηφία	**Κωδικοποίηση σε Μορς**	**Ψηφία**	**Κωδικοποίηση σε Μορς**
1	·————	6	−····
2	··———	7	——···
3	···——	8	———··
4	····—	9	————·
5	·····	0	—————

4.2. Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΤΗ ΛΟΓΟΤΕΧΝΙΑ (DANCING MEN – SERLOK HOLMES)

Περιεχόμενα

Ο κ. Hilton Cubitt του Ridling Thorpe Manor στο Norfolk επισκέπτεται τον Σέρλοκ Χολμς και του δίνει ένα κομμάτι χαρτί με την εξής μυστηριώδη ακολουθία των αριθμών ραβδιών.

Οι μικροί άνδρες που χορεύουν βρίσκονται στην καρδιά ενός μυστηρίου που φαίνεται να κινεί η νέα του σύζηγος Elsie . Την παντρεύτηκε πριν απο ένα περίπου χρόνο, και μέχρι πρόσφατα, όλα ήταν καλά. Είναι Αμερικάνα, και πριν από το γάμο, ζήτησε απο τον άντρα της να της υποσχεθεί να μην τη ρωτήσει ποτέ για το παρελθόν της, αφού η ίδια πέρασε απο κάποιες "πολύ δυσάρεστες καταστάσεις" στη ζωή της, αν και είπε ότι δεν υπήρχε τίποτα σημαντικό για το οποίο θα έπρεπε να ντρέπεται γι'αυτην. Ο κ. Cubitt ορκίστηκε πως θα τηρησει την υπόσχεση του και, όντας ένας έντιμος Άγγλος υπήκοος.
Το πρόβλημα ξεκίνησε όταν Elsie έλαβε μια επιστολή από τις Ηνωμένες Πολιτείες, η οποία την διατάραξε προφανώς, με αποτέλεσμα να ρίξει την επιστολή στην πυρκαγιά. Στη συνέχεια, οι άνδρες εμφανίστηκαν και άρχισαν να χορεύουν, μερικές φορές σε ένα κομμάτι χαρτί που είχε απομείνει στο ηλιακό ρολόι , μερικές φορές σχεδιασμένοι απο κιμωλία σε τοίχους ή πόρτες, ακόμη και ένα windowsill. Κάθε φορά, η εμφάνισή τους έχει μια προφανή, τρομακτική επίδραση στην Elsie, αλλά δεν θα πει στο σύζυγό της τι συμβαίνει. Ο Holmes λέει στον Cubitt ότι θέλει να δει κάθε εμφάνιση των ανδρών να χορεύουν. Στην συνέχεις, θα πρέπει να αντιγράφθηκαν ή να στάλθηκαν σε αυτόν στην οδό 221B Baker Str. Ο Cubitt παρέχει στον Χολμς μια σημαντική ένδειξη. Ο Holmes συνειδητοποιεί ότι είναι ένα κρυπτογράφημα. Έτσι, σπάει τον κωδικό με την ανάλυση συχνοτήτων. Το τελευταίο από τα μηνύματα που μεταφέρονται από τους άνδρες που χορεύουν είναι ένα ιδιαίτερα ανησυχητικό μήνυμα.

Ο Holmes ορμά κάτω στο Ridling Thorpe Manor και βρίσκει τον Cubitt νεκρό από μια σφαίρα στην καρδιά και τη σύζυγό του τραυματισμένη σοβαρά στο κεφάλι. Ο επιθεωρητής Martin της χωροφυλακής Norfolk πιστεύει ότι πρόκειται για μια δολοφονία-αυτοκτονία. Η Elsie είναι ο κύριος ύποπτος για το θάνατο του συζύγου της. Ο Holmes βλέπει τα πράγματα διαφορετικά. Γιατί υπάρχει μια τρύπα από σφαίρα στο περβάζι , δηλαδή συνολικά τρεις βολές, ενώ ο Cubitt και η σύζυγός του σε κάθε πυροβολισμό πυροβόλισαν μόνο μια φορά; Γιατί μόνο δύο θάλαμοι στο περίστροφο του Cubitt άδειοι; Τι κάνει ένα μεγάλο ποσό των χρημάτων μέσα στο δωμάτιο; Η ανακάλυψη ενός καταπατημένου παρτεριού που φαίνεται έξω από το παράθυρο, και ένα περίβλημα απο 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 γνωρίζει ορισμένα πράγματα σε αντίθεση με τον Επιθεωρητή Martin. Εκείνος τυχαία επιλέγει φαινομενικά το όνομα "Elrige", και ο βοηθός του Cubitt το αναγνωρίζει ως το όνομα ενός τοπικού αγρότη. Ο Holmes γράφει γρήγορα ένα μήνυμα - στους άνδρες που χορεύουν - και στέλνει το αγόρι στους στάβλους του Elrige για να το παραδώσει σε έναν ένοικο που ήταν εκεί, του οποίου το όνομα έχει επίσης επιλεχθεί τυχαία. Φυσικά, ο Holmes έχει μάθει τα ονόματα των δύο ανδρών με την ανάγνωση του κώδικα των ανδρών που χορεύουν. Περιμένοντας για το αποτέλεσμα αυτού του μηνύματος, ο Χολμς παίρνει την ευκαιρία να εξηγήσει στον Watson και τον Επιθεωρητή Martin πώς κατάφερε να σπάσει τον κωδικό των ανδρών που χορεύουν, και τα μηνύματα αποκαλύπτονται. Το τελευταίο μήνυμα, που προκάλεσε την οδήγηση του Σέρλοκ Χολμς στη χωροφυλακή Norfolk, έλεγε "Elsie προετοιμάσου να γνωρίσεις το Θεό σου".

Ο ένοικος, ο κ. Abe Slaney, ένας άλλος Αμερικανός, όπου αγνοεί ότι η Elsie είναι ετοιμοθάνατη και δεν είναι σε θέση να επικοινωνήσει, φτάνει στο Ridling Thorp Manor λίγο αργότερα, προς μεγάλη έκπληξη όλων, εκτός από τον Holmes,ο οποίος έχει στείλει μήνυμα στον Slaney μέσω των ανδρών που χορεύουν, θέλοντας να τον παγηδέψει και να πιστέψει ότι το μήνυμα προέρχεται από την Elsie. Είναι κατασχέθηκαν καθώς έρχεται μέσα από την πόρτα. Λέει όλη την ιστορία. Είναι ένας πρώην εραστής από το Σικάγο και έχει έρθει στην Αγγλία για να επιζητήσει Elsie πίσω. Κατέφυγε αρχικά νύχια του, γιατί ήταν μια επικίνδυνη εγκληματική, όπως Holmes έχει ανακαλύψει μέσω τηλεγραφική ερευνών στις ΗΠΑ. Όταν μια συνάντηση στο παράθυρο, όπου συνέβη η δολοφονία έγινε βίαια με την εμφάνισή Hilton Cubitt στο δωμάτιο, Slaney έβγαλε το όπλο του και πυροβόλησε πίσω σε Cubitt, οι οποίοι είχαν ήδη πυροβολήσει. Cubitt σκοτώθηκε και Slaney τράπηκαν σε φυγή. Προφανώς, Elsie αυτοκτόνησε στη συνέχεια. Slaney φαίνεται πραγματικά αναστατωμένος ότι Elsie έχει έρθει να βλάψουν. Η απειλητική φύση ορισμένων από χορό-man μηνύματά του εξηγείται από το Slaney χάνοντας την ψυχραιμία του σε προφανή απροθυμία Elsie να αφήσει τον άντρα της. Τα χρήματα που βρέθηκαν στην αίθουσα ήταν, προφανώς για να έχουν μια δωροδοκία για να κάνουν Slaney πάει μακριά.
Λίγα λόγια για τον κώδικα του Σέρλοκ Χόλμς.

Ο αριθμός ραβδιών είναι ένας πολύ ακατέργαστος τύπος σχεδίου, γενικά παριστάνεται με τη βοήθεια ανθρώπινων μορφών, ή και ζώων (παραδείγματος χάριν, ένας αριθμός ραβδιών απο σκύλους). Σε έναν αριθμό ραβδιών, το κεφάλι αντιπροσωπεύεται από έναν κύκλο. Ο λαιμός, τα όπλα, τα πόδια και ο κορμός αντιπροσωπεύονται από ενιαίες ευθείες γραμμές. Ο λαιμός και ο κορμός είναι διαφορετικά τμήματα μιας ευθείας γραμμής.

Οι αριθμοί ραβδιών είναι χαρακτηριστικά μια μορφή διανυσματικής τέχνης. Στους κινηματογράφους οι αριθμοί ραβδιών δημιουργούνται συχνά με τη βοήθεια του Macromedia. Οι αριθμοί ραβδιών χρησιμοποιούνται συχνά επειδή είναι εύκολη η αναπαράστασή τους. Αν και εμφανίζονται συχνά σε ένα 2D περιβάλλον, ο τρισδιάστατος κόσμος προσπαθεί να τον μιμηθεί μερικές φορές.

4.3. Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΤΟ Β' ΠΑΓΚΟΣΜΙΟ ΠΟΛΕΜΟ ΜΗΧΑΝΗ ΑΙΝΙΓΜΑ (ENIGMA)

Περιεχόμενα

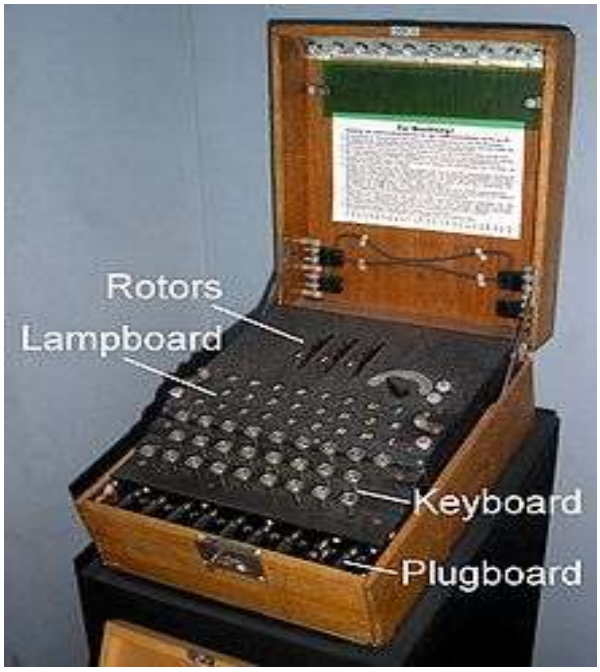
Η δεύτερη περίοδος της κρυπτογραφίας τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950. Καλύπτει, επομένως, τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων (λόγω της εξαιρετικά μεγάλης ανάγκης που υπήρξε για ασφάλεια κατά την μετάδοση ζωτικών πληροφοριών μεταξύ των στρατευμάτων των χωρών) αναπτύχθηκε η κρυπτογραφία τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές». Η κρυπτανάλυση τους, απαιτεί μεγάλο αριθμό προσωπικού, το οποίο εργαζόταν επί μεγάλο χρονικό διάστημα ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ. Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά την διάρκεια αυτής της περιόδου η κρυπτανάλυση τους είναι συνήθως επιτυχημένη. Οι Γερμανοί έκαναν εκτενή χρήση (σε διάφορες παραλλαγές) ενός συστήματος γνωστού ως Enigma.

Μια συσκευή Enigma είναι μια οποιαδήποτε συσκευή από μια οικογένεια συσχετιζόμενων ηλεκτρομηχανικών rotor συσκευών που χρησιμοποιήθηκαν για την κρυπτογράφηση και αποκρυπτογράφηση μυστικών μηνυμάτων. Η πρώτη συσκευή Enigma εφευρέθηκε από τον Γερμανό μηχανικό Arthur Scherbius στο τέλος του Πρώτου Παγκοσμίου Πολέμου. Αυτό το μοντέλο και οι παραλλαγές του χρησιμοποιήθηκαν εμπορικά από της αρχές της δεκαετίας του 1920, και υιοθετήθηκαν από στρατιωτικές και κυβερνητικές υπηρεσίες από διάφορες χώρες, πιο αξιοσημείωτα από την Ναζιστική Γερμανία πριν και κατά διάρκεια του Δευτέρου Παγκοσμίου Πολέμου. Αρκετά διαφορετικά μοντέλα συσκευών Enigma παρήχθησαν, αλλά τα Γερμανικά στρατιωτικά μοντέλα, τα *Wehrmacht* Enigmas, είναι τα πιο πολυσυζητημένα.

