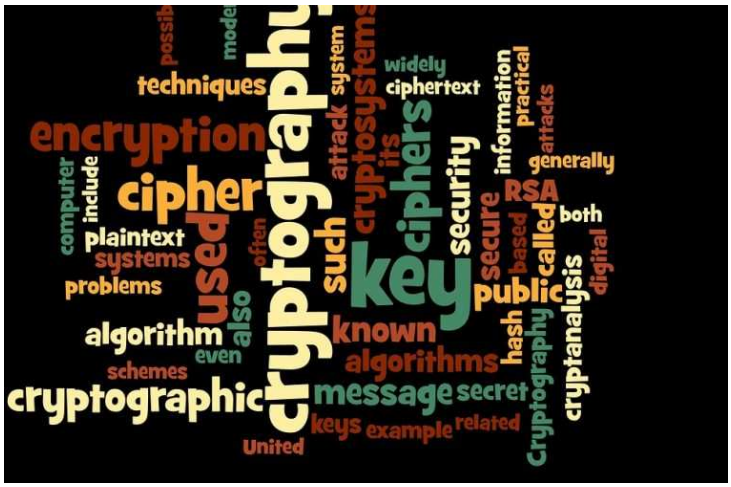
Ακαδημία Εμπορικού Ναυτικού Ασπροπύργου
Σχολή Μηχανικών

Πτυχιακή εργασία

Κωδικοποίηση και κρυπτογραφία



Σπουδαστής: **Καβαλιώτης Δημήτριος** (ΑΜ **7969**)

Επιβλέπων Καθηγητής: **Στέφανος Ι. Καρναβάς, Μαθηματικός (M.Ed.),**
Επίκουρος Καθηγητής

Ακαδημαϊκό έτος: **2021–2022**

Ημερομηνία ανάθεσης: 11.05.2020
Ημερομηνία κατάθεσης: ….09.2021
Ημερομηνία εξέτασης: ….09.2021

Α/Α	Ονοματεπώνυμο	Χαρακτηρισμός	Υπογραφή
1	Στέφανος Ι. Καρναβάς Μαθηματικός (M.Ed.) Επίκουρος Καθηγητής	Διακεκριμένη	
2	Αντωνάτος Χαράλαμπος Ναυπηγός Μηχανολόγος Μηχανικός Καθηγητής		
3	Αθανασία Χρηστίδου Ηλεκτρολόγος Μηχανικός Επίκουρη Καθηγήτρια		
Τελικός χαρακτηρισμός			

Περιεχόμενα

1. Η κρυπτογραφία από την αρχαιότητα έως το 19ο αιώνα

Η κρυπτογραφία είναι μια αρχαία πρακτική, ίσως τόσο αρχαία όσο και η ανάγκη επικοινωνίας. Ωστόσο, δεν αποτελεί το μοναδικό τρόπο μυστικής μετάδοσης της πληροφορίας. Τελικά, κάθε κείμενο πρέπει να έχει μια βάση και, αν καταφέρουμε να κάνουμε αυτή τη βάση αόρατη σε όλους εκτός από τον παραλήπτη, θα έχουμε επιτύχει το στόχο μας. Στεγανογραφία ονομάζεται η τεχνική της απόκρυψης ακόμα και της ύπαρξης του μηνύματος και οι ρίζες της ανάγονται στην ίδια εποχή με εκείνες της κρυπτογραφίας.

2. Η στεγανογραφία

Ο Ηρόδοτος, που θεωρείται πατέρας της ιστοριογραφίας λόγω των ερευνών που πραγματοποίησε κατά τον 5ο αιώνα π.Χ., αναφέρει στα χρονικά των πολέμων ανάμεσα στους Έλληνες και τους Πέρσες δύο παράξενες μεθόδους στεγανογραφίας, που αποδεικνύουν μια αξιοθαύμαστη αγχίνοια. Η **πρώτη**, που απαντά στο βιβλίο Γ' του μεγάλου του έργου «*Ιστορίαι*», χρησιμοποιείται από τον τύραννο της Μιλήτου, Ιστιαίο, ο οποίος ζήτησε από έναν άντρα να ξυρίσει το κεφάλι του. Στη συνέχεια, έγραψε στο κρανίο του το μήνυμα που ήθελε να μεταφέρει και περίμενε να μεγαλώσουν τα μαλλιά του, για να τον στείλει εκεί όπου έπρεπε να πάει, στο στρατόπεδο του Αρισταγόρα. Μόλις έφτασε σώος και αβλαβής, ο άντρας αποκάλυψε το μυστικό και αφού ξύρισε το κεφάλι του, παρέδωσε το πολυαναμενόμενο μήνυμα στον παραλήπτη του. Η **δεύτερη** μέθοδος έχει ακόμα καλύτερη ιστορική σημασία, καθώς επέστρεψε στον Δημάρατο, Σπαρτιάτη βασιλιά εξόριστο στην Περσία, να προειδοποιήσει τους συμπατριώτες του για το σχέδιο εισβολής του Πέρση βασιλιά Ξέρξη. Ο Ηρόδοτος διηγείται στο Βιβλίο Ζ' του ίδιου έργου:

«*Το πρόβλημα [για τον Δημάρατο] ήταν ότι δεν μπορούσε να τους ειδοποιήσει εύκολα. Είχε λοιπόν την εξής ιδέα, έξυσε το κερί που κάλυπτε μια πλάκα δύο σελίδων και κατέγραψε τα σχέδια του μονάρχη, χαράζοντας το μήνυμα πάνω στην ξύλινη επιφάνεια, έπειτα, μόλις τελείωσε κάλυψε ξανά με κερί την επιφάνεια της πλάκας, ώστε αυτός που θα τη μετέφερε να μην είχε το παραμικρό πρόβλημα με τους φρουρούς που θα συναντούσε στο δρόμο του. Όταν η πλάκα έφτασε τελικά στη Λακεδαιμονία [Σπάρτη], οι κάτοικοι δεν μπορούσαν να βρουν την εξήγηση, ώσπου, σύμφωνα με τα λεγόμενα, ο Γόργος πρότεινε τελικά να ξύσουν το κερί, υποδεικνύοντάς τους πως έτσι θα έβρισκαν το μήνυμα χαραγμένο στο ξύλο*».

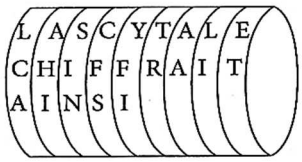
Ένα στεγανογραφικό μέσο που διέσχισε τους αιώνες είναι εκείνο του <u>αόρατου μελανιού,</u> σε όλες του τις μορφές. Παρόν σε χιλιάδες ιστορίες και ταινίες, το αόρατο μελάνι που χρησιμοποιείται για το σκοπό αυτό προέρχεται από υλικά οργανικής προέλευση, όπως <u>είναι ο χυμός λεμονιού, ο χυμός των φυτών ή ακόμα και τα ανθρώπινα ούρα,</u> λόγω της υψηλής φυσικής περιεκτικότητας τους σε άνθρακα και επομένως της τάσης τους να σκουραίνουν όταν υποβάλλονται σε λίγο υψηλότερη θερμοκρασία, όπως στη φλόγα ενός κεριού. Η στεγανογραφία είναι ένα μέσο αναμφισβήτητα χρήσιμο, αλλά φυσικά αναποτελεσματικό στην περίπτωση πληθώρας επικοινωνιών. Επιπλέον, όταν χρησιμοποιείται ως μοναδικό μέσο, παρουσιάζει ένα σημαντικό μειονέκτημα, αν το μήνυμα υποκλαπεί, το περιεχόμενο της είναι ξεκάθαρο. Ακριβώς, γι' αυτό τον λόγο η στεγανογραφία χρησιμοποιείται συμπληρωματικά της κρυπτογραφίας, για να ενισχύσει την ασφάλεια της μετάδοσης. Όπως αφήνουν να εννοηθεί τα διαφορετικά παραδείγματα που προαναφέρθηκαν, οι ένοπλες συγκρούσεις αποτέλεσαν μεγάλη κινητήρια δύναμη για την ιστορία της ασφαλούς μετάδοσης. Έτσι, δεν προκαλεί έκπληξη το γεγονός πως <u>οι Σπαρτιάτες</u>, λαός κατεξοχήν φιλοπόλεμος και γνώστης της τέχνης της στεγανογραφίας, αν πιστέψουμε τον Ηρόδοτο, <u>ήταν οι πρωτοπόροι στην ανάπτυξη της κρυπτογραφίας</u>.

