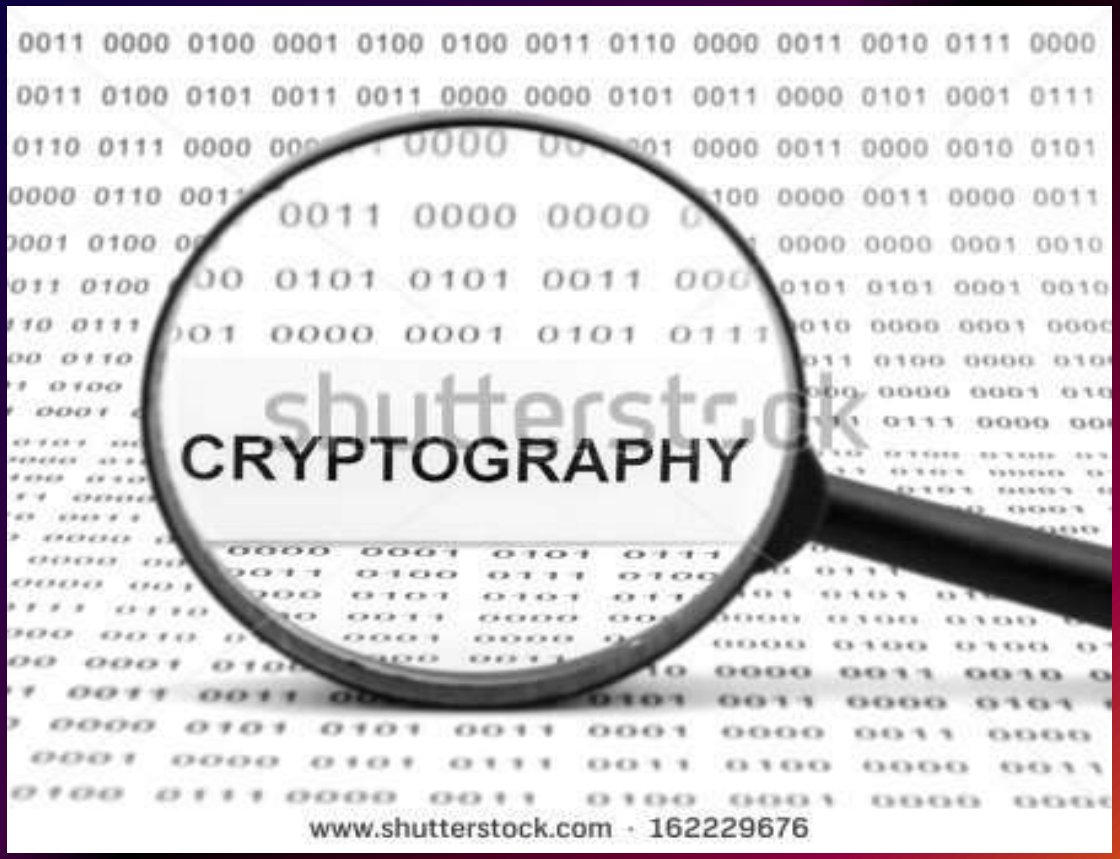
Κρυπτογραφία - Cryptography



ΠΕΡΙΛΗΨΗ

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

ΟΡΙΣΜΟΣ

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

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

Ιστορικά η κρυπτογραφία χρησιμοποιήθηκε για τη μετατροπή της πληροφορίας μηνυμάτων από μια κανονική, κατανοητή μορφή σε έναν «γρίφο», που χωρίς τη γνώση του κρυφού μετασχηματισμού θα παρέμενε ακατανόητος. Κύριο χαρακτηριστικό των παλαιότερων μορφών κρυπτογράφησης ήταν ότι η επεξεργασία γινόταν πάνω στην γλωσσική δομή του μηνύματος.

Στις νεότερες μορφές η κρυπτογραφία κάνει χρήση του αριθμητικού ισοδύναμου (πίνακας αντιστοίχησης γραμμάτων με αριθμούς), ενώ η έμφαση έχει μεταφερθεί σε διάφορα πεδία των μαθηματικών (π.χ διακριτά μαθηματικά, θεωρία αριθμών, θεωρία πληροφορίας, στατιστική και συνδυαστική ανάλυση).