Το Αίνιγμα (Enigma), δεν ήταν, όμως, η μόνη συσκευή δημιουργίας κωδικοποιημένων μηνυμάτων. Αντίστοιχες είχαν κατασκευάσει η Siemens και η Lorenz. Η ύπαρξη αυτών των συσκευών προκάλεσε, εκ μέρους των Βρετανών, τη δημιουργία ειδικού υπολογιστή για το "σπάσιμο" των κωδικών τους (υπολογιστής Mark 1 Colossus, χρησιμοποιήθηκε ιδιαίτερα για την αποκρυπτογράφηση μηνυμάτων των συσκευών Lorenz SZ 40 και SZ 42 (Schlüsselzusatz), με τα οποία ο Χίτλερ επικοινωνούσε με τους στρατηγούς του).

Στην αρχή του πολέμου, η κρυπτογραφία της Βέρμαχτ θεωρούνταν άτρωτη. Η Enigma είχε τη δυνατότητα αμέτρητων συνδυασμών. Ομως, τον Μάιο 1941 το βρετανικό αντιτορπιλικό Bulldog αιχμαλώτισε ένα γερμανικό υποβρύχιο και απέσπασε από αυτό μια Enigma πριν από το υποβρύχιο αυτοανατιναχθεί. Με αυτό το λάφυρο, μερικοί από τους πιο φημισμένους μαθηματικούς επιστρατεύτηκαν στο εργαστήριο Μπλέτσλεϊ Παρκ, ώστε να σπάσουν το ναζιστικό κώδικα. ο πραγματικός σταρ στο Μπλέτσλεϊ Παρκ ήταν ο Αλαν Τιούρινγκ, ένας από τους μεγαλύτερους μαθηματικούς του αιώνα, και κατά πολλούς ο «πατέρας των υπολογιστών».

Η ομάδα του Μπλέτσλεϊ Παρκ αποκαλύφτηκε 30 χρόνια μετά τον πόλεμο και αυτό από μόνο του ήταν ένας λόγος να ξαναγραφτεί η Ιστορία. Σύμφωνα με μια πρόσφατη βιογραφία του Ουίνστον Τσόρτσιλ, όταν ο Βρετανός πρωθυπουργός στεκόταν αγέρωχος στη στέγη του Ναυαρχείου στο Λονδίνο, αψηφώντας τους πιθανούς βομβαρδισμούς, στην πραγματικότητα είχε λάβει μηνύματα Enigma που διαβεβαίωναν πως οι ναζί δεν θα έστελναν αεροπλάνα εκείνο το βράδυ...



ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΣΥΓΧΡΟΝΗ ΤΕΧΝΟΛΟΓΙΑ

5. ΚΩΔΙΚΟΠΟΙΗΣΗ ΠΛΗΡΟΦΟΡΙΩΝ

5.1. ΔΥΑΔΙΚΟ ΣΥΣΤΗΜΑ ΑΡΙΘΜΗΣΗΣ

Περιεχόμενα

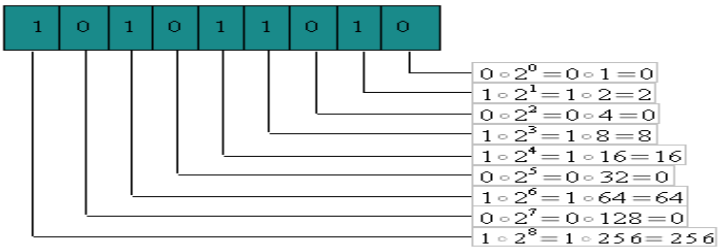
Το δυαδικό σύστημα αρίθμησης αναπαριστά αριθμητικές τιμές χρησιμοποιώντας δύο σύμβολα, το 0 και το 1. Πιο συγκεκριμένα, το δυαδικό είναι ένα θεσιακό σύστημα με βάση το δύο. Κάθε ψηφίο ανήκει σε μία τάξη μεγέθους μεγαλύτερη κατά ένα από αυτήν του ψηφίου στα δεξιά του. Έτσι, κάθε ψηφίο ενός δυαδικού αριθμού από δεξιά προς τ' αριστερά δηλώνει μονάδες, δυάδες, τετράδες, οκτάδες κ.ο.κ.

Η αποθήκευση και επεξεργασία των δεδομένων στους ηλεκτρονικούς υπολογιστές γίνεται ψηφιακά. Οδηγώντας, για παράδειγμα, την είσοδο ενός λογικού κυκλώματος με τάση ρεύματος μεγαλύτερη μιας συγκεκριμένης τιμής (π.χ +3 Volts)αναπαριστούμε το ψηφίο "1", ενώ οδηγώντας την είσοδο με τάση ρεύματος μικρότερη μιας συγκεκριμένης τιμής (π.χ +2 Volts) αναπαριστούμε το ψηφίο "0".

5.1.1. Μετατροπή από δεκαδικό στο δυαδικό.

Ξεκινάμε με το 1821 μια σειρά από ακέραιες διαιρέσεις με το 2 (χωρίς δεκαδικά) και σταματάμε την διαδικασία όταν το πηλίκο γίνει 0. Ας δούμε παρακάτω το παράδειγμα.

Ακέραια Διαίρεση	Ακέραιο Πηλίκο	Υπόλοιπο δυαδικό ψηφίο	Τι εκφράζει το υπόλοιπο
1821:2	=910	1	2^0
910:2	=455	0	2^1
455:2	=227	1	2^2
227:2	=113	1	2^3
113:2	=56	1	2^4
56:2	=28	0	2^5
28:2	=14	0	2^6
14:2	=7	0	2^7
7:2	=3	1	2^8
3:2	=1	1	2^9
1:2	=0	1	2^{10}



Ο αριθμός στο δυαδικό προκύπτει από την παραπάνω διαδικασία αν βάλουμε τα υπόλοιπα που βρήκαμε στην σειρά ξεκινώντας με από δεξιά προς τα αριστερά με το 1ο υπόλοιπο που βρήκαμε. Έτσι ο αριθμός είναι ο $11100011101_{(2)}$.

Η μετατροπή ενός αριθμού από το δεκαδικό σύστημα γίνεται με μια σειρά από συνεχόμενες διαιρέσεις με το 2. Από κάθε διαίρεση κρατάμε το ψηφίο που δείχνει το υπόλοιπο (0 ή 1) και διαιρούμε το πηλίκο ξανά. Η διαδικασία αυτή ολοκληρώνεται όταν το πηλίκο γίνει ίσο με 1. Τότε γράφουμε το τελευταίο πηλίκο και μετά κάθε υπόλοιπο που έχουμε υπολογίσει. Στο παράδειγμά μας το 23 γράφεται στο δυαδικό κάνοντας τις επόμενες πράξεις:23:2=11+111:2=5+15:2=2+12:2=1+0 έτσι το 23 γράφεται στο δυαδικό σαν 10111_2.

5.1.2. Μετατροπή από το δεκαδικό στο δυαδικό σύστημα

Έστω ότι έχουμε τον αριθμό 13_{10}, όπως στο αρχικό παράδειγμα. Γράφουμε τις δυνάμεις του 2, μέχρι να προκύψει αριθμός μικρότερος ή ίσος από τον ζητούμενο αριθμό, οπότε σταματάμε.

Θέση	τιμή
0	$2^0 = 1$
1	$2^1 = 2$
2	$2^2 = 4$
3	$2^3 = 8$

Στην προκειμένη περίπτωση ο ζητούμενος αριθμός είναι το 13, άρα σταματάμε στο 2^3=8, γιατί 2^4=16>13. Παρατηρούμε ότι ο αριθμός 2^3 χωράει μια φορά στο 13, άρα σημειώνουμε x1. Το αποτέλεσμα της αφαίρεσης είναι 5. Το 2^2 χωράει μια φορά στο 5 άρα σημειώνουμε x1. Μένει 1 , όμως το 2^1 δε χωράει στο ένα άρα σημειώνουμε x0. Τέλος το 2^0 χωράει μια φορά στο ένα , άρα σημειώνουμε x1.

13
-2^3 x1
5
-2^2 x1
1
-2^1 x0
1
-2^0 x1
0

Γράφοντας τις σημειώσεις στη σειρά από πάνω ως κάτω, προκύπτει ο αριθμός σε δυαδική μορφή. Δηλαδή, $1101_2 = 13_{10}$.

5.2. ΚΩΔΙΚΑΣ ASCII

Περιεχόμενα

Ο κώδικας ASCII (*American Standard Code for Information Interchange, Αμερικανικός Πρότυπος Κώδικας για Ανταλλαγή Πληροφοριών*), είναι ένα κωδικοποιημένο σύνολο χαρακτήρων του λατινικού αλφάβητου όπως αυτό χρησιμοποιείται σήμερα στην Αγγλική γλώσσα και σε άλλες δυτικοευρωπαικές γλώσσες. Χρησιμοποιείται για αναπαράσταση κειμένου στους υπολογιστές. σε συσκευές τηλεπικοινωνίας, καθώς και σε άλλες συσκευές που δουλεύουν με κείμενο. Οι περισσότερες σύγχρονες κωδικοποιήσεις χαρακτήρων βασίζονται στον ASCII, αν και υποστηρίζουν πολύ περισσότερους χαρακτήρες.

Ιστορικά, ο ASCII αναπτύχθηκε από τηλεγραφικούς κώδικες. Η πρώτη εμπορική χρήση του ήταν ως κώδικας ενός τηλέτυπου επτά bit της Bell. Σε σύγκριση με τους παλαιότερους τηλεγραφικούς κώδικες, ο προτεινόμενος κώδικας της Bell και ο ASCII ήταν διατεταγμένοι για πιο άνετη ταξινόμηση (π.χ. αλφαβητική σειρά) καταλόγων ενώ είχαν χαρακτηριστικά και για άλλες συσκευές εκτός από τηλέτυπα.

Ο ASCII περιλαμβάνει ορισμούς για 128 χαρακτήρες: 33 είναι μη εκτυπώσιμοι χαρακτήρες ελέγχου (πλέον κατά κύριο λόγο παρωχημένοι) που επηρεάζουν το πως γίνεται η επεξεργασία του κειμένου και των κενών, 94 είναι εκτυπώσιμοι χαρακτήρες, και το κενό που θεωρείται αόρατο γραφικό. Η πλέον κοινώς χρησιμοποιούμενη κωδικοποίηση χαρακτήρων στο διαδίκτυο ήταν η US-ASCII μέχρι τον Δεκέμβριο του 2007, οπότε ξεπεράστηκε από την κωδικοποίηση UTF-8.

ASCII Code Chart

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

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 0x20. 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.

Πολλοί από τους μη αλφαριθμητικούς χαρακτήρες τοποθετήθηκαν έτσι ώστε να αντιστοιχούν με την αλλαγμένη (*shifted*) θέση της γραφομηχανής. Έτσι τα #, $ και % τοποθετήθηκαν ώστε να αντιστοιχούν στα 3, 4, και 5 στη διπλανή στήλη. Οι παρενθέσεις ωστόσο, δεν ήταν δυνατόν να αντιστοιχούν στο 9 και 0, καθώς η αντίστοιχη θέση του 0 είχε καταληφθεί από τον χαρακτήρα κενού. Τελικώς επιλέχθηκαν οι θέσεις 8 και 9, καθώς πολλές ευρωπαϊκές γραφομηχανές είχαν εκεί τις παρενθέσεις. Το σύμβολο @ δεν χρησιμοποιούνταν στην ηπειρωτική Ευρώπη και έτσι η επιτροπή περίμενε ότι στη γαλλική εκδοχή θα αντικαθιστούνταν με το À, έτσι το @ τοποθετήθηκε στη θέση 0x40 δίπλα στο γράμμα A.

5.3. ΚΩΔΙΚΑΣ UNICODE

Περιεχόμενα

Στους υπολογιστές, το διεθνές πρότυπο Unicode στοχεύει στην κωδικοποίηση όλων των συστημάτων γραφής που χρησιμοποιούνται στον πλανήτη ώστε να γίνει δυνατή η αποθήκευση στη μνήμη ενός υπολογιστή το κείμενο μιας οποιασδήποτε γλώσσας συμπεριλαμβανομένων και συμβόλων επιστημών, όπως μαθηματικά, φυσική κτλ.