3. Η κρυπτογραφία της μετάθεσης

Κατά τη διάρκεια του πολέμου ανάμεσα στους Σπαρτιάτες και τους Αθηναίους για την ηγεμονία της Πελοποννήσου, έγινε συνηθής η χρήση επιμηκών λωρίδων χαρτιού πάνω στις

οποίες έγραφαν το μήνυμα και μετά τις τύλιγαν σε μία ράβδο, τη σκυτάλη. Η κρυπτογράφηση βασιζόταν στην τροποποίηση του πρωτότυπου μηνύματος με την παρεμβολή άχρηστων συμβόλων, τα οποία εξαφανίζονταν μόλις το μήνυμα τυλιγόταν στην ράβδο, προκαθορισμένου μήκους και πάχους. Ακόμα κι αν γνώριζε την τεχνική που είχε χρησιμοποιηθεί, δηλαδή τον αλγόριθμο κρυπτογράφησης, αυτός που υπέκλεπτε το μήνυμα είχε πολλές δυσκολίες να το αποκωδικοποιήσει αν δεν ήξερε τις ακριβείς διαστάσεις της σκυτάλης. Το μήκος και το πάχος αυτής αποτελούσαν τελικά το κλειδί του συστήματος.

Όταν η λωρίδα του χαρτιού ξετυλιγόταν, το μήνυμα δεν μπορούσε να διαβαστεί από όσους δεν ήξεραν τη μέθοδο ή δεν διέθεταν ράβδο ίδιου πάχους. Στο σχέδιο που ακολουθεί, το μήνυμα που πρέπει να μεταδοθεί είναι τι ακόλουθο «*La scytale chiffrait ainsi (Η σκυτάλη κρυπτογραφήθηκε έτσι)*». Στην ξετυλιγμένη λωρίδα χαρτιού εμφανιζόταν ένα ακατάληπτο σύνολο λέξεων «*Ica ahi sin cfs yfi tr aa li et*».



M = LA SCYTALLE CHIFFRAIT AINSI
C = LCA AHI SIN CFSYFI TR AA LI ET

Η μέθοδος της σκυτάλης είναι μια κρυπτογραφική μέθοδος, γνωστή με το όνομα μετάθεση και συνίσταται στην αναδιοργάνωση των χαρακτήρων ενός μηνύματος. Για να πάρουμε μια ιδέα της ισχύος αυτής της μεθόδου, ας χρησιμοποιήσουμε την απλή περίπτωση μετάθεσης τριών χαρακτήρων: Α, Ο & Ρ. Χωρίς κανένα είδος υπολογισμού, βλέπουμε γρήγορα ότι υπάρχουν έξι τρόποι αναδιοργάνωσης αυτών των τριών γραμμάτων: ΑΟΡ, ΑΡΟ, ΟΑΡ, ΟΡΑ, ΡΟΑ και ΡΑΟ. Η διαδικασία είναι η ακόλουθη: Αφού επιλέγει ένας από τους χαρακτήρες στην πρώτη θέση από τις τρεις πιθανές, μας μένουν μόνο δύο χαρακτήρες που μπορούν να τοποθετηθούν με δύο διαφορετικούς τρόπους, δηλαδή σύνολο 3x2=6 συνδυασμών. Στην περίπτωση ενός πιο μεγάλου μηνύματος, 10 χαρακτήρων, για παράδειγμα, ο αριθμός των πιθανών συνδυασμών είναι 10x9x8x7x6x5x4x3x2x1 (μαθηματική πράξη που γράφεται 10!), δηλαδή σύνολο 3.628.800.

Γενικεύοντας τα παραπάνω, για n χαρακτήρες υπάρχουν n! τρόποι αναδιοργάνωσής τους. Έτσι, ένα μήνυμα 40 χαρακτήρων αθροίζει τέτοιον αριθμό πιθανών συνδυασμών των οποίων η εξακρίβωση καθίσταται εντελώς αδύνατη. Θα είχαμε βρει λοιπόν τέλεια κρυπτογραφική μέθοδο; Όχι. Στην πραγματικότητα, ένας τυχαίος αλγόριθμος μετάθεσης προσφέρει ένα υψηλό επίπεδο ασφάλειας, αλλά ποιο είναι το κλειδί αποκρυπτογράφησης; Ο τυχαίος χαρακτήρας της διαδικασίας είναι ταυτόχρονα η ισχύς και η αδυναμία της. Έπρεπε να βρεθεί μια άλλη μέθοδος κρυπτογράφησης που θα επέτρεπε τη δημιουργία απλών κλειδιών, εύκολων στην απομνημόνευση και στη μετάδοση, χωρίς να διακυβεύεται υπερβολικά η ασφάλεια. Έτσι, ξεκίνησε η αναζήτηση του τέλειου αλγόριθμου από τους Ρωμαίους αυτοκράτορες.

3.1 Εγχειρίδιο δεσποινίδων

Το Kama–Sutra είναι ένα τεράστιο έργο, που ασχολείται μεταξύ άλλων με τις γνώσεις που πρέπει να έχει μια γυναίκα για να είναι καλή σύζυγος και καλή σύντροφος. Γραμμένο γύρω στον 4ο αιώνα π.Χ. από το Βραχμάνο Vatsyyayana, προτείνει 64 ξεχωριστές δεξιότητες, μεταξύ των οποίων η μουσική, η μαγειρική και το σκάκι. Η δεξιότητα αριθμός 45 μας ενδιαφέρει ιδιαίτερα, καθώς έχει να κάνει με την τέχνη της μυστικής γραφής που

αποκαλείται mlecchita–vikalpa. Ο Ινδός λόγιος προτείνει διάφορες μεθόδους, μεταξύ των οποίων η διαίρεση της αλφαβήτου στα δύο και εν συνέχεια το ζευγάρωμα των γραμμάτων με τυχαίο τρόπο. Σ' αυτό το σύστημα, κάθε ζεύγος γραμμάτων αποτελεί ένα κλειδί. Ένα τέτοιο ζευγάρωμα θα μπορούσε να είναι για παράδειγμα:

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

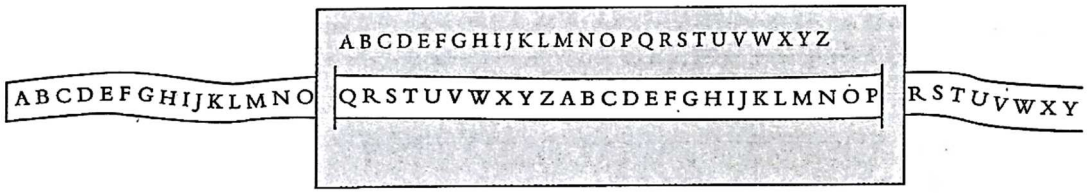
3.2 Με μικρά γράμματα

Κατά τη διάρκεια του ψυχρού πολέμου, οι ταινίες κατασκοπείας έβριθαν μηνυμάτων που μεταδίδονται πάνω σε βάσεις πρακτικά αόρατες λόγω του εξαιρετικά μικρού τους μεγέθους, τα μικροφίλμ. Μερικές δεκάδες χρόνια νωρίτερα, κατά τον Β' Παγκόσμιο Πόλεμο, οι Γερμανοί πράκτορες χρησιμοποιούσαν συχνά ένα στεγανογραφικό μέσο, γνωστό με το όνομα μικροσημείο, το οποίο μίκραινε το μέγεθος της φωτογραφίας ενός κειμένου όσο ένα τυπογραφικό σημείο. Αυτό εν συνέχεια εισχωρούσε ως συμπληρωματική ένδειξη σε ένα κείμενο, το οποίο με τη σειρά του ήταν αβλαβές.