Ιστορική αναδρομή

- **ΙΕΡΟΓΛΥΦΙΚΑ**

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

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

Ιερογλυφικά

ΓΡΑΜΜΙΚΗ ΓΡΑΦΗ Α΄

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

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

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

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

Ο δίσκος της Φαιστού

ΓΡΑΜΜΙΚΗ ΓΡΑΦΗ Β΄

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

Γραμμική γραφή Β

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

Η κρυπτογραφία στους Ελληνορωμαϊκούς χρόνους

- **ΣΠΑΡΤΙΑΤΙΚΗ ΣΚΥΤΑΛΗ**

Η πρώτη σπαρτιατική σκυτάλη εμφανίστηκε τον 5ο αιώνα π.Χ.

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

Η Σπαρτική Σκυτάλη

➢ Ο ΚΩΔΙΚΑΣ ΤΟΥ ΠΟΛΥΒΙΟΥ

Στον Πολύβιο αποδίδεται ένα χρήσιμο εργαλείο στην τηλεγραφία, το οποίο είναι χρήσιμο για την αποστολή κωδικοποιημένων γραμμάτων. Στην ιδέα αυτή επίσης στηρίζονται η κρυπτογραφία και η στενογραφία. Το εργαλείο αυτό είναι γνωστό ως το «Τετράγωνο του Πολύβιου». Πρόκειται για ένα τετράγωνο 5Χ5, διαιρεμένο σε 25 μικρότερα ίσα τετραγωνάκια, όπου τοποθετούνται με τη σειρά οι χαρακτήρες της αλφαβήτου, από αριστερά προς τα δεξιά και από τα πάνω προς τα κάτω. Στη συνέχεια, οι σειρές και οι στήλες αριθμούνται οριζοντίως και καθέτως, συνήθως με τους αριθμούς από 1 έως 5.

Έτσι, το κάθε ζεύγος 2 αριθμών αντιστοιχεί σε ένα συγκεκριμένο γράμμα και με τον τρόπο αυτό μπορεί να συνταχθεί κρυπτογραφικά ολόκληρη επιστολή. Το τετράγωνο του Πολυβίου ή αλλιώς Σκακιέρα του Πολυβίου είναι ένας τρόπος που εφευρέθηκε από τον Πολύβιο και χρησιμοποιήθηκε από τους Αρχαίους Έλληνες. Ο λόγος που ο Πολύβιος δημιούργησε αυτόν τον πίνακα δεν ήταν άλλος παρά να δημιουργήσει μια μέθοδο που θα μπορούσε με απλό σχετικά τρόπο να μεταδώσει πληροφορίες μεταξύ απομακρυσμένων σημείων. 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 τετράγωνο του Πολύβιου

➢ Ο ΚΩΔΙΚΑΣ ΤΟΥ ΚΑΙΣΑΡΑ

Στους Ελληνορωμαϊκούς χρόνους η πρώτη μέθοδος υποκατάστασης γραμμάτων για στρατιωτικούς σκοπούς εμφανίστηκε στους γαλατικούς πολέμους. Σήμερα το σύστημα κρυπτογράφησης που στηρίζεται στην αντικατάσταση των γραμμάτων του αλφάβητου με άλλα που βρίσκονται σε καθορισμένο αριθμό θέσης πριν ή μετά λέγεται κρυπτοσύστημα αντικατάστασης του Καίσαρα.

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

Ο κώδικας του Καίσαρα

Η κρυπτογραφία στο Μεσαίωνα

- **ΤΟ ΧΕΙΡΟΓΡΑΦΟ ΒΟΪΝΙΤΣ**

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

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

Χειρόγραφο Βόινιτς

ΚΡΥΠΤΟΓΡΑΦΙΑ - ΠΡΩΤΟΙ ΑΛΓΟΡΙΘΜΟΙ

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

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

Τα πρώτα συνοπτικά λεξιλόγια σιγά-σιγά αναπτύχθηκαν και χρησιμοποιήθηκαν για αρκετούς αιώνες στις διπλωματικές συνομιλίες σε όλες σχεδόν τις Ευρωπαϊκές κυβερνήσεις. Ο Trithemius, το 1510, έγραψε την “Polygraphia”, την πρώτη εκδιδόμενη εργασία για την κρυπτογραφία. Για πρώτη φορά παρουσίασε την ιδέα ενός τετραγώνου, στο οποίο η αλφαβήτα, μεταφερόταν σε ένα προκαθορισμένο αριθμό διαστημάτων.