Η καθιέρωση του Unicode είναι ένα φιλόδοξο σχέδιο αφού σκοπεύει να αντικαταστήσει όλες τις υπάρχουσες κωδικοποιήσεις συνόλων χαρακτήρων, οι οποίες έχουν περιορισμούς που τις καθιστούν προβληματικές για χρήση σε πολυγλωσσικά υπολογιστικά συστήματα.

Παρά τα τεχνικά προβλήματα που έχουν παρουσιαστεί το Unicode έχει καθιερωθεί σαν το πιο πλήρες σύνολο χαρακτήρων και σαν η προτιμότερη κωδικοποίηση σε πολυγλωσσικό λογισμικό. Πολλά πρόσφατα πρότυπα όπως το XML, καθώς και λογισμικό συστήματος όπως λειτουργικά συστήματα, έχουν υιοθετήσει το Unicode για να αναπαριστούν εσωτερικά κείμενο.

5.3.1. Γέννηση και ανάπτυξη του προτύπου

Το πρότυπο Unicode είχε τον στόχο να ξεπεράσει τους περιορισμούς των παραδοσιακών κωδικοποιήσεων χαρακτήρων όπως αυτοί ορίζονται από το ISO 8859 πρότυπο που χρησιμοποιήθηκε ευρέως σε πολλές χώρες στον κόσμο αλλά παρουσίαζε προβλήματα ασυμβατότητας μεταξύ των διαφορετικών υλοποιήσεών του.

Πολλές παραδοσιακές κωδικοποιήσεις χαρακτήρων μοιράζονται ένα κοινό πρόβλημα στο ότι επιτρέπουν υποστήριξη δύο αλφαβήτων, συνήθως του Λατινικού και ενός τοπικού, αλλά δεν υποστηρίζουν πολλές γλώσσες.

Το Unicode κωδικοποιεί αφηρημένους χαρακτήρες προμηθεύοντας ένα κωδικό σημείο — σε καθέναν τους, όχι συγκεκριμένες μορφές που αυτοί μπορούν να πάρουν σε διάφορες γραμματοσειρές. Με άλλα λόγια το πρότυπο Unicode αφήνει το ανάλογο λογισμικό (πλοηγός Διαδικτύου, επεξεργαστής κειμένου) να "αποφασίσει" αυτό την οπτική αναπαράσταση (στύλ, μέγεθος, γραμματοσειρά) των χαρακτήρων.

Επίσης στο πρότυπο περιλαμβάνει και σχετικά θέματα όπως ιδιότητες χαρακτήρων, φόρμες κανονικοποίησης κειμένου, κατεύθυνση εμφάνισης(για γλώσσες που διαβάζονται και από τα δεξιά προς τα αριστερά όπως η Αραβική γλώσσα και τα Εβραϊκά.

5.3.2. Χρήση του Unicode

- ✓ Λειτουργικά συστήματα

Παρά τα τεχνικά προβλήματα τους περιορισμούς και την κριτική στη πορεία ,το Unicode έχει επικρατήσει σαν το κυρίαρχο σχήμα κωδικοποίησης χαρακτήρων. Τα Windows NT και οι απόγονοί του Windows 2000 και Windows XP κάνουν εκτεταμένη χρήση του σχήματος κωδικοποίησης UTF-16 για εσωτερική αναπαράσταση κειμένου. UNIX λειτουργικά συστήματα όπως GNU/Linux, Plan 9 από Bell Labs, BSDκαι Mac OS X έχουν υιοθετήσει το σχήμα UTF-8, σαν τη βάση για την αναπαράσταση πολυγλωσσικό κείμενο.

- ✓ Ηλεκτρονική αλληλογραφία

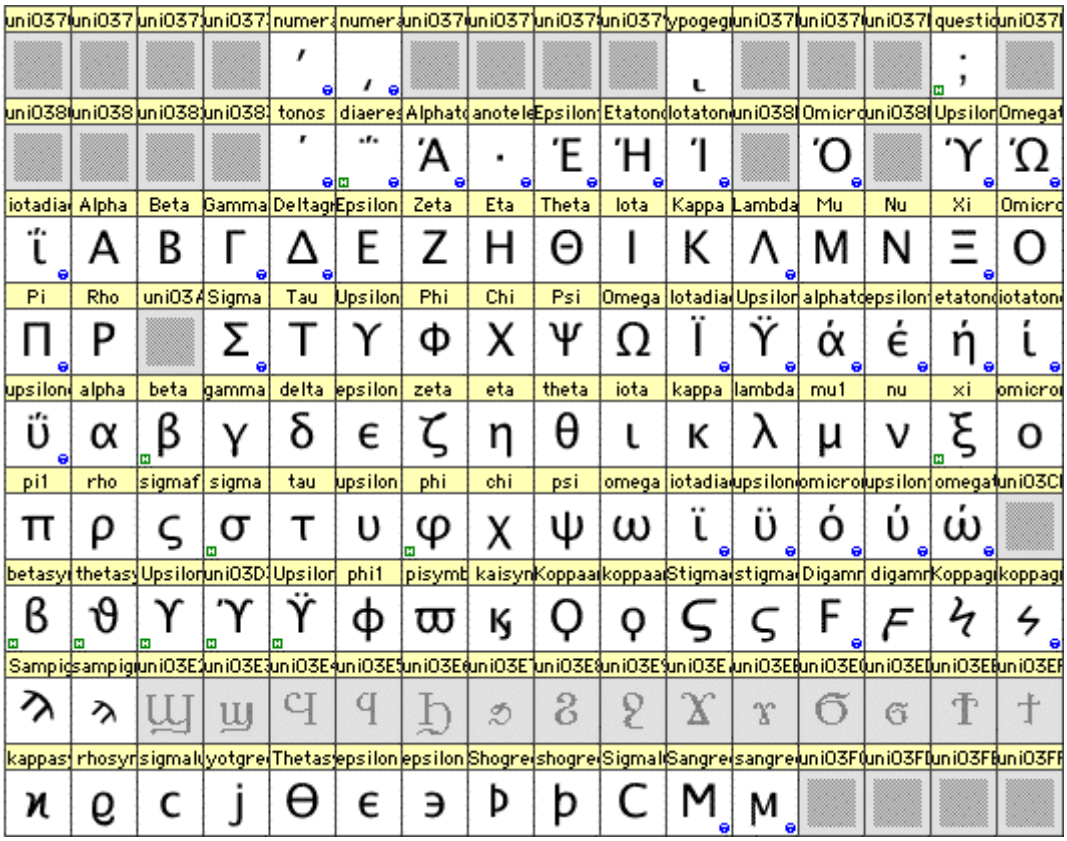
Το πρότυπο MIME ορίζει δυο διαφορετικούς μηχανισμούς για κωδικοποίηση όχι-ASCII χαρακτήρων στα μηνύματα ηλεκτρονικής αλληλογραφίας, e-mails, ανάλογα με το αν οι χαρακτήρες είναι στις επικεφαλίδες του ηλ. μηνύματος όπως πχ η επικεφαλίδα "Θέμα:" ή βρίσκονται στο κυρίως κείμενο του ηλεκτρονικού μηνύματος. 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 ηλ. αλληλογραφίας.

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

Το Unicode ορίζει δυο τρόπους απεικόνισης:

- Τις UTF (Unicode Transformation Format) κωδικοποιήσεις
- Και τις UCS (Universal Character Set) κωδικοποιήσεις

Αναπαράσταση ελληνικών χαρακτήρων σε Unicode



6. ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΥΠΟΛΟΓΙΣΤΕΣ

6.1. ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΚΑΙ ΑΛΓΟΡΙΘΜΟΙ

Περιεχόμενα

Στους συμμετρικούς αλγόριθμους το κλειδί κρυπτογράφησης μπορεί να υπολογιστεί από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση και το ανάποδο. Μάλιστα στις περισσότερες περιπτώσεις τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης είναι τα ίδια. Αυτοί οι αλγόριθμοι χρειάζονται την συμφωνία μεταξύ του αποστολέα και του παραλήπτη για το κλειδί που θα χρησιμοποιηθεί, 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.

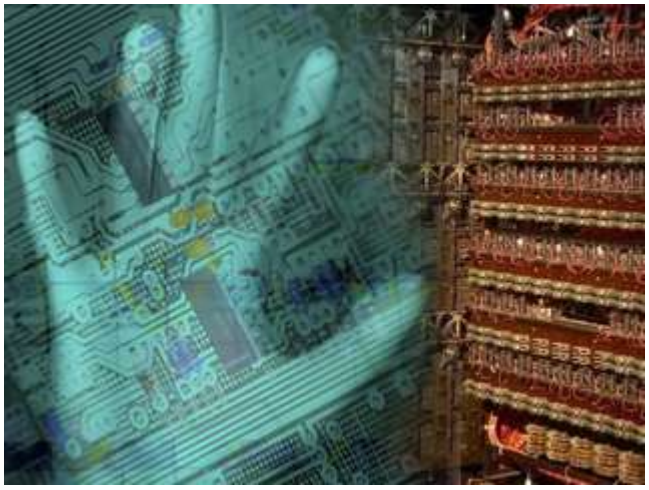
Παραδείγματα συμμετρικών αλγορίθμων είναι οι DES, IDEA, RC5 και SAFER.
Data Enrcyption - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτογράφηση Δεδομένων* και αναφέρεται στη χρήση μαθηματικών εργαλείων για την καθιέρωση της εμπιστοσύνης ανάμεσα στον αποστολέα και τον παραλήπτη (αποδέκτη) ενός μηνύματος. Η 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 κλειδί αποκωδικοποίησης.

Symmetric Encryption - 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.

6.1.1. Κρυπτογράφηση Συμμετρικού Κλειδιού

Ένα πρόβλημα το οποίο υφίσταται στους αλγόριθμους κρυπτογράφησης είναι η αδυναμία ανταλλαγής του κλειδιού με κάποιο ασφαλή τρόπο. Στην σύγχρονη ψηφιακή εποχή ο αποστολέας και ο παραλήπτης του μηνύματος πολλές φορές δεν γνωρίζονται, οπότε για την μετάδοση του κλειδιού από τον έναν στον άλλο θα πρέπει να υπάρχει κάποιο ασφαλές κανάλι επικοινωνίας. Φυσικά το διαδίκτυο δεν μπορεί να αποτελέσει κανάλι ασφαλούς επικοινωνίας, οπότε η χρήση της συμμετρικής κρυπτογράφησης σε εφαρμογές ηλεκτρονικού εμπορίου, ανταλλαγής ηλεκτρονικών μηνυμάτων κοκ ουσιαστικά δεν υφίσταται.

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



6.1.2. Λίστα Συμμετρικών Κρυπταλγορίθμων

Οι συμμετρικοί κρυπτογραφικοί αλγόριθμοι μπορούν να χωριστούν σε δύο διαφορετικές κατηγορίες με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων:

- Δέσμης (Block Ciphers), οι οποίοι χωρίζουν το μήνυμα σε κομμάτια και κρυπτογραφούν κάθε ένα από τα κομμάτια αυτά χωριστά.
- Ροής (Stream Ciphers), οι οποίοι κρυπτογραφούν μία ροή μηνύματος (stream) χωρίς να την διαχωρίζουν σε τμήματα.

6.2. ΑΛΓΟΡΙΘΜΟΙ ΣΥΜΜΕΤΡΙΚΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ Περιεχόμενα

6.2.1. DES (Data Encryption Standard)

DES είναι το ακρωνύμιο των λέξεων *Data Encryption Standard*. Αντιπροσωπεύει την τυποποίηση *Federal Information Processing Standard (FIPS)* 46-1 που επίσης περιγράφει τον *Data Encryption Algorithm (DEA)*. Αρχικά αναπτύχθηκε από την IBM, ενώ σημαντικό ρόλο στην ανάπτυξη του έπαιξε η NSA και το *National Institute of Standards and Technology (NIST)*. Είναι ο πιο γνωστός και παγκόσμια χρησιμοποιούμενος συμμετρικός αλγόριθμος. Ο DES είναι block cipher, με μέγεθος block 64 bit. Χρησιμοποιεί κλειδί 64 bits από τα οποία τα 8 αποτελούν bits ισοτιμίας.