4. Τα του Καίσαρος τω Καίσαρι

Παράλληλα με τις κωδικοποιήσεις μετάθεσης, αναπτύχθηκαν και εκείνες της αντικατάστασης. Αντίθετα από τη μετάθεση, η αυστηρή αντικατάσταση αλλάζει ένα γράμμα με ένα άλλο, στην ουσία με ένα οποιοδήποτε σύμβολο, ανεξάρτητα από το αν αυτό το τελευταίο βρίσκεται μέσα στο μήνυμα. Για να το θυμόμαστε, θα πούμε πως στη μετάθεση το γράμμα αλλάζει θέση αλλά διατηρεί το ρόλο του (ένα ίδιο γράμμα έχει την ίδια σημασία τόσο στο πρωτότυπο όσο και στο κωδικοποιημένο μήνυμα), ενώ στην αντικατάσταση, το γράμμα διατηρεί τη θέση του, αλλά αλλάζει σημασία (ένα ίδιο γράμμα έχει μια σημασία στο πρωτότυπο μήνυμα και μια άλλη στο κωδικοποιημένο μήνυμα). Ένας από τους πρώτους αλγόριθμους αντικατάστασης είναι το τετράγωνο του Πολύβιου, που ονομάστηκε έτσι προς τιμήν του γνωστού Έλληνα ιστορικού (203 π.Χ. –120 π.Χ.) που το εφηύρε.

Περίπου πενήντα χρόνια αργότερα, τον 1ο μ.Χ. αιώνα, εμφανίστηκε μια άλλη κρυπτογράφηση αντικατάστασης, γνωστή ως κώδικας του Καίσαρα, καθώς ο αυτοκράτορας αυτός ήταν ένας από τους πιο επιμελείς χρήστες του. Πρόκειται για έναν από τους πιο μελετημένους κώδικές στον τομέα της κρυπτογραφίας, διότι επιτρέπει τη χρήση των αρχών της αριθμητικής υπολοίπων, μιας εκ των ακρογωνιαίων λίθων της μαθηματικής μελέτης της γραφής με κλειδί κρυπτογράφησης. Το κρυπτογράφημα του Καίσαρα συνιστάται στην αντιστοίχιση κάθε γράμματος του αλφάβητου με ένα άλλο, καταλήγοντας στη μετάθεση του αλφάβητου κατά ένα συγκεκριμένο αριθμό γραμμάτων. Όπως περιγράφει ο Σουητώνιος στο βιβλίο του «*Οι Ζωές των Δώδεκα Καισάρων*», ο Ιούλιος Καίσαρας κρυπτογραφούσε την προσωπική του αλληλογραφία με τη βοήθεια ενός αλγόριθμου αντικατάστασης αυτού του τύπου. Κάθε γράμμα του αρχικού μηνύματος αντικαθίστατο από εκείνο που ακολουθούσε μετά από τρις θέσεις στο αλφάβητο: το γράμμα Α αντικαθίστατο από ένα Δ, το Β από ένα Ε και ούτω καθεξής ως το τελευταίο. Η κρυπτογράφηση και η αποκρυπτογράφηση ενός μηνύματος που είχε κωδικοποιηθεί με αυτό τον τρόπο μπορούσαν να γίνουν με τη βοήθεια μιας μηχανής από τις πιο απλές, όπως αυτή που απεικονίζεται παρακάτω:



Ας εξετάσουμε τώρα τη διαδικασία με πιο λεπτομερή τρόπο. Ο πίνακας που ακολουθεί δείχνει το αλφάβητο εκκίνησης και το αλφάβητο μετατιθέμενο κατά τρεις θέσεις, σύμφωνα με το κρυπτογράφημα του Καίσαρα, για το ελληνικό αλφάβητο που απαρτίζεται απο 24 γράμματα: το αρχικό αλφάβητο βρίσκεται στην άνω γραμμή και το κρυπτογραφημένο αλφάβητο στην κάτω γραμμή.

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

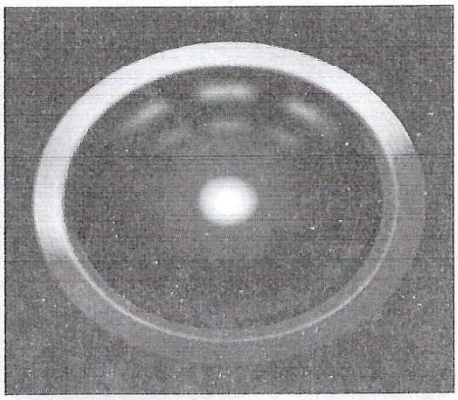
Με τα δύο αλφάβητα, το πρωτότυπο ή καθαρό και το κρυπτογράφημα, αρκεί απλά, για να κρυπτογραφήσει κανείς ένα οποιοδήποτε μήνυμα, να αντικαταστήσει τους χαρακτήρες του πρώτου με τους χαρακτήρες του δεύτερου. Το κλειδί κρυπτογράφησης είναι ο χαρακτήρας που αντικαθιστά το πρώτο γράμμα του αλφάβητου, δηλαδή εδώ το Δ που αντικαθιστά το Α. Η κλασική λοιπόν έκφραση «*ΑΒΕ ΚΑΙΣΑΡ*» θα γινόταν «*ΔΕΘ ΝΔΜΦΔΥ*». Αντίστροφα, αν το κρυπτογραφημένο μήνυμα είναι «*ΗΘΙΠΧΥΣ*», το αποκρυπτογραφημένο μήνυμα είναι «*ΔΕΝΤΡΟ*». Στην περίπτωση ενός κρυπτογραφήματος του Καίσαρα, όπως αυτό που περιγράφεται παραπάνω, ένας κρυπταναλυτής που θα είχε υποκλέψει το μήνυμα και θα γνώριζε τον αλγόριθμο αλλά όχι το κλειδί, θα έπρεπε να δοκιμάσει όλες τις πιθανές μετατοπίσεις ώσπου το μήνυμα να βγάζει νόημα και γι' αυτό να εξετάσει όλα τα κλειδιά, δηλαδή όλες τις μετατοπίσεις. Για ένα αλφάβητο n γραμμάτων, αυτό σημαίνει n πιθανές μετατοπίσεις και άλλα τόσα κρυπτογραφημένα αλφάβητα ή κλειδιά.

Ο ΙΟΥΛΙΟΣ ΚΑΙΣΑΡΑΣ ΕΦΤΑΣΕ (100-44 π.Χ.)