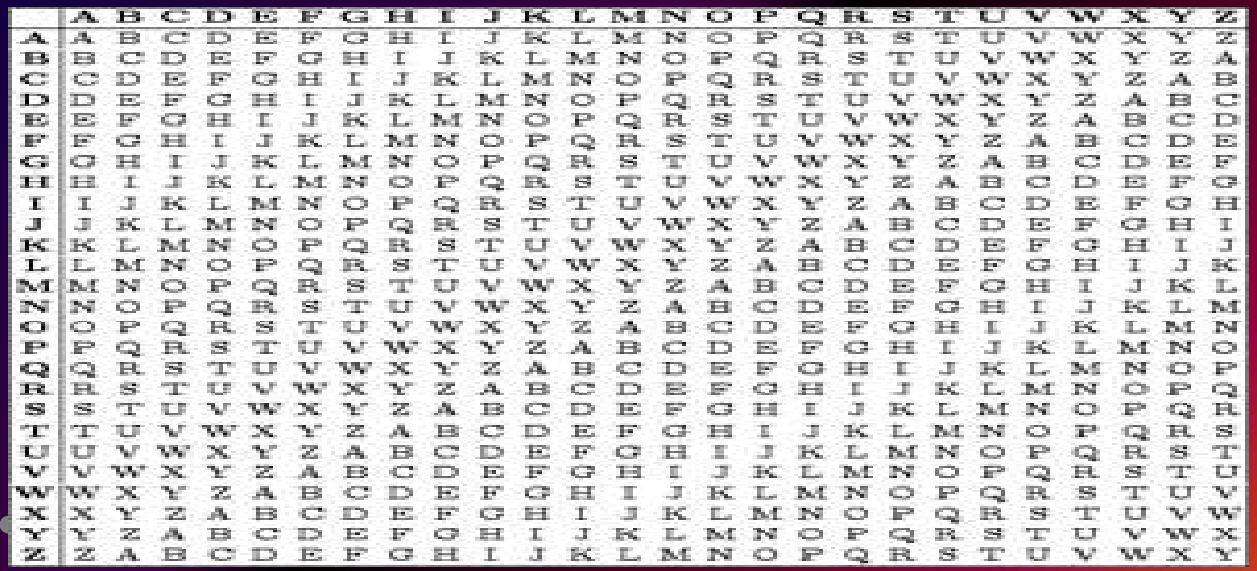
Κάθε σειρά στην αλφαβήτα, στη συνέχεια, χρησιμοποιούταν για να κρυπτογραφήσει ένα προκαθορισμένο αριθμό διαστημάτων. Για παράδειγμα, το πρώτο γράμμα κρυπτογραφούταν με το πρώτο αλφάβητο, το δεύτερο γράμμα με το δεύτερο κοκ. τότε η λέξη Secret θα γινόταν: S(S+0) F(E+1) E(C+2) U(R+3)I(E+4) Y(T+5) δηλαδή SFEUIY.

Αργότερα, το 1605, ο Francis Bacon, παρουσιάζει το Κρυπτοσύστημα του, το οποίο βασιζόταν στη δημιουργία συνδυασμών των γραμμάτων a και b ανά 5, που ο καθένας τους σήμαινε ένα γράμμα της αλφαβήτου. Ο συγκεκριμένος κώδικας, παρουσιάζει για πρώτη φορά την αρχή ότι ο κώδικας με δύο σύμβολα μπορεί να χρησιμοποιηθεί για τη μεταφορά πληροφοριών. Τα κρυπτογραφικά συστήματα επικρατούσαν στις στρατιωτικές επικοινωνίες, εκτός από τις επικοινωνίες μεταξύ των υψηλά ιστάμενων, εξαιτίας της δυσκολίας στην προστασία των βιβλίων με τα κρυπτοσυστήματα στο πεδίο της μάχης.