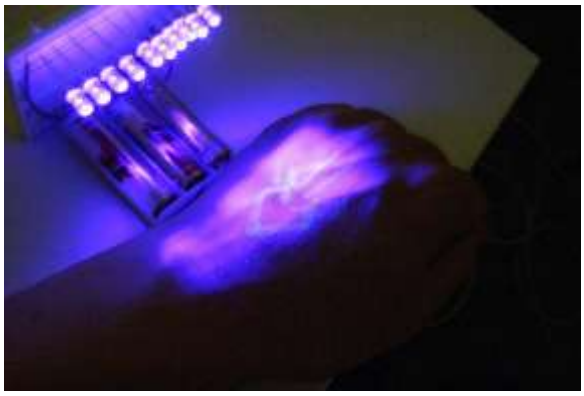
6.2.2. Triple-DES

Είναι μια παραλλαγή του DES όπου το μήνυμα κρυπτογραφείται και αποκρυπτογραφείται διαδοχικά με διαφορετικά κλειδιά για την ενίσχυση του βασικού αλγόριθμου. Υπάρχουν τέσσερις διαφορετικοί τρόποι για να επιτευχθεί αυτό:

- DES-EEE3 *(Encrypt-Encrypt-Encrypt)*:
- DES-EDE3 *(Encrypt-Decrypt-Encrypt)*

- DES-EEE2:
- DES-EDE2:

Από αυτούς τους τρόπους, ο πιο ασφαλής είναι ο DES-EEE3, με την τριπλή κρυπτογράφηση και τα τρία διαφορετικά κλειδιά.



6.2.3. DESX

Ο DESX είναι μια άλλη παραλλαγή του DES. Η διαφορά του DES και του DESX είναι ότι η είσοδος στο DESX περνάει από μια X-OR πράξη με ένα επιπλέον κλειδί 64 bits και ομοίως η έξοδος της κρυπτογράφησης.

AES (Advanced Encryption Standard)

Το ακρωνύμιο AES είναι ένας block cipher που προορίζεται να αντικαταστήσει τον DES.

DSS (Digital Signature Algorithm)

Το *Digital Signature Algorithm (DSS)* έχει καθιερωθεί σαν το επίσημο αλγόριθμο παραγωγής ψηφιακών υπογραφών της κυβέρνησης των Η.Π.Α.

Χρησιμοποιείται μόνο για παραγωγή ψηφιακών υπογραφών.

Το DSS έχει ολοκληρωθεί σε πολλά συστήματα ασφαλείας, αν και έχει λάβει πολλές άσχημες κριτικές. Τα κυριότερα θέματα κριτικής είναι η έλλειψη ευελιξίας, η αργή επαλήθευση των υπογραφών, η αδυναμία συνεργασίας με άλλο πρωτόκολλο πιστοποίησης ταυτότητας και τέλος ότι ο αλγόριθμος δεν είχε αποκαλυφθεί.

6.2.4. RC2, RC4, RC5

Ο RC2 είναι ένας block cipher με κλειδί μεταβλητού μήκους. Τα αρχικά σημαίνουν "Ron's Code" ή "Rivest's Cipher".Η ασφάλειά του είναι ανάλογη με το μήκος του κλειδιού. Είναι έως και τρεις φορές ταχύτερος από τον DES.

Ο RC4 είναι ένας stream cipher . Που έχει μεταβλητό μήκος κλειδιού και λειτουργεί στο επίπεδο του byte. Θεωρείται εξαιρετικά ασφαλής.

Ο RC5 είναι ένας block cipher. Έχει μεταβλητό μήκος κλειδιού και μεταβλητό μέγεθος block. Τυπικές επιλογές για το μέγεθος του block είναι 32 bits (για πειραματικές εφαρμογές), 64 bits και 128 bits.

IDEA (International Data Encryption Algorithm)

Ο IDEA είναι ένας block cipher. Χρησιμοποιεί block μεγέθους 64 bits και κλειδιά 128 bits.Αποτελεί ένα πολύ δυνατό αλγόριθμο που είναι απρόσβλητος από τα περισσότερα είδη επιθέσεων.

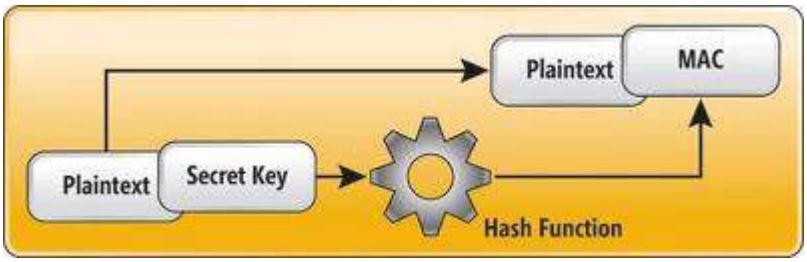
Blowfish

Ο Blowfish είναι ένας block cipher με μέγεθος block 64 bits και μεταβλητό μήκος κλειδιού, με μέγιστο μήκος 448 bits. Είναι σημαντικά ταχύτερος από τον DES και θεωρείται ακόμα ασφαλής αλγόριθμος.

6.3. Message Authentication Code (MAC)

Περιεχόμενα

Message Authentication Code είναι ένα κώδικας που συνοδεύει το μήνυμα και πιστοποιεί την ταυτότητα του αποστολέα και την ακεραιότητα του μηνύματος. Τα MACs υπολογίζονται και επαληθεύονται με το ίδιο κλειδί, έτσι ώστε να μπορούν να επαληθευθούν μόνο από τον προοριζόμενο παραλήπτη. Υπάρχουν τέσσερις τύποι MAC: (1) τα άνευ όρων ασφαλή, (2) τα βασιζόμενα σε hash functions, (3) τα βασιζόμενα σε stream ciphers και (4) τα βασιζόμενα σε block ciphers.



1. Ο άνευ όρων ασφαλής MAC βασίζεται στην κρυπτογράφηση με ένα one-time pad. Επειδή το κλειδί ενός one-time pad είναι πολύ μεγάλο, δεν χρησιμοποιούνται στην πράξη.
2. Τα MACs που βασίζονται σε hash functions χρησιμοποιούν ένα μυστικό κλειδί σε συνδυασμό με ένα hash function για να παράγουν το checksum που συνοδεύει το μήνυμα. Το κλειδί χρησιμοποιείται για να κρυπτογραφήσει το message digest του μηνύματος.
3. Τα MACs που βασίζονται σε stream ciphers. Στον αλγόριθμο που ανέπτυξαν, ένας δοκιμασμένος για την ασφάλεια του stream cipher, εφαρμόζεται στα δύο μισά ενός μηνύματος.
4. Τέλος, τα MAC μπορούν να δημιουργηθούν από block ciphers, όπως τον DES-CBC.

6.4. ΤΟ ΠΡΩΤΟΚΟΛΛΟ SSL

Περιεχόμενα

Το πρωτόκολλο SSL (Secure Sockets Layer) αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Η έκδοση 3.0 του πρωτοκόλλου κυκλοφόρησε από την Netscape το 1996 και αποτέλεσε την βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (Transport Layer Security), το οποίο πλέον τείνει να αντικαταστήσει το SSL. Τα δύο αυτά πρωτόκολλα χρησιμοποιούνται ευρέως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου.

Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών) εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και 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 .

Η μετάδοση πληροφοριών μέσω του διαδικτύου γίνεται ως επί το πλείστον χρησιμοποιώντας τα πρωτόκολλα TCP/IP (Transfer Control Protocol / Internet Protocol). Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου, όπως είναι για παράδειγμα το HTTP (προβολή ιστοσελίδων), το FTP (μεταφορά αρχείων) και το IMAP (email). Άρα λοιπόν αυτό που ουσιαστικά κάνει το SSL είναι να παίρνει τις πληροφορίες από τις εφαρμογές υψηλότερων επιπέδων, να τις κρυπτογραφεί και στην συνέχεια να τις μεταδίδει στο Internet προς τον Η/Υ που βρίσκεται στην απέναντι πλευρά και τις ζήτησε.

6.4.1. Τρόπος λειτουργίας

Το πρωτόκολλο SSL χρησιμοποιεί έναν συνδυασμό της κρυπτογράφησης δημοσίου και συμμετρικού κλειδιού. Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ πιο γρήγορη και αποδοτική σε σχέση με την κρυπτογράφηση δημοσίου κλειδιού, παρ' όλα 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 ταυτότητά του στον client χρησιμοποιώντας τεχνικές κρυπτογράφησης δημοσίου κλειδιού και στην συνέχεια επιτρέπει στον client και τον 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 επίσης στον client να αποδείξει την ταυτότητά του στον server. Αναλυτικότερα, η διαδικασία χειραψίας έχει ως εξής:

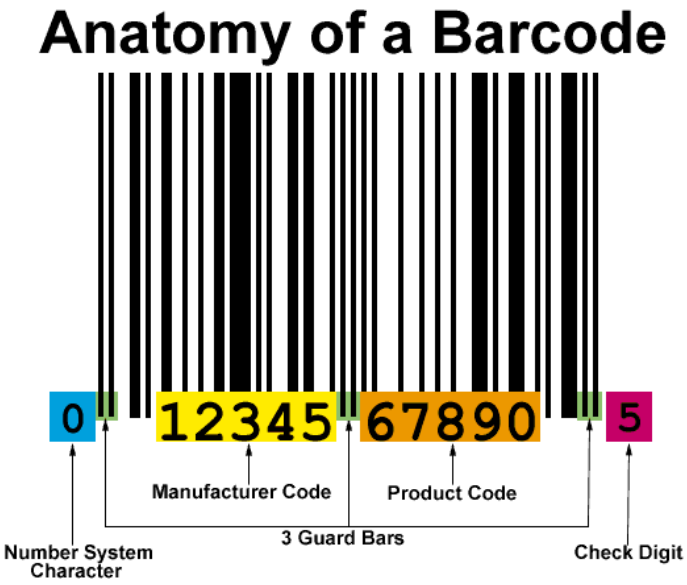
1. Αρχικά ο client στέλνει στον server την έκδοση του SSL που χρησιμοποιεί, τον επιθυμητό αλγόριθμο κρυπτογράφησης, μερικά δεδομένα που έχουν παραχθεί τυχαία και οποιαδήποτε άλλη πληροφορία χρειάζεται ο server για να ξεκινήσει μία σύνδεση SSL.
2. Ο server απαντά στέλνοντας παρόμοιες πληροφορίες με προηγουμένως 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 τον 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 στον 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. Στην συνέχεια ο server χρησιμοποιώντας το ιδιωτικό του κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα και να αποκτήσει το συμμετρικό κλειδί που θα χρησιμοποιηθεί για την σύνδεση.
5. Ο client στέλνει ένα μήνυμα στον server ενημερώνοντάς τον ότι είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
6. Ο server στέλνει ένα μήνυμα στον client ενημερώνοντάς τον ότι και αυτός είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.

Από εδώ και πέρα η χειραψία έχει ολοκληρωθεί και τα μηνύματα που ανταλλάσσουν τα δύο μηχανήματα (client - server) είναι κρυπτογραφημένα

7. ΑΛΛΕΣ ΕΦΑΡΜΟΓΕΣ

7.1. ΡΑΒΔΩΤΟΣ ΚΩΔΙΚΑΣ (BAR CODE)

Περιεχόμενα



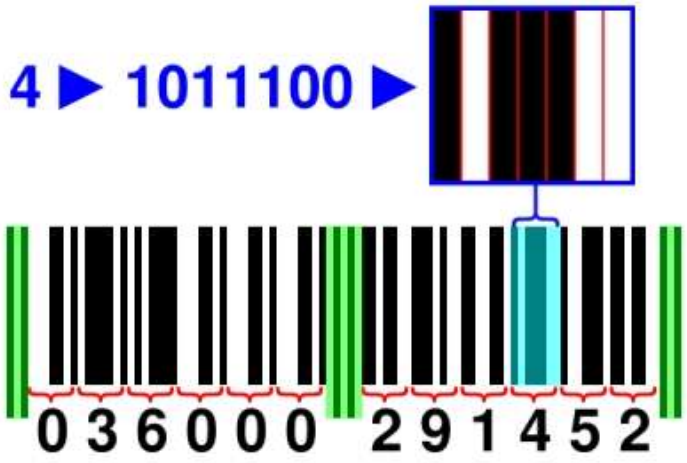
Ο ραβδωτός κώδικας είναι μια αναπαράσταση πληροφοριών η οποία μπορεί να αναγνωριστεί από μια μηχανή και βρίσκεται αναγραμμένος σε μία επιφάνεια, όπως για παράδειγμα σε προιόντα που πωλούνται σε καταστήματα λιανικής πώλησης, σε κάρτες αναγνώρισης και σε πακέτα ταχυδρομίων. Σκοπός της χρήσης του κώδικα είναι ο προσδιορισμός ενός συγκεκριμένου προιόντος, ενός ανθρώπου ή μιας τοποθεσίας.