Στρατιωτικός και πολιτικός του οποίου η δικτατορία έβαλε τέλος στη ρωμαϊκή δημοκρατία. Αφότου ανέλαβε το ρόλο του κυβερνήτη στην Ισπανία (Hispania Baetica), συνεργάζεται με άλλες δυο ισχυρές προσωπικότητες της εποχής εκείνης, τον Πομπήιο και τον Κράσσο, για να σχηματίσει την πρώτη τριανδρία, την οποία ενδυναμώνει παντρεύοντας την κόρη του, Ιουλία, με τον Πομπήιο. Μοίρασαν μεταξύ τους τις ζώνες επιρροής της Ρωμαϊκής Αυτοκρατορίας: ο Κράσσος ανέλαβε τη διακυβέρνηση των χωρών της Ανατολής, ο Πομπήιος παρέμεινε στη Ρώμη και ο Καίσαρας ανέλαβε τη στρατιωτική διοίκηση της Γαλατίας εντεύθεν των Άλπεων κι έγινε κυβερνήτης των γαλατικών επαρχιών της Ναρμπόν. Ξεκίνησε έτσι ένα δύσκολο πόλεμο ενάντια στους Γαλάτες, ο οποίος θα κρατούσε οκτώ χρόνια και θα τέλειωνε με τη ρωμαϊκή κατάκτηση της Γαλατίας. Ο Καίσαρας προέλασε τότε στην πρωτεύουσα και εγκαταστάθηκε ως μοναδικός δικτάτορας.

ΚΙΝΗΜΑΤΟΓΡΑΦΙΚΟΙ ΚΩΔΙΚΕΣ

Στη μεγάλη κλασική ταινία επιστημονικής φαντασίας *2001: Η Οδύσσεια του Διαστήματος*, σε σενάριο και σκηνοθεσία Στάνλεϊ Κιούμπρικ του 1968, εμφανίζεται ένας υπερ-υπολογιστής προικισμένος με το χάρισμα της συνείδησης, αποκαλούμενος HAL 9000 που καταλήγει να τρελαθεί και επιχειρεί να σκοτώσει το πλήρωμα του διαστημόπλοιου που ελέγχει. Ας πάρουμε έναν κώδικα του Καίσαρα κλειδιού Β κι ας τον εφαρμόσουμε στη λέξη «HAL» σαν να επρόκειτο για ένα μήνυμα κρυπτογραφημένο με αυτό τον κώδικα. Παρατηρούμε ότι το γράμμα Η αντιστοιχεί στο γράμμα Ι, το Α στο Β και το L στο Μ, δηλαδή «IBM», που ήταν την εποχή εκείνη μια μεγάλη βιομηχανική πολυεθνική, η οποία μονοπωλούσε τον κλάδο της κατασκευής ηλεκτρονικών υπολογιστών. Μήπως ο Κιούμπρικ προσπαθούσε να προειδοποιήσει τους θεατές για τους κινδύνους της ανεξέλεγκτης τεχνητής νοημοσύνης;



Το φωτεινό μάτι του HAL 9000 στην ταινία 2001: Η Οδύσσεια του Διαστήματος.

5. Η αριθμητική υπολοίπων και τα μαθηματικά του κρυπτογραφήματος του Καίσαρα

Η λειτουργία ενός κώδικα του Καίσαρα μπορεί να σχηματοποιηθεί με ένα εργαλείο πολύ συνηθισμένο στα μαθηματικά και ακόμα πιο συνηθισμένο στην κρυπτογραφία, την αριθμητική των υπολοίπων ή «ωρολογιακή αριθμητική». Αυτή η τεχνική έχει τις ρίζες της στη δουλειά του μαθηματικού Ευκλείδη (325–265 π.Χ.) που αποτελεί μια θεμελιώδη βάση των πρόσφατων συστημάτων ασφάλειας της πληροφορίας. Αυτή η παράγραφος παρουσιάζει με απλό τρόπο τις στοιχειώδεις μαθηματικές αρχές που συνδέονται με τη συγκεκριμένη αριθμητική. Ας αναλογιστούμε ένα κλασικό αναλογικό ρολόι κι ας το συγκρίνουμε με ένα αριθμητικό ρολόι. Η αναλογική ωριαία κατανομή διαιρεί τον κύκλο σε δώδεκα μέρη, τα οποία θα ορίσουμε από το 0, το 2, το 3, το 4, το 5, το 6, το 7, το 8, το 9, το 10 και το 11. Η ωριαία αντίστοιχα ανάμεσα σε ένα αναλογικό και σε ένα αριθμητικό ρολόι απεικονίζεται στον παρακάτω πίνακα.

0	1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22	23

Όπως λέμε «η ώρα είναι 16», έτσι λέμε και «η ώρα είναι 4 το απόγευμα». Η ίδια αρχή χρησιμοποιείται για τις μετρήσεις της γωνίας, μία γωνία 370° είναι αντίστοιχη με μία γωνία 10°, επειδή πρέπει να της αφαιρέσουμε έναν ολόκληρο κύκλο 360°. Σημειώστε ότι 370=(1•360)+10 ή ακόμα ότι το 10 είναι το υπόλοιπο του 370 διαιρεμένο με το 360. Σε πόσες μοίρες αντιστοιχούν οι 750°; Αφού αφαιρέσουμε από το 750 τον αριθμό των ολόκληρων κύκλων, συμπεραίνουμε ότι μια γωνία 750° ισοδυναμεί με μια γωνία 30°. Βλέπουμε πως 750=2•360+30 και ότι το 30 είναι το υπόλοιπο του 750 διαιρεμένο με το 360.

Στην επιστημονική σημειογραφία, αυτή η σχέση γράφεται 750*30 (mod. 360) και διαβάζουμε «750 είναι ταυτόσημο με 30 modulo 360». Στη περίπτωση του ρολογιού, θα γράφαμε 14*2 (mod. 12). Θα μπορούσαμε αντίστοιχα να φανταστούμε ένα ρολόι με αρνητικούς αριθμούς. Σ' αυτή την περίπτωση τι ώρα θα είναι όταν ο δείκτης δείξει –7; Ή, ισοδύναμα, με ποιον αριθμό είναι ταυτόσημο το –7 modulo 12; Υπενθυμίζοντας ότι η τιμή «0» του ρολογιού μας ισοδυναμεί με το «12», μπορούμε να γράψουμε –7=–7+ 0*–7+12=5.

Τα μαθηματικά των υπολογισμών με το αναλογικό μας ρολόι που αποτελείται από 12 μέρη ονομάζεται *αριθμητική modulo* 12. Γενικά, λέμε ότι a * b (mod. M), αν το υπόλοιπο της διαίρεσης (ευκλείδειας διαίρεσης) του a με το m είναι b ή αν τα a, m και b είναι ακέραιοι αριθμοί. Ο αριθμός b είναι το υπόλοιπο της διαίρεσης του a με το m. Τα παρακάτω είναι ισοδύναμα:

a b (mod. m), b* a (mod. m), a–b * 0 (mod. m), a–b είναι πολλαπλάσιο του m.*

Το ερώτημα «σε τι αναλογική ώρα αντιστοιχούν οι 19 ώρες» είναι ισοδύναμο του ερωτήματος «Με πόσο το 19 είναι ταυτόσημο modulo 12»; Για να απαντήσουμε, πρέπει να λύσουμε την εξίσωση 19 (mod. 12). Διαιρώντας το 19 με το 12, έχουμε πηλίκο 1 και υπόλοιπο 7, άρα 19 * 7(mod. 12). Και στην περίπτωση των 127 ωρών; Διαιρούμε το 127 με το 12 και έχουμε 10 με υπόλοιπο 7, άρα 127 * 7 (mod. 12). Για να ανακεφαλαιώσουμε τα όσα είδαμε ως τώρα, ας ρίξουμε μια ματιά στις ακόλουθες πράξεις, modulo 7, που λύνονται παρακάτω:

(**1**) 3 + 3*6 (**2**) 3+14*3
(**3**) 3×3=9*2 (**4**) 5×4 = 20*6
(**5**) 7 * 0 (**6**) 35 * 0
(**7**) –44 = –44 + 0 * –44 + 7 × 7 * 5 (**8**) –33=–33 + 0*–3 +5×7*2

