Κρυπτογραφία

Τα μοτίβα έχουν χρησιμοποιηθεί για την κρυπτογράφηση μηνυμάτων, σε διάφορες περιόδους της ιστορίας.

Ο Κώδικας του Καίσαρα είναι γνωστή και απλή τεχνική κρυπτογράφησης. Λειτουργεί ως εξής:

Ας πούμε ότι θέλουμε να κρυπτογραφήσουμε την λέξη ΥΠΟΧΩΡΗΣΗ και να την στείλουμε κρυπτογραφημένη στον παραλήπτη. Πρώτα ο κρυπτογράφος αποφασίζει ποιο θα είναι το «κλειδί» του κρυπτογραφημένου μηνύματος, δηλαδή ένας φυσικός αριθμός από 1 έως 23(αν πρόκειται για τα ελληνικά). Ας πούμε ότι επιλέγει το 5. Τότε μετατοπίζεται το αλφάβητο, όπως παρακάτω, γιατί το Ζ απέχει 5 θέσεις από το Α.

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

Στη συνέχεια, ο κρυπτογράφος αντικαθιστά κάθε γράμμα της λέξης ΥΠΟΧΩΡΗΣΗ χρησιμοποιώντας την παραπάνω αντιστοιχία, από την πάνω στην κάτω γραμμή. Δηλαδή:

- Το Υ με Ω.
- Το Π με Φ.
- Το Ο με Υ.
- Το Χ με Γ.
- Το Ω με Ε.
- Το Ρ με Ψ.
- Το Η με Μ.
- Το Σ με Χ.

Έτσι η λέξη ΥΠΟΧΩΡΗΣΗ κρυπτογραφείται ως ΩΦΥΓΕΨΜΧΜ.

Κατόπιν το μήνυμα φεύγει για τον παραλήπτη, ο οποίος όμως χρειάζεται να γνωρίζει το κλειδί για να το αποκρυπτογραφήσει, ακολουθώντας την αντίστροφη διαδικασία αντικατάστασης. Το κλειδί δεν στελνόταν μαζί με το κρυπτογραφημένο μήνυμα, γιατί αν έπεφτε στα χέρια κάποιου άλλου, θα μπορούσε κι αυτός να το αποκρυπτογραφήσει.

Μια πιο περίπλοκη μέθοδος κρυπτογράφησης, αλλά παρόμοια με αυτή του Καίσαρα είναι ο Κώδικας Vigenère.

Με αυτή τη μέθοδο ο κρυπτογράφος επιλέγει μια «λέξη-κλειδί», αντί για αριθμό.

Ας πούμε ότι επιλέγει τη λέξη ΝΕΟ.

Τότε, για να κρυπτογραφήσει τη λέξη ΥΠΟΧΩΡΗΣΗ κάνει το εξής:

Επαναλαμβάνει τη λέξη-κλειδί ΝΕΟ αντιστοιχίζοντας τα γράμματά της με τα γράμματα της λέξης ΥΠΟΧΩΡΗΣΗ, όπως φαίνεται παρακάτω

Ν	Ε	Ο	Ν	Ε	Ο	Ν	Ε	Ο
Υ	Π	Ο	Χ	Ω	Ρ	Η	Σ	Η

Το Υ αντιστοιχεί στο Ν, του κλειδιού. Τώρα θα χρησιμοποιήσει τον παρακάτω πίνακα. Αναζητά στην πρώτη στήλη το γράμμα Ν. Θα κρυπτογραφήσει το Υ σύμφωνα με τη γραμμή Ν και την πρώτη γραμμή του πίνακα.

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

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

Από την πρώτη γραμμή του πίνακα και την γραμμή Ν, προκύπτει η παρακάτω αντιστοιχία:

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

Άρα το Υ αντιστοιχεί στο Θ.