Κατά τη διάρκεια του Εμφυλίου, ο στρατός των Βορείων πρώτος χρησιμοποίησε κρυπτοσυστήματα στα οποία μία λέξη κλειδί έδειχνε τον τρόπο με τον οποίο θα έπρεπε να διαβαστούν οι στήλες στο κείμενο ή άλλα κρυπτοσυστήματα στα οποία υπήρχε αντικατάσταση κειμένου από άλλες λέξεις ή κώδικα. Από την άλλη πλευρά ο στρατός των Νοτίων χρησιμοποιούσε το Κρυπτοσύστημα Vigenère και κατά περίπτωση αντικαταστάσεις μόνο γραμμάτων.

ΚΩΔΙΚΑΣ VIGENERE

Η κρυπτογράφηση Vigenere είναι μια μέθοδος κρυπτογράφησης αλφαβητικού κειμένου με την χρήση μιας σειράς διαφορετικών αλγόριθμων κρυπτογράφησης του Καίσαρα με βάση τα γράμματα μιας λέξης-κλειδιού. Είναι μια απλή μορφή πολυαλφαβητικης υποκατάστασης. Ο κώδικας Vigenere έχει εφευρεθεί εκ νέου πολλές φορές. Η μέθοδος αρχικά περιγράφεται από τον Giovan Battista Bellaso το 1553 στο βιβλίο του La cifra del.Sig.-Giovan Battista Bellaso.



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

ΠΟΛΥΑΛΦΑΒΗΤΙΚΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΤΕΤΡΑΓΩΝΟΥ VIGENERE

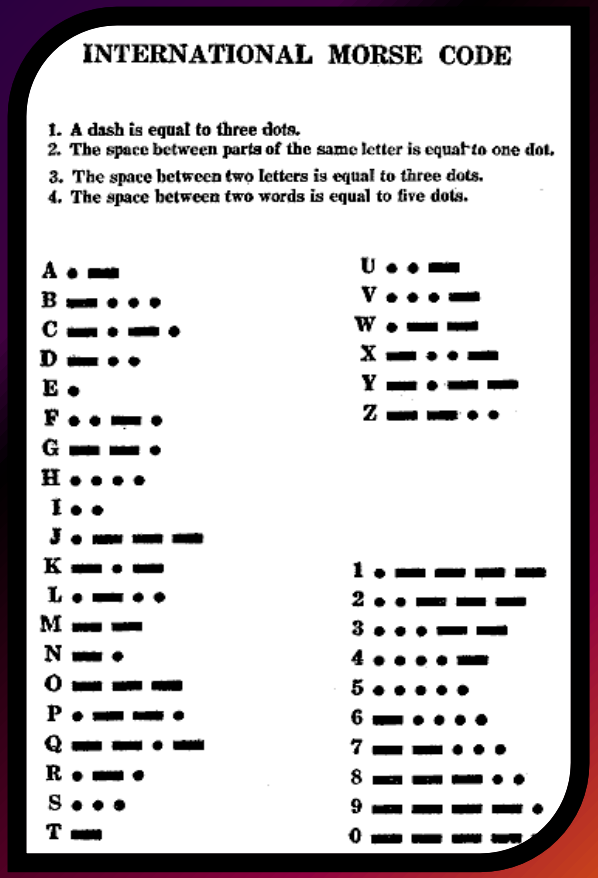
Στα πολυαλφαβητικά κρυπτοσυστήματα κάθε γράμμα του μηνύματος αντικαθίσταται με ένα σύμβολο κάθε φορά από διαφορετικό αλφάβητο. Κάθε γράμμα του μηνύματος αντικαθίσταται με ένα σύμβολο κάθε φορά από διαφορετικό αλφάβητο. Ορίζεται ένας πίνακας αντιστοίχησης 1-1 από το αλφάβητο της γλώσσας σε πολλά διαφορετικά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

Η κρυπτογραφία την εποχή του ηλεκτρισμού – Κώδικας Μορς

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

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

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



Διεθνής κώδικας Μορς

Ευχαριστούμε για την προσοχή σας!

Ζαχαρία Δήμητρα-Μαρία

Ζαχαρία Μαίρη

Κάμπαξη Μαργαρίτα