Οι πληροφορίες που βρίσκονται στον γραμμωτό κώδικα έχουν την μορφή μιας μικρής εικόνας με γραμμές και διαστήματα. Όμως στην πραγματικότητα ο ένας ραβδωτός κώδικας είναι δυαδικός, είναι μια αλληλουχία από 0 και 1, και η αλληλουχια αυτή δημιουργεί ένα κείμενο το οποίο μεταφράζεται σε πολλές γλώσσες.

Στη πιο συνηθισμένη μορφή του, ο κώδικας αυτός αποτελείται από μία διαδοχή μαύρων και άσπρων λωριδών τυπωμένων πάνω σε κάποιο προιόν. Ο πιο κοινός τύπος κώδικας είναι ο EAN(European Article Numbering), ο οποίος αποτελείται από μια αριθμοσειρά 13 ψηφίων. Βέβαια υπάρχουν πάνω από 250 είδη ραβδωτών κωδικών.

Για να μπορούν να αναγνωστούν οι ραβδωτοί κώδικες απαιτείται η χρήση οπτικών σαρωτών. Για να πραγματοποιήσουν την ανάγνωση χρισιμοποιούν διάφορες τεχνολογίες. Οι πιο συνηθησμένες είναι τα λέιζερ και οι κάμερες. Η διαδικασία αναγνώρισης ενός τέτοιου κώδικα περιλαμβάνει τα παρακάτω βήματα: αρχικά ο κωδικός μεταφράζεται μέσα σε κλάσματα δευτερολέπτου από κάποιο σαρωτή σε γλώσσα Η/Υ. Η ανάγνωση συνιστάται στην αποκωδικοποίηση της ανάκλασης μιας δέσμης ακτινών λέιζερ που πέφτει πάνω στην ετικέτα του ραβδωτού κώδικα. Η

ανάκλαση είναι μεταβλητή, δηλαδή ξεχωριστή για κάθε προιόν. Στη συνέχεια οι σαρωτές αποκωδικοποιούν την μεταβλητη ανάκλαση και την μετατρέπουν σε αριθμούς ή γράμματα τα οποία ταυτίζονται ως προς το περιεχόμενο με τους χαρακτήρες που κωδικοποιήθηκαν με τον κώδικα αυτό.



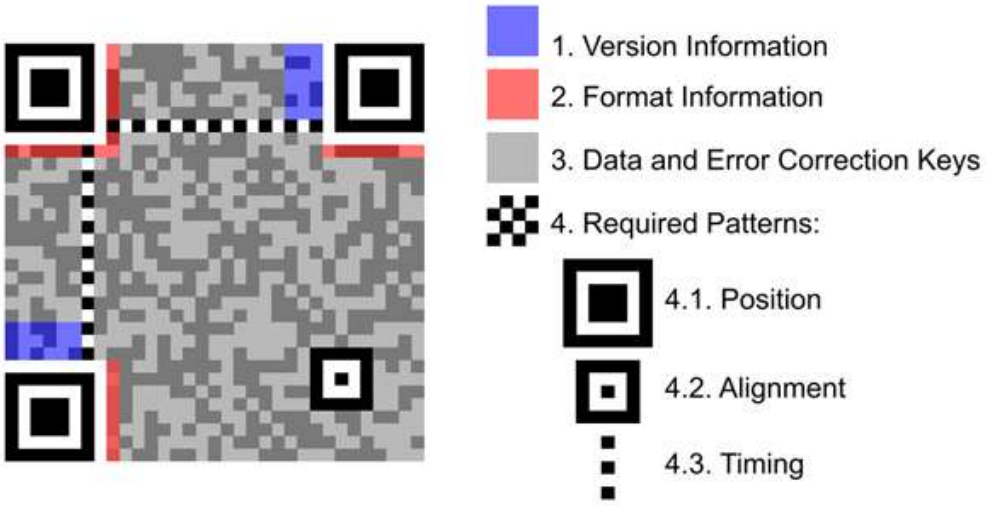
Μόνο οι 10 από τους 12 χαρακτήρες απαιτούνται για την ταυτοποίηση του προϊόντος. Οι 5 πρώτοι χαρακτήρες αντιστοιχούν στον παραγωγό και οι επόμενοι 5 στο συγκεκριμένο προιόν.

7.2. ΓΡΑΜΜΩΤΟΣ ΚΩΔΙΚΑΣ ΔΥΟ ΔΙΑΣΤΑΣΕΩΝ (QR CODE)

Περιεχόμενα

Ο κώδικας QR είναι ένας γραμμωτός κώδικας (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 QR κώδικας αποτελείται από μαύρες ενότητες διατεταγμένες σε ένα τετράγωνο μοτίβο σε λευκό φόντο και περιέχει πληροφορίες τόσο στην κάθετη όσο και στην οριζόντια κατεύθυνση, ενώ το bar code περιέχει δεδομένα σε μία μόνο κατεύθυνση (οριζόντια). Έτσι ο QR Κωδικός κατέχει πολύ μεγαλύτερο όγκο πληροφοριών από το ένα bar code.

Οι κώδικες QR χρησιμοποιούνται σήμερα σε ένα πολύ ευρύτερο πλαίσιο, συμπεριλαμβανομένων και εμπορικών εφαρμογών καθώς και ευκολία εντοπισμού προσανατολισμένων εφαρμογών που αποσκοπούν στους χρήστες κινητής τηλεφωνίας. Οι QR Κώδικες αποθηκεύουν τις διευθύνσεις και τα URL και μπορούν να εμφανιστούν σε περιοδικά, σε πινακίδες, λεωφορεία, κάρτες ή για κάθε αντικείμενο που μπορεί να χρειάζονται οι χρήστες πληροφορίες σχετικά με αυτό. Οι χρήστες μέσω της κάμερας του κινητού τηλεφώνου που είναι εξοπλισμένα με το σωστό λογισμικό ανάγνωσης μπορούν να σαρώσουν την εικόνα του κώδικα QR με αποτέλεσμα το πρόγραμμα περιήγησης (browser) του τηλεφώνου να ξεκινήσει και να ανακατευθύνει στο καταχωρημένο URL. Αυτή η ενέργεια της σύνδεσης από φυσικά αντικείμενα-λέξεις είναι γνωστό ως hardlink ή physical world hyperlinks.



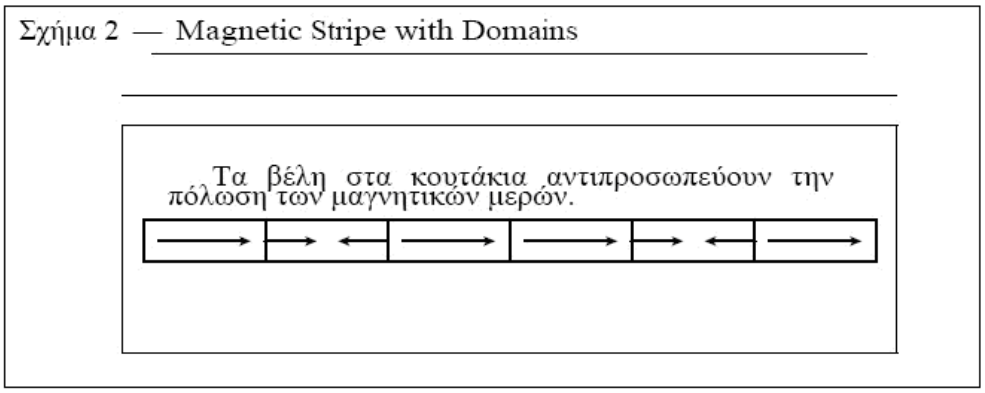
7.3. ΜΑΓΝΗΤΙΚΗ ΚΑΡΤΑ ΛΩΡΙΔΩΝ (Magnetic Stripe Card)

Περιεχόμενα

Αν μελετηθεί οπτικά μια πιστωτική κάρτα, πιθανότατα στο πίσω της μέρος θα υπάρχει μια μαύρη λωρίδα, περίπου μισή ίντσα πάχος, που διατρέχει όλη την κάρτα σε μήκος. Αυτή η μαύρη λωρίδα, που αποτελείται από τρεις διαδρομές των μαγνητικών μορίων που συνδέονται με το υπόστρωμα καρτών, είναι ο πυρήνας μιας μαγνητικής κάρτας λωρίδων. Οι μαγνητικές κάρτες λωρίδων εισήχθησαν για τρεις λόγους:

- Να αποθηκεύουν δεδομένα που είναι αναγνώσιμα από κατάλληλες συσκευές
- Να ελαχιστοποιούν την χρήση φυσικού χαρτιού σε χρηματικές συναλλαγές
- Να επιτρέπουν την αυτοματοποίηση διαφόρων λειτουργιών

Όπως εξηγήθηκε πριν, η μαγνητική λωρίδα αποτελείται από τρεις διαδρομές. Μια διαδρομή διαιρείται σε μικροσκοπικές περιοχές, κάθε περιοχή είναι το 1/75 μιας ίντσας. Για να αποθηκεύσουν τα στοιχεία όσον αφορά τη μαγνητική κάρτα λωρίδων, τα μόρια σε μια περιοχή είναι μαγνητισμένα με ένα ιδιαίτερο τρόπο (δείτε το σχήμα 2). Εάν μέσα σε μια περιοχή η πόλωση αλλάζει, υπάρχει μια αντιστροφή ροής και αντιπροσωπεύει το 1. Όταν η μαγνητική κάρτα λωρίδων διαβάζεται, βασισμένος στις αντιστροφές ροής, ο αναγνώστης παίρνει τα στοιχεία αποθηκευμένα σε αυτήν. Η μαγνητική λωρίδα που παρουσιάζεται στο σχήμα 2 θα διαβαζόταν σαν: 010010

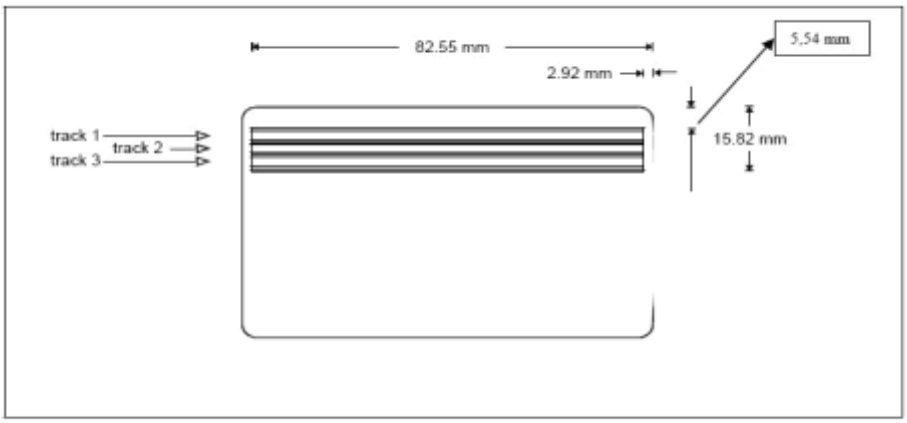


Μαγνητική λωρίδα

Η μαγνητική λωρίδα είναι περίπου τέσσερις ίντσες σε μήκος και αποτελείται από τρεις διαδρομές. Κάθε διαδρομή αποτελείται από περιοχές 1/75 της ίντσας σε μέγεθος. Κάθε περιοχή αντιπροσωπεύει ένα bit. Ως εκ τούτου, η συνολική ικανότητα μεταφοράς δεδομένων μιας μαγνητικής κάρτας λωρίδων είναι 900 bit.