(**1**) καθώς το 6 είναι κατώτερο του modulo, παραμένει αναλλοίωτο
(**2**) 3+14=17; 17:7=14 και μένει 3
(**3**) 3×3=9; 9:7=1 και μένει 2
(**4**) 5×4=20; 20:7= 2 και μένει 6
(**5**) 7 = 7; 7:7=1 και μένει 0
(**6**) 35 = 35; 35:7=7 και μένει 0
(**7**) –44 = – 44+ 0; –44 + (7 × 7) = 5
(**8**) –33 = – 33+0; –33 + (5 × 7) = 2

Ποια σχέση υπάρχει ανάμεσα στην αριθμητική των υπολοίπων και την κρυπτογράφηση του Καίσαρα; Για να απαντήσουμε σε αυτή την ερώτηση, ας πάρουμε το συμβατικό γαλλικό αλφάβητο των 26 χαρακτήρων και το αλφάβητο μετατοπισμένο κατά 3 γράμματα, κι ας τους προσθέσουμε, από πάνω, μια αριθμητική αντιστοίχιση.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	S	Y	Z
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

Η κρυπτογραφημένη εκδοχή ενός χαρακτήρα ×σειράς στο αρχικό αλφάβητο είναι ο χαρακτήρας σειράς × + 3 στο ίδιο αλφάβητο. Κατά συνέπεια, είναι ενδιαφέρον να βρούμε ένα μετασχηματισμό που να επιτρέπει το συσχετισμό, σε κάθε αριθμητική τιμή, της τιμής αυξημένης κατά 3 και να δίνει το αποτέλεσμα modulo 26. Πρέπει να σημειώσουμε πως το 3 είναι το κλειδί της κρυπτογράφησης. Ορίζουμε μια συνάρτηση C (×)=×+3(mod. 26),

Όπου × είναι η μη κρυπτογραφημένη τιμή και C (×) η κρυπτογραφημένη τιμή. Αρκεί λοιπόν να αντικαταστήσουμε το γράμμα με το αριθμητικό του ισοδύναμο και να του εφαρμόσουμε το μετασχηματισμό. Ας πάρουμε, για παράδειγμα, το μήνυμα «*BLEU*» («*ΜΠΛΕ*») κι ας το κρυπτογραφήσουμε:

*Το Β θα γίνει 1, C (1)=1+ 3*4 (mod. 26) που αντιστοιχεί στο Ε.*
*Το Λ θα γίνει 11, C (11)=11+3=14*14 (mod.26) που αντιστοιχεί στο Ο.*
*Το Ε θα γίνει 4, C (4)=4+3=7*7 (mod.26) που αντιστοιχεί στο Η.*
*Το U θα γίνει 20, C (20)=20+3=23*23 (mod.26) που αντιστοιχεί στο γράμμα Χ.*
Το μήνυμα «BLEU» κρυπτογραφημένο με το κλειδί 3 γίνεται «*ΕΟΗΧ*».

Γενικά, αν το x δείχνει τη σειρά του γράμματος που θέλουμε να κρυπτογραφήσουμε (0 για το Α, 1 για το β κ.ο.κ.), η σειρά του κρυπτογραφημένου γράμματος [C(x)] δίνεται από τον τύπο C(x)= (x+k) (mod.n). Όπου n=το μήκος του αλφάβητου (26 για τη γαλλική γλώσσα) και k=το κλειδί, τιμή σύμφωνα με την οποία θα αλλάξει το κρυπτογραφημένο μήνυμα. Η αποκρυπτογράφηση του μηνύματος είναι η αντίστροφη πράξη της κρυπτογράφησης. Στο παράδειγμα, η αποκρυπτογράφηση ισοδυναμεί με την εφαρμογή του αντίστροφου τύπου και με τη χρήση του για κρυπτογράφηση, δηλαδή

$$C^{-1}(x) = (x–k) \text{ (mod.n)}.$$

Στην περίπτωση του κρυπτογραφημένου μηνύματος «*ΕΟΗΧ*»,με μία κρυπτογράφηση του Καίσαρα κλειδιού 3 εφαρμοσμένη στο γαλλικό αλφάβητο, k=3 και n=26 άρα:

$C^{-1}(x) = (x–3)$ (mod. 26). Αυτό μας δίνει:

Για το Ε, x = 4, $C^{-1}(4) = 4–3*31$ *(mod. 26) που αντιστοιχεί στο γράμμα Β.*

Για το Ο, x = 14, $C^{-1}(14) = 14–3*11$ *(mod. 26) που αντιστοιχεί στο γράμμα L.*

Για το Η, x = 7, $C^{-1}(7) = 7– 3*4$ *(mod.26) που αντιστοιχεί στο γράμμα Ε.*

Για το Χ, x = 23, $C^{-1}(23) = 23–3*20$ *(mod. 26) που αντιστοιχεί στο γράμμα U.*

Το μήνυμα «ΕΟΗΧ» κρυπτογραφημένο με έναν κώδικα του Καίσαρα κλειδιού 3, αντιστοιχεί στο καθαρό κείμενο «BLEU». Για να ολοκληρώσουμε μπορούμε να καθορίσουμε ένα νέο μετασχηματισμό, αποκαλούμενο ομοπαραλληλική ή αφινική κρυπτογράφηση του Καίσαρα. Αυτός ο μετασχηματισμός ορίζεται ως εξής

$$C_{(a,b)}(x) = (a \bullet x + b) \text{ (mod.n)},$$

όπου a και b δύο ακέραιοι αριθμοί μικρότεροι του αριθμού n γραμμάτων του αλφάβητου. Ο μέγιστος κοινός διαιρέτης του a και του n πρέπει να είναι το 1 [MDK (a, n)=1], διαφορετικά θα μπορούσαμε να κρυπτογραφήσουμε έναν ίδιο χαρακτήρα με διαφορετικούς τρόπους, όπως θα δούμε παρακάτω. Το κλειδί κρυπτογράφησης καθορίζεται από το ζεύγος (a, b).

Το κρυπτογράφημα του Καίσαρα κλειδιού 3 είναι λοιπόν μια ομοπαραλληλική κρυπτογράφηση τιμής a=1 και b=3. Οι γενικές ομοπαραλληλικές κρυπτογραφήσεις που έχουν αυτή τη μορφή προσφέρουν καλύτερη ασφάλεια από το συμβατικό κώδικα του Καίσαρα. Γιατί; Επειδή, όπως είδαμε, τα κλειδιά μιας ομοπαραλληλικής κρυπτογράφησης είναι τα ζεύγη (a, b). Στην περίπτωση ενός μηνύματος γραμμένου σε ένα αλφάβητο 26 γραμμάτων και κωδικοποιημένου σύμφωνα με έναν ομοπαραλληλικό αλγόριθμο, το a και το b μπορούν να έχουν οποιαδήποτε τιμή μεταξύ 1 και 25. Ο αριθμός των πιθανών κλειδιών αυτού του συστήματος κωδικοποίησης για ένα αλφάβητο 26 γραμμάτων είναι λοιπόν 26x26=676. Έτσι, ο αριθμός των κλειδιών για ένα αλφάβητο n γραμμάτων είναι n φορές μεγαλύτερος εκείνου ενός κώδικα του Καίσαρα. Πρόκειται για αξιόλογη αύξηση αλλά εξακολουθεί να είναι πιθανή σ' αυτή την περίπτωση η αποκρυπτογράφηση με ωμή βία.