Στη συνέχεια, για να κρυπτογραφήσει το Π πηγαίνει στη γραμμή Ε, αφού σε αυτό το γράμμα της λέξης ΝΕΟ αντιστοιχεί το Π της λέξης ΥΠΟΧΩΡΗΣΗ. Σύμφωνα με τη γραμμή Ε και την πρώτη γραμμή του πίνακα, το Π κρυπτογραφείται ως Υ.

Συνεχίζοντας με παρόμοιο τρόπο για κάθε γράμμα, η λέξη ΥΠΟΧΩΡΗΣΗ κρυπτογραφείται ως ΘΥΕΚΔΗΤΧΦ.

Ένα πλεονέκτημα του Κώδικα Vigenère σε σύγκριση με τον Κώδικα του Καίσαρα είναι ότι το ίδιο γράμμα μπορεί εμφανιστεί με διαφορετικό τρόπο στο κρυπτογραφημένο μήνυμα. Για παράδειγμα, στην λέξη ΥΠΟΧΩΡΗΣΗ, το Η κρυπτογραφήθηκε την μια φορά ως Τ και την άλλη ως Φ.

Αυτό κάνει πολύ δύσκολη την αποκρυπτογράφηση του μηνύματος χωρίς το κλειδί, δηλαδή το «σπάσιμο» το κρυπτογραφημένου μηνύματος. Το σπάσιμο είναι εφικτό στον Κώδικα του Καίσαρα, όχι εύκολα, αλλά σίγουρα πιο εύκολα από τον Κώδικα Vigenère. Έτσι σε περίπτωση που το κρυπτογραφημένο μήνυμα πέσει σε «λάθος χέρια», ο αποστολέας είναι πιο ήσυχος αν έχει χρησιμοποιήσει τον Κώδικα Vigenère.

Το σπάσιμο κρυπτογραφημένων μηνυμάτων είναι μια πολύ σοβαρή υπόθεση. Στο Β΄ Παγκόσμιο Πόλεμο οι Γερμανοί χρησιμοποίησαν το «Αίνιγμα», έναν τύπο ηλεκτρικής μηχανής, για την επικοινωνία τους με κρυπτογραφημένα μηνύματα. Το Αίνιγμα κωδικοποιούσε τα μηνύματα, μεταβάλλοντας το «κλειδί» της κρυπτογράφησης με έναν εξαιρετικά πολύπλοκο τρόπο. Για την αποκρυπτογράφηση του μηνύματος ήταν απαραίτητο ο παραλήπτης να έχει κι εκείνος την ίδια μηχανή. Άρα όποιος ήθελε να στείλει ή να λάβει μήνυμα που να μπορεί να το διαβάσει θα έπρεπε να έχει στη διάθεσή του ένα «Αίνιγμα». Αλλά δεν αρκούσε αυτό. Οι ρυθμίσεις της μηχανής άλλαζαν καθημερινά και έτσι ο αποστολέας και ο παραλήπτης χρειαζόταν να γνωρίζουν και αυτές τις απόρρητες ρυθμίσεις.

Τα μηνύματα εν πολλοίς αφορούσαν θέσεις, πραγματικές ή προτιθέμενες, γερμανικών πλοίων επιφανείας και υποβρυχίων και εκπέμπονταν με τρόπο, ώστε ήταν εύκολο για τους συμμάχους

(αντίπαλοι των Γερμανών) να τα υποκλέψουν. Δηλαδή οι Γερμανοί επένδυσαν στην μέθοδο κρυπτογράφησης και όχι στην ασφάλεια των επικοινωνιών τους. Συνεπώς το δύσκολο κομμάτι δεν ήταν η υποκλοπή των μηνυμάτων, αλλά η αποκρυπτογράφησή τους. Όπως είναι προφανές η αποκρυπτογράφηση του περιεχομένου των μηνυμάτων θα έφερνε σε πλεονεκτική θέση τους συμμάχους.