Το κύριο πρόβλημα με τις μαγνητικές κάρτες λωρίδων είναι ότι τα στοιχεία μπορούν να διαβαστούν εύκολα και να αλλαχθούν από τον καθένα με την προϋπόθεση της πρόσβασης στο σωστό είδος εξοπλισμού. Ο όρος "card skimming" είναι ο όρος που δίνεται στη διαδικασία όπου τα στοιχεία μιας έγκυρης κάρτας αντιγράφονται bit ανά bit επάνω σε μια άλλη κάρτα. Οι αναγνώστες για τις μαγνητικές κάρτες λωρίδων κοστίζουν περίπου $100 ενώ οι κωδικοποιητές κοστίζουν ως $1000. Ως αποτέλεσμα αυτού του μειονεκτήματος, αυτές οι κάρτες δεν μπορούν να χρησιμοποιηθούν για την αποθήκευση των εμπιστευτικών πληροφοριών.

Στην επόμενη εικόνα φαίνονται αναλυτικά τα στοιχεία μιας μαγνητικής κάρτας.



Στοιχεία μαγνητικής κάρτας

Στον παρακάτω πίνακα βλέπουμε τα χαρακτηριστικά των τριών tracks (περιοχών) όπως ορίζεται στο πρότυπο.

Feature	Track 1	Track 2	Track 3
Ποσότητα χαρακτήρων	79 χαρακτήρες	40 χαρακτήρες	107 χαρακτήρες
Κωδικοποίηση	6-bit αλφαριθμητικό	4-bit BCD	4-bit BCD
Πυκνότητα δεδομένων	210 bpi	75 bpi	210 bpi
Εγγραφή	Δεν επιτρέπεται	Δεν επιτρέπεται	Επιτρέπεται
Χωρητικότητα σε bit	840	300	840
Ποσότητα σε bit	474	160	428

Χαρακτηριστικά των περιοχών (tracks)

7.4. ΑΣΦΑΛΕΙΑ ΣΥΝΑΛΛΑΓΩΝ

Περιεχόμενα

Ηλεκτρονικό κατάστημα (e-shop) είναι ο όρος που χρησιμοποιείται για να αναφερθεί κάποιος σε ένα Διαδικτυακό τόπο (site) μέσω του οποίου πραγματοποιούνται πωλήσεις διαφόρων ειδών.

Οι πολίτες της Ευρώπης και των Ηνωμένων Πολιτειών δαπανούν κάθε μήνα, κατά μέσο όρο, 25-32[1] ώρες χρησιμοποιώντας το Διαδίκτυο. Κατά τη διάρκεια αυτών των ωρών προσπελαύνουν χιλιάδες διαφορετικών υπηρεσιών του Διαδικτύου, όπως

online banking, e-shopping, και ιστοχώρους κοινωνικής δικτύωσης. Σχεδόν για κάθε υπηρεσία, οι χρήστες πρέπει να δημιουργήσουν ένα προσωπικό προφίλ χρήστη και, στη συνέχεια, τους δίνεται η δυνατότητα προσπέλασης της υπηρεσίας είτε μέσω μίας διαδικασίας εισαγωγής ονόματος χρήστη (username) και κωδικού (password) είτε, για περισσότερη ασφάλεια, μέσω ηλεκτρονικών πιστοποιητικών που βασίζονται στην κρυπτογραφία.

Οι τεχνολογίες Identity Mixer της IBM και U-Prove της Microsoft χρησιμοποιούν εξελιγμένους, αλλά και αποδοτικούς, κρυπτογραφικούς αλγορίθμους για να διασφαλίσουν ότι η ταυτότητα του ατόμου δεν θα εκτίθεται ποτέ σε ένα πάροχο υπηρεσιών χωρίς τη συγκατάθεση του ίδιου του χρήστη. Αυτές οι τεχνολογίες είναι κατάλληλες για μία ευρεία γκάμα εφαρμογών, όπως οι υπηρεσίες ασφάλισης,οι ηλεκτρονικές αγορές κ.α. .Επίσης έχουν λάβει πολλά βραβεία.

Σήμερα οι δύο τύποι αξιόπιστων τεχνολογιών ασφάλειας που είναι διαθέσιμα για ηλεκτρονικές αγορές είναι το SSL (Secure Socket Layer) και το SET (Secure Electronic Transaction).

Η τεχνολογία SET αναπτύχθηκε για την εξακρίβωση και γνησιότητας ταυτότητας μεταξύ εμπόρων και καταναλωτών πριν από μία ηλεκτρονική συναλλαγή. Συγκεκριμένα παρέχει εμπιστευτικότητα και ακεραιότητα των κρίσιμων μεταδιδόμενων πληροφοριών αλλά και πιστοποίηση ότι ο έμπορος μπορεί να δέχεται συναλλαγές με πιστωτική κάρτα μέσω συνεργασίας από κάποιο οικονομικό οργανισμό αλλά και πιστοποίηση ότι ο κάτοχος της κάρτας είναι πραγματικά ο νόμιμος και γνήσιος χρήστης του λογαριασμού. Το SET δημιουργήθηκε από τη Visa και τη MasterCard.

Το πρωτόκολλο SSL (Secure Sockets Layer) είναι σήμερα το παγκόσμιο standard στο Internet και η πλέον αξιόπιστη τεχνολογία για την ασφάλεια των συναλλαγών και το απόρρητο των επικοινωνιών μέσω του Internet σε παγκόσμια κλίμακα, καθώς και για την πιστοποίηση δικτυακών τόπων (web sites) στους δικτυακούς χρήστες και για την κρυπτογράφηση στοιχείων μεταξύ των δικτυακών χρηστών και των δικτυακών εξυπηρετητών (web servers). Μια κρυπτογραφημένη SSL επικοινωνία απαιτεί όλες τις πληροφορίες που αποστέλλονται μεταξύ ενός πελάτη και ενός εξυπηρετητή (server) να κρυπτογραφούνται από το λογισμικό αποστολής και να αποκρυπτογραφούνται από το λογισμικό αποδοχής, προστατεύοντας έτσι προσωπικές πληροφορίες κατά τη μεταφορά τους. Επιπλέον, όλες οι πληροφορίες που αποστέλλονται με το πρωτόκολλο SSL, προστατεύονται από ένα μηχανισμό που αυτόματα εξακριβώνει εάν τα δεδομένα έχουν αλλαχτεί κατά τη μεταφορά.

Το SSL ξεκινά την κωδικοποίηση από τα 40bit. Στο LivePay χρησιμοποιούμε κρυπτογράφηση στα 128bit η οποία είναι ένα τρισεκατομμύριο φορές πολυπλοκότερη, και άρα ασφαλέστερη για την προστασία των προσωπικών σας δεδομένων από την αντίστοιχη των 40bit.

Το SSL είναι σήμερα το παγκόσμιο standard στο Διαδίκτυο και προσφέρει στον ηλεκτρονικό επισκέπτη του web site, κρυπτογραφημένη SSL επικοινωνία 256 bit.
Το πρόθεμα "https" επιβεβαιώνει ότι η συναλλαγή είναι ασφαλής χωρίς να ξέρετε τίποτα για το μυστικό κλειδί. Η διαδικασία χρησιμοποιεί «public-key» αλγόριθμους και ξεχωρίζει δύο κλειδιά για την χρήση τους: το δημόσιο κλειδί που μοιράζεται με άλλους συνομιλητές για συναλλαγές και το άλλο που είναι ιδιωτικό και κρυφό, γνωστό μόνο από το χρήστη. Ο,τι κρυπτογραφείται με το «public-key», αποκαλύπτεται με το ιδιωτικό κλειδί ώστε μόνο αυτοί που πρέπει, να μπορούν να αποκαλύψουν το μήνυμα.

Το SSL χρησιμοποιεί και τα δύο κλειδιά για επίτευξη ισορροπίας ταχύτητας, ασφάλειας και πρακτικότητας. Οι αλγόριθμοι του μυστικού κλειδιού είναι πολύ ταχύτεροι και μπορούν να μεταφέρουν περισσότερα δεδομένα με ασφάλεια, συγκριτικά με τους αλγόριθμους του public-key. Αποφασιστικώς παράγοντας στην απόπειρα ''σπασίματος'' του SSL είναι το "μέγεθος" του μυστικού κλειδιού, που μετριέται σε bits. Τα περισσότερα browsers μπορούν να χρησιμοποιήσουν κλειδιά μεγέθους 128-bit, που προσφέρουν1038 δισεκατομμύρια πιθανά κλειδιά..

7.1.1. Πως δουλεύει ένα SSL certificate

- Ο πελάτης ζητά ασφαλές περιεχόμενο
- Το website σας παρουσιάζει το ιδιωτικό του πιστοποιητικό SSL.
- Ο πελάτης ελέγχει το πιστοποιητικό σας και παράγει ένα μοναδικό κλειδί
- Ο πελάτης εξάγει το δημόσιο κλειδί από το πιστοποιητικό σας και κρυπτογραφεί το μοναδικό κλειδί
- Ο πελάτης στέλνει το κρυπτογραφημένο κλειδί στο website σας
- Το website σας αποκρυπτογραφεί το κλειδί και οι δύο έχουν τώρα ένα κοινό κλειδί για την συναλλαγή
- Ο ιστοχώρος σας και ο πελάτης μπορούν τώρα να επικοινωνήσουν ασφαλώς.
- Το SSL ξεκινά την κωδικοποίηση από τα 40bit. Εμείς χρησιμοποιούμε κρυπτογράφηση στα 128bit η οποία είναι ένα τρισεκατομμύριο φορές πολυπλοκότερη, και άρα ασφαλέστερη για την προστασία των προσωπικών σας δεδομένων από την αντίστοιχη των 40bit.

7.1.2. 3D-Secure

Το 3-D Secure βασίζεται σε XML και χρησιμοποιείται ως ένα επιπλέον επίπεδο ασφάλειας για online συναλλαγές με πιστωτικές και χρεωστικές κάρτες για την εξακρίβωση της νόμιμης κατοχής τους. Δημιουργήθηκε από την Visa για τη βελτίωση της ασφάλειας των πληρωμών στο Διαδίκτυο και διατέθηκε στους πελάτες ως η υπηρεσία Verified by Visa. Οι υπηρεσίες που στηρίζονται στο πρωτόκολλο έχουν επίσης υιοθετηθεί από την MasterCard. Το 3-D Secure δεν πρέπει να συγχέεται με τον Κωδικό Ασφαλείας της κάρτας ο οποίος είναι ένας μικρός αριθμητικός κωδικός, τυπωμένος πάνω στην κάρτα.

7.1.3. Τι είναι οι υπηρεσίες Verified by Visa και MasterCard SecureCode

Οι υπηρεσίες Verified by Visa και MasterCard SecureCode έχουν σχεδιαστεί με βάση το πρωτόκολλο 3D-Secure για να μειώσουν τον κίνδυνο από τη μη εξουσιοδοτημένη χρήση της κάρτας ενός πελάτη, πιστοποιώντας τον κάτοχο της κάρτας κατά τη διενέργεια μιας online συναλλαγής σε ένα e-shop.