5.1 Ο πατέρας της αναλυτικής κρυπτογραφίας

Το κυριότερο έργο του Ευκλείδη, τα «Στοιχεία», αποτελείται από 13 τόμους, όπου μελετώνται θέματα όπως η επίπεδη γεωμετρία, οι αναλογίες γενικά, οι ιδιότητες των αριθμών, τα μη μετρήσιμα μεγέθη και η γεωμετρία του διαστήματος. Αν και αποτελούν κομμάτι αυτού του τελευταίου κλάδου, οι εργασίες του Έλληνα μαθηματικού, στην αριθμητική των πράξεων σε τέλεια αριθμητικά σύνολα, συνιστούν ένα από τα θεμέλια της επίσημης μελέτης της κρυπτογραφίας. Ο Ευκλείδης ήταν γνωστός στους Άραβες, οι οποίοι τον εκτιμούσαν πολύ. Η πρώτη ευρωπαϊκή έκδοση των έργων του, όμως, πραγματοποιήθηκε στη Βενετία μόλις το 1482. Τόσο οι Άραβες όσο και οι Βενετσιάνοι υπήρξαν δεξιοτέχνες της κρυπτογραφίας.

5.2 Πίνακας πολλαπλασιασμού modulo 5 και εφαρμογές excel

Ο πίνακας πολλαπλασιασμού modulo 5 θα είχε ως εξής:

0	**1**	**2**	**3**	**4**

0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Είναι εύκολο να κατασκευαστεί ο παραπάνω πίνακας, καθώς κι άλλοι παρόμοιοι με στοιχειώδεις γνώσεις του περιβάλλοντος Excel. Στο παράδειγμα η σύνταξη συγκεκριμένων οδηγιών σε αυτό το περιβάλλον περιγράφεται παρακάτω. Η έννοια «υπόλοιπο της διαίρεσης με το 5» μεταφράζεται στη γλώσσα του Excel ως «=MOD(4•3, 5)» που θα μας δώσει τον αριθμό 2. Αυτοί οι πίνακες έχουν μεγάλη χρησιμότητα για κάποιον που δουλεύει στην αριθμητική των υπολοίπων.

	0	1	2	3	4
0	=MOD(B$5*$A6;5)	=MOD(C$5*$A6;5)	=MOD(D$5*$A6;5)	=MOD(E$5*$A6;5)	=MOD(F$5*$A6;5)
1	=MOD(B$5*$A7;5)	=MOD(C$5*$A7;5)	=MOD(D$5*$A7;5)	=MOD(E$5*$A7;5)	=MOD(F$5*$A7;5)
2	=MOD(B$5*$A8;5)	=MOD(C$5*$A8;5)	=MOD(D$5*$A8;5)	=MOD(E$5*$A8;5)	=MOD(F$5*$A8;5)
3	=MOD(B$5*$A9;5)	=MOD(C$5*$9;5)	=MOD(D$5*$9;5)	=MOD(E$5*$9;5)	=MOD(F$5*$9;5)
4	=MOD(B$5*$A10;5)	=MOD(C$5*$A10;5)	=MOD(D$5*$A10;5)	=MOD(E$5*$A10;5)	=MOD(F$5*$A10;5)

5.3 Υπολογισμοί υπολοίπων

Πώς υπολογίζεται το 231 modulo 17 με κομπιουτεράκι; Κατ' αρχάς, διαιρούμε το 231 με το 17: το αποτέλεσμα είναι 13,58823529. Στη συνέχεια πολλαπλασιάζουμε το 13 με το 17 =221. Έτσι, εξαφανίζουμε τους δεκαδικούς της πράξης. Έπειτα αφαιρούμε το 221 από το 231, δηλαδή 10, για να πάρουμε το υπόλοιπο της διαίρεσης. 231 modulo 17 είναι το 10 και αυτό το αποτέλεσμα γράφεται 231*10 (mod. 17).

6. Ο μέγιστος κοινός διαιρέτης (ΜΚΔ)

Ο μέγιστος κοινός διαιρέτης δύο αριθμών μπορεί να αποκτηθεί με τον αλγόριθμο του Ευκλείδη. Συνίσταται στη διαίρεση των δύο αριθμών και στη συνέχεια σε διαδοχικές διαιρέσεις του προηγούμενου πηλίκου με το καινούργιο υπόλοιπο. Η πράξη ολοκληρώνεται όταν το υπόλοιπο είναι μηδενικό, με τον πιο μεγάλο κοινό διαιρέτη να είναι ο διαιρέτης της τελευταίας διαίρεσης. Ας δούμε ένα παράδειγμα, ποιος είναι ο

ΜΚΔ(48,30);

Διαιρούμε το 48 με το 30 και παίρνουμε υπόλοιπο 18 για πηλίκο 1.
Διαιρούμε το 30 με το 18 και παίρνουμε υπόλοιπο 12 για πηλίκο 6.
Διαιρούμε το 18 με το 12 και παίρνουμε υπόλοιπο 6 για πηλίκο 1.
Διαιρούμε το 12 με το 6 και παίρνουμε υπόλοιπο 0 για πηλίκο 2.
Ο αλγόριθμος ολοκληρώθηκε. Ο ΜΚΔ(48, 30) είναι το 6.
Έστω ΜΚΔ (α,n)=1, τότε λέμε ότι οι αριθμοί α και n είναι πρώτοι μεταξύ τους. Η ισότητα Bezout, πολύ σημαντική στην κρυπτογραφία, ορίζει ότι για δυο ακέραιους αριθμούς μεγαλύτερους το 0 υπάρχουν δύο ακέραιοι k και q ώστε ο ΜΚΔ(α, n)=ka+nq.

7. Παίζοντας τους κατασκόπους

Στην περίπτωση των ομοπαραλληλικών κρυπτογραφημάτων, ποιες είναι οι συνθήκες αποκρυπτογράφησης, τόσο για τον παραλήπτη όσο και για έναν κατάσκοπο; Θα εξετάσουμε τώρα αυτό το ερώτημα με τη βοήθεια ενός απλού παραδείγματος κρυπτογράφησης με το αλφάβητο των ακόλουθων έξι γραμμάτων:

0	1	2	3	4	5
Α	Β	Γ	Δ	Ε	Ζ

Το κείμενο θα κωδικοποιηθεί με το ομοπαραλληλικό κρυπτογράφημα C(x) = 2x + 1 (mod. 6) ως εξής:

*Το γράμμα Α με το C(0)=2×0+ 1*1 (mod. 6) που αντιστοιχεί στο Β.*
*Το γράμμα Β με το C(1)=2×1+1*3 (mod. 6) που αντιστοιχεί στο Δ.*
*Το γράμμα Γ με το C(2)=2×2+1*5 (mod. 6) που αντιστοιχεί στο Ζ.*
*Το γράμμα Δ με το C(3)=2×3+1=7*1 (mod. 6) που αντιστοιχεί στο γράμμα Β.*
*Το γράμμα Ε με το C(4)=2×4+1=9*3 (mod. 6) που αντιστοιχεί στο γράμμα Δ.*
*Το γράμμα Ζ με το C(5)=2×5+1=11*5 (mod. 6) που αντιστοιχεί στο γράμμα Ζ.*

Παρατηρούμε πως το προτεινόμενο ομοπαραλληλικό κρυπτογράφημα κωδικοποιεί με τον ίδιο τρόπο τα μηνύματα «ΑΒΓ» και «ΔΕΖ». Είναι αδύνατο να ξέρουμε ποιο είναι το αρχικό μήνυμα. Τι συνέβη; Αν δουλέψουμε με ένα κρυπτογράφημα διατύπωσης $C_{(a,b)}$ (x) =(ax+b)= y (mod. n), θα μπορέσουμε να αποκρυπτογραφήσουμε το μήνυμα με μονοσήμαντο τρόπο, αν και μόνο αν ΜΚΔ(a, b)=1. Σ' αυτό το παράδειγμα, το ΜΚΔ(2,6)=2 δεν ικανοποιεί. Η μαθηματική πράξη αποκρυπτογράφησης ισοδυναμεί με την αναζήτηση του αγνώστου x, δεδομένου ότι η τιμή y είναι modulo n, δηλαδή:

$$C_{(a,b)}(x) = (ax + b) = y \text{ (mod. n)}$$
$$(ax + b)= y \text{ (mod. n)}$$
$$ax=y-b \text{ (mod. n)}.$$