Ο μαθηματικός Alan Turing (192-1954) ήταν επικεφαλής της ομάδας Βρετανών μαθηματικών-κρυπταναλυτών, που «έσπασαν» τον γερμανικό κώδικα, «έλυσαν το Αίνιγμα» και αυτό συνέβαλε αποφασιστικά στην τελική νίκη των συμμαχικών δυνάμεων. Αυτή η προσπάθειά τους κρατήθηκε μυστική για πολλά χρόνια μετά το τέλος του Β΄ Παγκοσμίου Πολέμου και έτσι ο Turing δεν έτυχε δημόσιας αναγνώρισης.

Ο Turning είχε καταλήξει σε σπουδαία θεωρητικά αποτελέσματα, για τα Μαθηματικά, ήδη από μεταπτυχιακός φοιτητής, πολύ πριν ασχοληθεί με την κρυπτανάλυση. Για τα αποτελέσματά του αυτά, συχνά αποκαλείται «Πατέρας του Υπολογιστή». Ένας άλλος κλάδος της επιστήμης των υπολογιστών στον οποίο οTuring ήταν μπροστά από την εποχή του ήταν εκείνος της Τεχνητής Νοημοσύνης. Υπήρξε πρωτοπόρος στην σχεδιασμό σκακιστικών μηχανών δίνοντας έμφαση στη δυνατότητα να μαθαίνουν οι υπολογιστές μέσα από το παιχνίδι. Η θέση του ήταν ότι θα έχουμε πετύχει την Τεχνητή Νοημοσύνη, όταν ένας υπολογιστής θα είναι σε θέση να απαντά σε ερωτήσεις με τέτοια επιδεξιότητα, ώστε ο ερωτών να μην μπορεί να καταλάβει αν οι απαντήσεις δίνονται από υπολογιστή ή από άνθρωπο.

Ο Turning πέθανε νέος, σε ηλικία 41 ετών, κατά τα φαινόμενα αυτοκτονώντας με κυάνιο. Αν και τα αίτια δεν είναι εντελώς ξεκάθαρα, κάποια ιδιαίτερη συμβολή φαίνεται να είχε η σύλληψή του για ομοφυλοφιλία το 1952.

Πηγη:

Davis, D.M. (2007). Η Φύση και η Δύναμη των Μαθηματικών (Δ. Καραγιανάκης, Μ. Μαγειρόπουλος, Απόδοση και Επιμέλεια). Ηράκλειο: Πανεπιστημιακές εκδόσεις Κρήτης.

ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΤΟΙΧΕΙΑ

ΤΙΤΛΟΣ: Κρυπτογραφία

ΣΧΕΔΙΑΣΜΟΣ / ΔΗΜΙΟΥΡΓΙΑ / ΤΕΧΝΙΚΗ ΥΛΟΠΟΙΗΣΗ:

Δημήτρης Διαμαντίδης

Ελισσάβετ Καλογερία

Ειρήνη Περυσινάκη

Γιάννης Σταμπόλας

Κώστας Στουραΐτης

Βαγγέλης Φακούδης

Γιώργος Ψυχάρης

ΕΚΔΟΣΗ: 1.0

ΗΜΕΡΟΜΗΝΙΑ: 28-12-2024

Το παρόν αναπτύχθηκε στο πλαίσιο της Πράξης «Συγγραφή, Αξιολόγηση και Ένταξη διδακτικών βιβλίων στο Μητρώο Διδακτικών Βιβλίων και στην Ψηφιακή Βιβλιοθήκη Διδακτικών Βιβλίων» με κωδικό ΟΠΣ (MIS) 6010165, του Προγράμματος «Ανθρώπινο Δυναμικό και Κοινωνική Συνοχή 2021-2027» που υλοποιείται από το Ινστιτούτο Εκπαιδευτικής Πολιτικής και συγχρηματοδοτείται από το Ευρωπαϊκό Κοινωνικό Ταμείο.