7.1.4. Διαδικασία ολοκλήρωσης μίας ηλεκτρονικής αγοράς με το σύστημα 3D Secure με απλά βήματα:

- Αφού επιλέξετε το προϊόν που επιθυμείτε, πληκτρολογείτε τα στοιχεία της πιστωτικής σας κάρτας στο κρυπτογραφημένο περιβάλλον, με κρυπτογράφηση 256 bit, στο περιβάλλον της Τράπεζας.
- Η Τράπεζα επικοινωνεί με το δίκτυο της Visa ή της MasterCard για να ελέγξει τόσο την κατάσταση της πιστωτικής κάρτας, όσο και αν τα στοιχεία της πιστωτικής κάρτας είναι εκείνα που τις αντιστοιχούν και αν συμμετέχει στο πρόγραμμα Verified by Visa και SecureCode by MasterCard.
- Η Visa ή MasterCard προωθεί τα παραπάνω στοιχεία στην εκδότρια Τράπεζα της κάρτας σας. Εκείνη επιβεβαιώνει τα παραπάνω στοιχεία ως αληθή στέλνοντας μήνυμα επικύρωσης στην Τράπεζα που διαθέτει το σύστημα για 3D Secure συναλλαγές.
- Εάν η κάρτα εμφανίζει status Verified by Visa ή SecureCode by MasterCard, τότε θα εμφανιστεί στον κάτοχο η αντίστοιχη φόρμα συμπλήρωσης κωδικού από την εκδότρια Τράπεζα.
- Η φόρμα θα περιέχει το κείμενο που είχατε γράψει ο ίδιος όταν εγγραφήκατε στο πρόγραμμα Verified by Visa ή SecureCode by MasterCard επιβεβαιώνοντας με αυτόν τον τρόπο ότι το μήνυμα που εμφανίζεται στο pop-up παράθυρο προέρχεται από την πραγματική εκδότρια Τράπεζα. Τέλος θα του ζητηθεί να εισάγει τον μυστικό κωδικό που γνωρίζει μόνο ο ίδιος και έχει στην κατοχή του αποκλειστικά για συναλλαγές μέσω διαδικτύου.
- Πληκτρολογείτε τον μυστικό κωδικό σας και ολοκληρώνετε επιτυχώς την συναλλαγή.
- Ένα αρχείο με το ιστορικό της συναλλαγής αποθηκεύεται στους servers της Visa ή MasterCard, με σκοπό την μελλοντική του χρήση ως αποδεικτικό επιτυχούς συναλλαγής.

7.5. ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ

Περιεχόμενα

Οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού. Ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Η διαφοροποίηση από την κρυπτογράφηση, έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού (ή κατατεμαχισμού -one way hash). Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου του μεγέθους του, παράγεται η «σύνοψή του», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη του μηνύματος (fingerprint ή message digest) είναι μία ψηφιακή αναπαράσταση του μηνύματος, είναι μοναδική για το μήνυμα και το αντιπροσωπεύει.

Η ψηφιακή υπογραφή αποτελείται από τρεις αλγόριθμους:

- Ο αλγόριθμος δημιουργίας δημόσιου και ιδιωτικού κλειδιού: Ο αλγόριθμος αυτός χρησιμοποιεί μια γεννήτρια τυχαίων αριθμών και με βάση αυτόν τον τυχαίο αριθμό δημιουργεί το δημόσιο και ιδιωτικό κλειδί (με το ιδιωτικό κλειδί δημιουργείται η ψηφιακή υπογραφή και με το δημόσιο κλειδί ελέγχεται η ψηφιακή υπογραφή).

- Ο αλγόριθμος προσθήκης ψηφιακής υπογραφής σε μηνύματα ή έγγραφα: Χρησιμοποιώντας το μήνυμα/έγγραφο και το ιδιωτικό κλειδί (το οποίο ανήκει μόνο σε αυτόν που υπογράφει το έγγραφο), δημιουργεί την ψηφιακή υπογραφή.

- Ο αλγόριθμος έλεγχου ψηφιακής υπογραφής μηνύματος ή εγγράφου: Χρησιμοποιώντας το μήνυμα/έγγραφο και το δημόσιο κλειδί (το δημόσιο κλειδί είναι διαθέσιμο σε όλους, και συσχετίζεται με το ιδιωτικό κλειδί και ανήκει αυτόν που υπέγραψε ψηφιακά το μήνυμα/έγγραφο), ελέγχει την αυθεντικότητα (ποιος το υπέγραψε) αλλά και ακεραιότητα (ότι το μήνυμα δεν παραποιήθηκε) του μηνύματος/εγγράφου.

7.1.5. Παράδειγμα

Έστω ότι η Alice και ο Bob θέλουν να επικοινωνήσουν μεταξύ τους και συγκεκριμένα η Alice θέλει να στείλει στον Bob ένα υπογεγραμμένο μήνυμα.

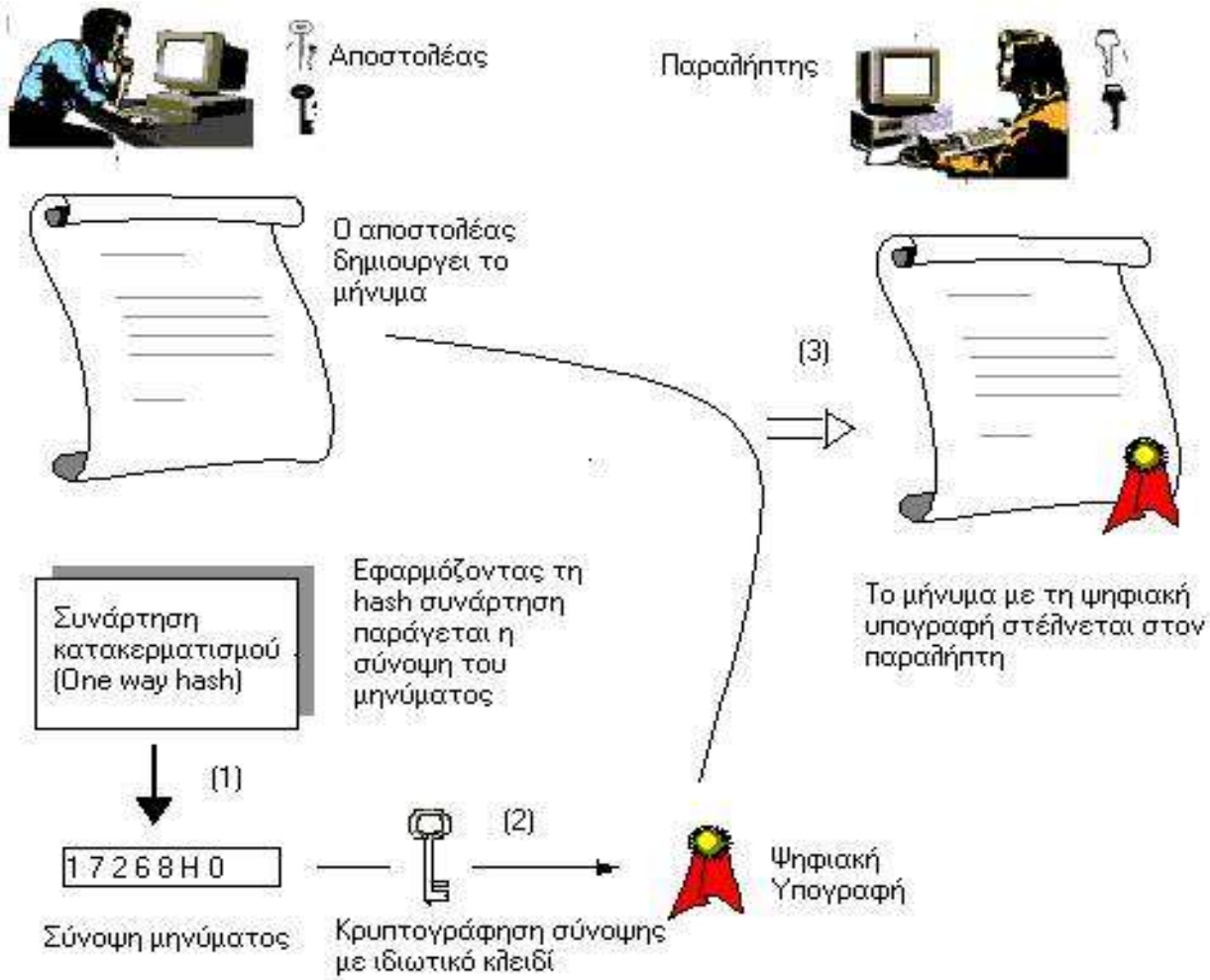
- Αρχικά η Alice και ο Bob θα πρέπει να συμφωνήσουν ποιον αλγόριθμο δημόσιου κλειδιού (ασυμμετρικής κρυπτογράφησης: π.χ. PGP, Digital Signature Standard) και ποιον αλγόριθμο κατατεμαχισμού (π.χ. MD5) θα χρησιμοποιήσουν.

- Και η Alice και ο Bob έχουν ζευγάρια δημοσίων και ιδιωτικών κλειδιών σύμφωνα με τον αλγόριθμο που επέλεξαν στο προηγούμενο βήμα. Θα πρέπει να ανταλλάξουν μεταξύ τους τα δημόσια κλειδιά τους.

- Η Alice θέλει να στείλει ένα υπογεγραμμένο μήνυμα στον Bob. Αρχικά θα περάσει το μήνυμα από τον αλγόριθμο κατατεμαχισμού που επέλεξαν στον πρώτο βήμα και θα παράγει την σύνοψη (digest) του μηνύματος.

- Η Alice θα κρυπτογραφήσει την σύνοψη με το ιδιωτικό κλειδί της και θα προσθέσει την κρυπτογραφημένη εκδοχή της στο τέλος του εγγράφου. Αν θέλει, μπορεί επίσης να προσθέσει και ένα πιστοποιητικό που πιστοποιεί ότι το δημόσιο κλειδί που θα χρησιμοποιηθεί από τον Bob αργότερα για την αποκρυπτογράφηση της υπογραφής ανήκει στην Alice (το πιστοποιητικό θα πρέπει να έχει εκδοθεί από ένα έμπιστο πάροχο υπηρεσιών πιστοποίησης). Θα αποστείλει στον Bob το τελικό έγγραφο (έγγραφο το οποίο έχει ψηφιακά υπογραφεί από την Alice - και ίσως περιέχει και ένα ψηφιακό πιστοποιητικό δημόσιου κλειδιού).

- Ο Bob θα ξεχωρίσει την κρυπτογραφημένη σύνοψη από το τέλος του εγγράφου και θα το αποκρυπτογραφήσει χρησιμοποιώντας το δημόσιο κλειδί της Alice (το έχει λάβει στον δεύτερο βήμα). Εφόσον η αποκρυπτογράφηση γίνει με επιτυχία γνωρίζει ότι η σύνοψη δεν έχει αλλοιωθεί και ότι ανήκει στην Alice. Κατόπιν θα πάρει το μήνυμα και θα το περάσει από τον αλγόριθμο κατατεμαχισμού που έχει συμφωνήσει στο πρώτο βήμα και θα συγκρίνει την σύνοψη που υπολόγισε ο ίδιος με την σύνοψη που αποκρυπτογράφησε από την ψηφιακή υπογραφή. Αν οι συνόψεις είναι ίδιες, ο Bob γνωρίζει ότι το αρχικό μήνυμα δεν έχει αλλοιωθεί. Αν θέλει να βεβαιωθεί ότι το δημόσιο κλειδί που χρησιμοποίησε ανήκει πραγματικά στην Alice θα διαβάσει το ψηφιακό πιστοποιητικό της Alice.


Αποστολέας
Παραλήπτης
Ο αποστολέας δημιουργει το μήνυμα
(3)
Συνάρτηση κατακερματισμού (One way hash)
Εφαρμόζοντας τη hash συνάρτηση παράγεται η σύνοψη του μηνύματος
Το μήνυμα με τη ψηφιακή υπογραφή στέλνεται στον παραλήπτη
(1)
17268H0
(2)
Ψηφιακή Υπογραφή
Σύνοψη μηνύματος
Κρυπτογράφηση σύνοψης με ιδιωτικό κλειδί

ΠΑΡΑΡΤΗΜΑ

4η Δραστηριότητα

Η μαγεία των αναποδογυρισμένων χαρτιών – Αναγνώριση & Διόρθωση σφαλμάτων

Περίληψη

Όταν τα δεδομένα αποθηκεύονται σε έναν δίσκο ή μεταφέρονται από τον έναν υπολογιστή στον άλλο, εμείς προϋποθέτουμε πως δεν μεταβάλλονται, κατά τη διάρκεια της διαδικασίας. Όμως, τα πράγματα μερικές φορές δεν πάνε έτσι και τα δεδομένα αλλοιώνονται κατά λάθος. Αυτή η δραστηριότητα δείχνει ένα μαγικό κόλπο για να μπορούμε να ανακαλύψουμε ποια δεδομένα υπέστησαν βλάβη και να μπορέσουμε να τα διορθώσουμε.

Αντιστοιχία με το σχολικό πρόγραμμα

✔ Μαθηματικά: Αριθμοί επιπέδου 3 και άνω. Εξερευνώντας τον Υπολογισμό (*computation*) και την Εκτίμηση (*estimation*).
✔ Άλγεβρα επιπέδου 3 και άνω. Εξερευνώντας τα Patterns και τις Σχέσεις.