Αυτό σημαίνει ότι ψάχνουμε μια τιμή α^{-1} (αντίστροφη του α) που να ικανοποιεί το $\alpha^{-1}\,\alpha$ = 1 με τέτοιον τρόπο ώστε:

$$A^{-1}\,\alpha x= \alpha^{-1}\,(y-b) \text{ (mod. n)}$$
$$x= a^{-1}\,(y-b) \text{ (mod. n)}.$$

Κατά συνέπεια, για να βεβαιωθούμε για την επιτυχία της αποκρυπτογράφησης, πρέπει να υπολογίσουμε τους αντίστροφους ενός αριθμού α modulo n, και για να μην κάνουμε άχρηστες προσπάθειες, για να ξέρουμε προκαταβολικά αν αυτοί οι αντίστροφοι αριθμοί υπάρχουν. Μια ομοπαραλληλική κρυπτογράφηση $C_{(a,b)}(x)=(\alpha x+b)$ (mod. 6) θα έχει αντίστροφο αν και μόνο αν ΜΚΔ (α,b)=1. Στο παράδειγμά μας, C(x)= 2x+1 (mod. 6), θα θέλαμε να ξέρουμε αν ο αριθμός α, ίσος εδώ με το 2, έχει αντίστροφο, δηλαδή αν υπάρχει ένα ακέραιο η μικρότερο του 6 ώστε 2 • n * 1 (mod. 6). Γι' αυτό δοκιμάζουμε όλες τις τιμές (0, 1, 2, 3, 4, 5): 2•0=0, 2•1=2,2•2=4,2•3=6*0,2•4=8,2•5=10*4

Καμία τιμή δεν ικανοποιεί στη συγκεκριμένη περίπτωση, επομένως το 2 δεν έχει αντίστροφο. Στην πραγματικότητα, το ξέραμε, εφόσον ΜΚΔ(2,6) ≠ 1. Έστω πως το μήνυμα «ΚΒΟCS» είχε υποκλαπεί και πως γνωρίζουμε πως είχε κωδικοποιηθεί με ένα ομοπαραλληλικό κρυπτογράφημα της μορφής C(x)=3x+3, γραμμένο με ένα παραδοσιακό αλφάβητο 26 γραμμάτων. Ποιο είναι το πρωτότυπο κείμενο; Πρώτα απ' όλα, ας υπολογίσουμε τον ΜΚΔ(3,26). Ισούται με 1: το μήνυμα μπορεί να αποκωδικοποιηθεί! Για το σκοπό αυτό, πρέπει να βρούμε την αντίστροφη λειτουργία του C(x)=3x+3 modulo 26. δηλαδή y=3x+3 άρα 3x=y–3. Για να απομονώσουμε το x, πρέπει να πολλαπλασιάσουμε τα δύο μέρη της εξίσωσης με το αντίστροφο του 3. Το αντίστροφο του 3 modulo 26 είναι ένα ακέραιο n του τύπου 3•n*1 (mod. 26), δηλαδή 9•3=27*1. Άρα X= 9 (y – 3).Τώρα μπορούμε να αποκωδικοποιήσουμε το μήνυμα. Το γράμμα Κ κατέχει τη θέση 10 και η

αποκωδικοποίησή του θα είναι 9(10-3) = 63*11 (mod. 26). Το γράμμα που κατέχει τη θέση 11 στο αλφάβητο είναι το L.

*Για το B 9(1-3)=18 + 26*8 (mod. 26) που αντιστοιχεί στο γράμμα I.*

*Για το O 9(14-3)=99*21 (mod. 26) που αντιστοιχεί στο γράμμα V.*

*Για το C 9(2-3)=-9+26*5 (mod. 26) που αντιστοιχεί στο γράμμα R.*

*Για το S 9(15-3)= 108*4 (mod. 26) που αντιστοιχεί στο γράμμα E.*

Το αποκωδικοποιημένο μήνυμα είναι «LIVRE», ΒΙΒΛΙΟ.

8. Πέραν του ομοπαραλληλικού ή αφινικού κρυπτογραφήματος

Επί αιώνες διάφορα συστήματα ασφάλειας βασίστηκαν στην ιδέα του κώδικα του Καίσαρα και στη γενίκευσή του που αποτελεί το ομοπαραλληλικό κρυπτογράφημα. Σήμερα ορίζουμε ως «κώδικα του Καίσαρα» κάθε κρυπτογράφημα για το οποίο κάθε γράμμα του πρωτότυπου μηνύματος αντικαθίσταται από ένα γράμμα μετατοπισμένο κατά συγκεκριμένο αριθμό θέσεων –όχι υποχρεωτικά όμως τρεις. Τώρα, απ' όλες τις ιδιότητες ενός αλγόριθμου, η πιο σημαντική είναι να μπορεί να παράγει μεγάλη ποσότητα κλειδιών. Τόσο ο συμβατικός κώδικας του Καίσαρα όσο και το ομοπαραλληλικό κρυπτογράφημα, το δεύτερο σε μικρότερο βαθμό, είναι ευάλωτα στην κρυπτανάλυση, λόγω του μικρού αριθμού κλειδιών που παράγουν. Αν εξαλείψουμε τους περιορισμούς που αφορούν τη σειρά των χαρακτήρων του κωδικοποιημένου αλφάβητου, ο δυνητικός αριθμός κλειδιών αυξάνεται αξιοσημείωτα.

Συνολικά απαριθμούμε 26!, δηλαδή 403.291.461.126.605.635.584.000.000 πιθανά κωδικοποιημένα αλφάβητα, δηλαδή 403 επτάκις εκατομμύρια κλειδιά. Ένας κατάσκοπος που θα δοκίμαζε ένα κλειδί κάθε δευτερόλεπτο θα χρειαζόταν πάνω από ένα δισεκατομμύριο φορές την εκτιμώμενη ζωή του σύμπαντος προτού εξαντλήσει όλες τις πιθανότητες.

Ένα τέτοιο πιθανό κλειδί ενός γενικού αλγόριθμου αντικατάστασης θα μπορούσε να είναι το ακόλουθο:

(1)	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
(2)	Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

(1) Κανονικό, (2) Κρυπτογραφημένο αλφάβητο

Τα έξι πρώτα γράμματα του κρυπτογραφημένου αλφάβητου αποτελούν τη βάση για να μαντέψουμε την επιλεγμένη οργάνωση: είναι η ακολουθία των γραμμάτων ενός συμβατικού πληκτρολογίου ονομαζόμενη «QWERTY».Για να κωδικοποιήσουμε το μήνυμα «VENI VIDI VICI» με το κλειδί QWERTY, ψάχνουμε για κάθε γράμμα, στο συμβατικό αλφάβητο, αυτό που του αντιστοιχεί στο κρυπτογραφημένο αλφάβητο.

(1)	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
(2)	Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

Τότε θα καταλήγαμε στο εξής κωδικοποιημένο μήνυμα: *CTFO CORO COEO*

Μ' αυτή τη μέθοδο κρυπτογράφησης, υπάρχει ένας απλός τρόπος για να παράγουμε έναν πρακτικά άπειρο αριθμό κλειδιών που απομνημονεύονται εύκολα. Αρκεί να συμφωνήσουμε στη λέξη-κλειδί ή σε μια φράση, και να την τοποθετήσουμε στην αρχή του κωδικοποιημένου αλφάβητου, και στη συνέχεια να συμπληρώσουμε τους υπόλοιπους χαρακτήρες με συμβατικό τρόπο ξεκινώντας από το τελευταίο γράμμα της λέξης-κλειδιού, φροντίζοντας να μην επαναλάβουμε κανένα χαρακτήρα. Ένα παράδειγμα αυτού είναι το «*CODE JANVIER*» («*ΚΩΔΙΚΟΣ ΙΑΝΟΥΑΡΙΟΣ*»). Κατ' αρχάς εξαλείφουμε το κενό και τους χαρακτήρες που επαναλαμβάνονται και έχουμε τη λέξη-κλειδί «CODEJANVIR».Το κωδικοποιημένο κατ' αυτό τον τρόπο αλφάβητο είναι το εξής:

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

Το μήνυμα «*VENI VIDI VICI*» αποκωδικοποιείται λοιπόν ως «*KJWI KIEI KIDI*».