Απαιτούμενες δεξιότητες

✔ Να ξέρεις να μετράς
✔ Να αναγνωρίζεις τους μονούς και τους ζυγούς αριθμούς

Ηλικία

✔ Από 9 χρονών και πάνω

Υλικά

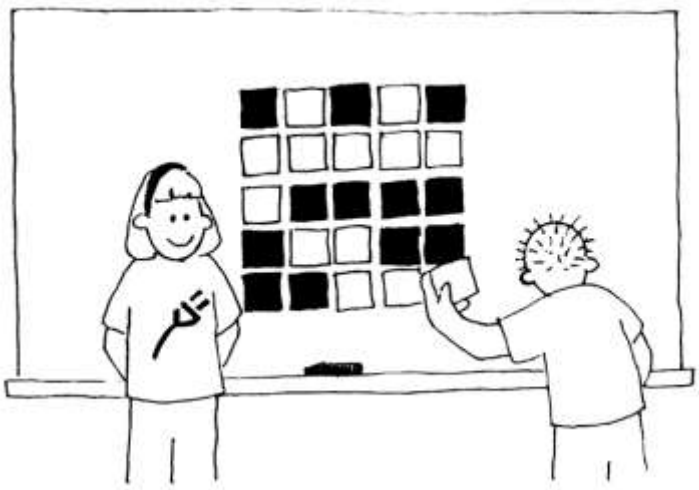
✔ 36 μαγνητάκια "για ψυγείο", χρωματισμένα μόνο από τη μία πλευρά.
✔ Μία μεταλλική επιφάνεια όπου να κολλήσουμε τα μαγνητάκια (συνήθως οι λευκοί πίνακες ταιριάζουν).
Κάθε ζεύγος μαθητών πρέπει να έχει:
✔ 36 ίδια χαρτιά, χρωματισμένα από μία μόνο πλευρά.
Μπορεί να φωτοτυπηθεί ελεύθερα για διδακτική χρήση.

Το "μαγικό κόλπο"

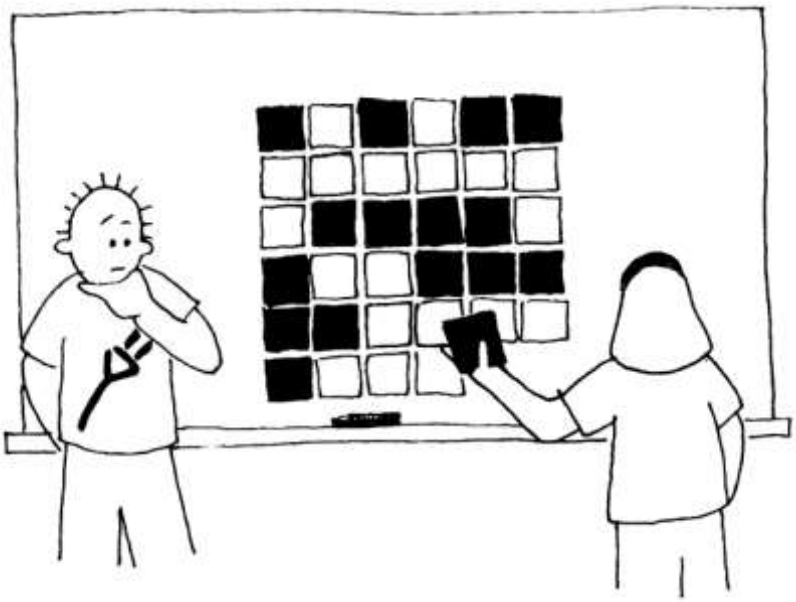
Επίδειξη

Αυτή είναι η ευκαιρία σας να γίνετε μάγος.
Χρειάζεστε ένα μάτσο με ίδια χαρτιά, χρωματισμένα κατά διαφορετικό τρόπο από τις δύο πλευρές τους (μπορείτε να τα φτιάξετε, κόβοντας ένα χαρτονάκι με χρώμα από τη μία μόνο πλευρά. Για να δείξετε τη μέθοδο, είναι πιο εύκολο να χρησιμοποιήσετε επίπεδες μαγνητικές κάρτες με διαφορετικά χρώματα στις δύο πλευρές τους. Τα μαγνητάκια "για ψυγείο" είναι ό,τι πρέπει.

1. Επιλέξτε έναν μαθητή/ μαθήτρια και ζητήστε του/ της να τοποθετήσει τα χαρτιά φτιάχνοντας ένα τετράγωνο 5x 5, διαλέγοντας τυχαία τις πλευρές των ορατών χαρτιών.



Εσείς προσθέστε "αδιάφορα" μία σειρά και μία στήλη επί πλέον, "έτσι, για να τα κάνουμε λίγο πιο δύσκολα".



Αυτά τα επιπλέον χαρτιά, είναι το κλειδί για το κόλπο μας. Δεν θα τα βάλετε τυχαία, αλλά με τέτοιο τρόπο, ώστε όλες οι σειρές και οι στήλες να έχουν ζυγό αριθμό χρωματιστών καρτών.

2. Ζητήστε τώρα από έναν άλλο μαθητή/ μαθήτρια να γυρίσει μόνο ένα χαρτί, ενώ εσείς του καλύπτετε τα μάτια. Η σειρά και η στήλη όπου αναποδογυρίστηκε το χαρτί, περιέχουν πλέον έναν μονό αριθμό χρωματιστών χαρτιών, και από αυτό και μόνο, μπορείτε να μαντέψετε το αλλαγμένο χαρτί.

Θα μπορέσουν οι μαθητές να αντιληφθούν πως λειτουργεί το κόλπο;

Διδάξτε το κόλπο στους μαθητές:

1. Δουλεύοντας ανά ζεύγη, οι μαθητές βάζουν τα χαρτιά να σχηματίζουν ένα τετράγωνο 5x5.
2. Πόσα χρωματιστά χαρτιά υπάρχουν σε κάθε σειρά και σε κάθε στήλη; Είναι μονός ή ζυγός αριθμός; Να θυμάστε ότι το μηδέν θεωρείται ως ζυγός αριθμός.
3. Τώρα προσθέστε ένα 6ο χαρτί σε κάθε σειρά, ούτως ώστε ο αριθμός των χρωματιστών χαρτιών σε κάθε σειρά, να είναι ζυγός. Αυτό το επιπρόσθετο χαρτί λέγεται χαρτί "ισότητας" ("parity card").
4. Προσθέστε μία 6η σειρά στο τέλος, έτσι που η κάθε στήλη να περιέχει ζυγό αριθμό χρωματιστών χαρτιών.
5. Τώρα αναποδογυρίστε ένα χαρτί. Τι παρατηρείτε για τη σειρά και τη στήλη; (θα έχουν μονό αριθμό χρωματιστών χαρτιών). Τα χαρτιά "ισότητας" χρησιμεύουν ακριβώς για να ειδοποιούν όταν γίνεται ένα λάθος.
6. Τώρα αλλάξτε ρόλους, για την επίδειξη του "κόλπου".

Προτάσεις επέκτασης:

1. Δοκιμάστε με χρήση άλλων αντικειμένων. Κάθε τι που διαθέτει δύο "καταστάσεις" ταιριάζει. Για παράδειγμα, μπορείτε να χρησιμοποιήσετε χαρτιά τράπουλας (κόκκινα ή μαύρα), νομίσματα (κορόνα ή γράμματα) ή χαρτιά με το 0 από τη μία, και το 1 από την άλλη, ούτως ώστε να συσχετιστούν με τη δραστηριότητα των δυαδικών αριθμών.
2. Τι θα συμβεί αν γυρίσουμε 2 ή παραπάνω χαρτιά; (δεν είναι πάντα εφικτό να ξέρουμε ποια 2 χαρτιά αλλαχθήκανε, αν και γενικά, είναι δυνατόν να πούμε ότι κάτι άλλαξε. Συνήθως, μπορούμε να το εντοπίσουμε σε 1 ή 2 ζεύγη χαρτιών, μέσα στα οποία θα είναι και τα αναποδογυρισμένα. Αναποδογυρίζοντας 4 χαρτιά, μπορεί όλα τα bit ισότητας να είναι, σωστά, ακόμη και μετά την αλλαγή, οπότε το σφάλμα δεν θα εντοπισθεί).
3. Μία άλλη ενδιαφέρουσα άσκηση συνίσταται στην ανάλυση του τελευταίου χαρτιού, κάτω δεξιά. Με βάση το πως περιγράφηκε η μέθοδος, αυτό το χαρτί λαμβάνεται υπ' όψη στον υπολογισμό, ώστε να έχουμε ζυγό αριθμό χρωματιστών χαρτιών στη στήλη των χαρτιών ισότητας της κάθε σειράς. Είναι κι' αυτό το ίδιο ένα χαρτί ισότητας για την τελευταία σειρά; (Ναι, πάντοτε).
4. Σ' αυτή την άσκηση χρησιμοποιήσαμε την ισότητα (ο αριθμός των χρωματιστών χαρτιών σε κάθε σειρά και στήλη πρέπει να είναι ζυγός). Αν, αντιθέτως, χρησιμοποιούσαμε την ανισότητα; (ο αριθμός των χρωματιστών χαρτιών στις σειρές και τις στήλες πρέπει να είναι μονός). Μπορούμε να κάνουμε τον ίδιο συλλογισμό, όπως και στο προηγούμενο σημείο; το τελευταίο κάτω δεξί χαρτί, ξαναφτιάχνει την ανισότητα, τόσο της τελευταίας σειράς όσο και της τελευταίας στήλης; (Μπορεί να συμβεί, αλλά σε γενικές γραμμές, λειτουργεί όταν ο αριθμός των σειρών και ο αριθμός των στηλών είναι ίσοι ή, τουλάχιστον και οι δύο ζυγοί ή μονοί. Λειτουργεί για την περίπτωση του 5x5, αλλά και για το 5x9 ή 4x6, αλλά όχι για το 3x4).

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Διπλωματική εργασία <Οι έξυπνες κάρτες και οι δυνατότητες εφαρμογών τους σε εκπαιδευτικά ιδρύματα> Κοντός Ευάγγελος
- http://www.dimitriskaranikolas.gr
- http://www.teicrete.gr
- http://en.wikipedia.org
- http://www.mathdemos.org
- hellenica.de
- http://www.krassanakis.gr
- http://www.google.com
- Computer Science Unplugged (http://csunplugged.org/)
- Θεματική Ενότητα ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ - Τόμος Γ'- Κρυπτογραφία - Βασίλειος Ζορκάδης – Ε. Α. Π. - Πάτρα 2002

Η Εργασία αυτή πραγματοποιήθηκε από τους μαθητές της Α΄Λυκείου :

ΟΜΑΔΑ 1η	**ΑΛΕΞΙΟΥ ΣΩΤΗΡΗΣ**
	ΜΑΥΡΟΜΑΤΗΣ ΙΟΡΔΑΝΗΣ
	ΚΥΔΩΝΗΣ ΘΑΝΟΣ
	ΠΟΥΛΚΑΣ ΓΙΑΝΝΗΣ
ΟΜΑΔΑ 2η	ΓΙΑΝΝΑΚΟΣ ΓΙΩΡΓΟΣ
	ΜΙΜΙΛΙΔΗ ΔΗΜΗΤΡΑ
	ΚΙΟΥΡΤΖΗ ΕΛΕΑΝΝΑ
	ΚΩΤΗ ΚΛΕΛΙΑ
	ΜΑΖΟΥΛΟΥΚΤΣΗ ΔΗΜΗΤΡΑ
ΟΜΑΔΑ 3η	ΔΗΜΗΤΡΟΠΟΥΛΟΥ ΕΥΗ
	ΔΗΜΗΤΣΑΚΗ ΚΑΤΙΑ
	ΜΕΝΤΕΚΙΔΗΣ ΓΙΩΡΓΟΣ
	ΜΠΑΡΜΠΑΚΥΡΙΑΚΟΥ ΞΕΝΙΑ
ΟΜΑΔΑ 4η	ΜΑΝΟΣ ΝΙΚΟΣ
	ΡΕΓΚΟΣ ΓΙΑΝΝΗΣ
	ΠΑΠΑΔΟΠΟΥΛΟΥ ΣΩΤΗΡΙΑ
	ΠΕΤΑΛΑ ΝΑΓΙΑ