Αυτό το σύστημα παραγωγής κλειδιών μπορεί με τέτοιον τρόπο ώστε τόσο ο αποστολέας όσο και ο παραλήπτης να έχουν λίγες πιθανότητες να σφάλουν και η πραγματοποίηση να είναι απλή. Στο παράδειγμα, θα αρκούσε ο αποστολέας και ο παραλήπτης να αλλάζουν το κλειδί «CODE JANVIER» («ΚΩΔΙΚΟΣ ΙΑΝΟΥΑΡΙΟΣ») κάθε μήνα με τη λέξη–κλειδί «CODE FEVRIER» («ΚΩΔΙΚΟΣ ΦΕΒΡΟΥΆΡΙΟΣ») και μετά «CODE MARS» («ΚΩΔΙΚΟΣ ΜΑΡΤΙΟΣ»), χωρίς να χρειάζεται να συνεννοηθούν πάνω από μία φορά για να συμφωνήσουν στο κλειδί. Η αξιοπιστία και η απλότητα του αλγόριθμου αντικατάστασης με λέξη–κλειδί έκαναν αυτό το σύστημα κρυπτογράφησης το πιο δημοφιλές για πολλούς αιώνες. Καθ' όλη αυτή την περίοδο, ήταν κοινώς παραδεκτό ότι οι κρυπτογράφοι είχαν σαφώς κερδίσει το παιχνίδι ενάντια στους κρυπταναλυτές.

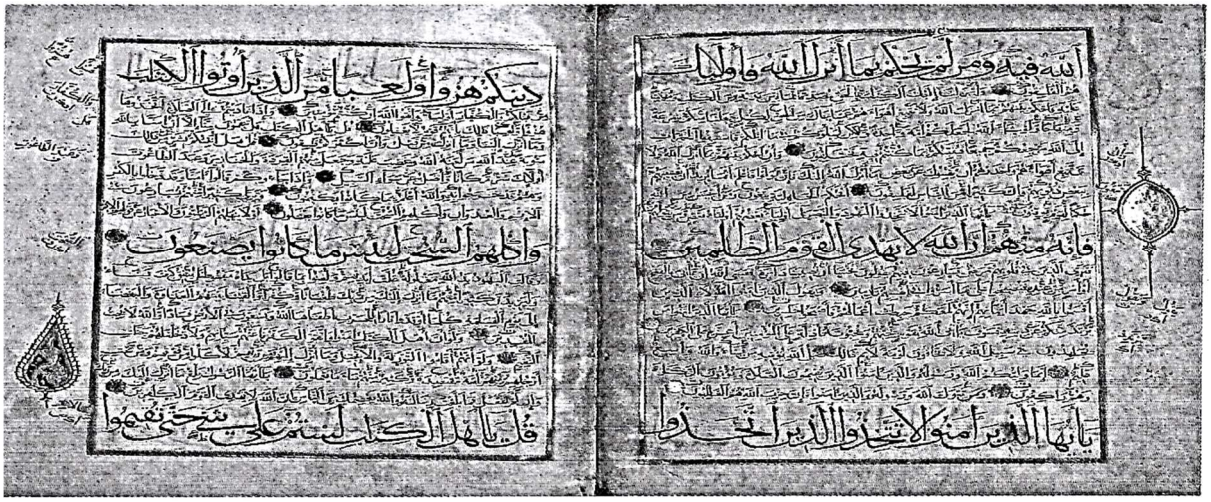
ΚΡΥΠΤΟΓΡΑΦΩΝΤΑΣ ΤΟ ΛΟΓΟ ΤΟΥ ΘΕΟΥ

Οι κρυπταναλυτές του Μεσαίωνα πίστεψαν ότι αποκάλυψαν τα κρυπτογραφήματα της Παλαιάς Διαθήκης και δεν είχαν άδικο. Πράγματι, αποσπάσματα του ιερού κειμένου είναι κωδικοποιημένα με μια κρυπτογράφηση αντικατάστασης που αποκαλείται *atbash*. Αυτό το κρυπτογράφημα συνίσταται στην αντικατάσταση κάθε γράμματος *n* με εκείνο που βρίσκεται σε απόσταση από το τέλος του αλφάβητου ίση με εκείνη του *n* από την αρχή. Για παράδειγμα, σ' ένα συμβατικό αλφάβητο, το Α θα αντικαθίστατο από το Ω, το Β από το Ψ κ.ο.κ. Στην περίπτωση της πρωτότυπης Παλαιάς Διαθήκης, οι υποκαταστάσεις γίνονται προφανώς βάσει του εβραϊκού αλφάβητου. Έτσι, στον Ιερεμία (25, 26), η λέξη «Βαβέλ» είναι κωδικοποιημένη ως «Seshach».

Εβραϊκή Βίβλος των αρχών του 18ου αιώνα.

9. Η ανάλυση συχνοτήτων

Το Κοράνι αποτελείται από 114 κεφάλαια, εκ των οποίων καθένα περιγράφει μια αποκάλυψη του Μωάμεθ. Αυτές οι αποκαλύψεις συλλέχθηκαν κατά τη διάρκεια της ζωής του προφήτη από διάφορους γραφείς και στη συνέχεια συγκεντρώθηκαν από τον Abu Bakr, τον πρώτο χαλίφη. Το έργο αυτό ολοκληρώθηκε από τον Όμαρ και τον Οθμάν, δεύτερο και τρίτο χαλίφη αντίστοιχα. Η αποσπασματική φύση των πρωτότυπων γραπτών αποτέλεσε αφορμή για τη δημιουργία ενός κλάδου της θεολογίας, αφιερωμένου στην ακριβή χρονολόγηση των διάφορων αποκαλύψεων, ενώ όσοι τις μελετούσαν χρησιμοποιούσαν, μεταξύ άλλων, την τεχνική μελέτης της συχνότητας εμφάνισης ορισμένων λέξεων που θεωρούσαν πιο σύγχρονες. Αν μια αποκάλυψη περιείχε επαρκή αριθμό τέτοιων λέξεων, μπορούσαν να υποθέσουν ότι ήταν σχετικά πιο πρόσφατη.



Χειρόγραφο του Κορανίου του 14ου αιώνα

Αυτές οι πρωτοβουλίες, καθώς και άλλες ακόμα, σχετικές με τη λεπτομερή μελέτη ιερών κειμένων, υπήρξαν η απαρχή του πρώτου επιστημονικού εργαλείου κρυπτανάλυσης που εφηύρε ο άνθρωπος: της ανάλυσης συχνοτήτων. Τα πρώτα γραπτά ίχνη αυτής της επαναστατικής μεθόδου είναι το έργο ενός λόγιου γεννημένου στη Βαγδάτη το 801, ονόματι al–Kindi. Υπήρξε αστρονόμος, γιατρός, μαθηματικός και γλωσσολόγος, αλλά η δουλειά του ως κρυπταναλυτή ήταν κυρίως αυτή που του προσέδωσε την αθάνατη φήμη του. Αν όχι ο πρώτος, είναι σίγουρα ο σημαντικότερος της ιστορίας.

Μόλις πρόσφατα μάθαμε τον πρωτοπόρο ρόλο που διαδραμάτισε. Το 1987, εμφανίζεται στα αρχεία της Κωνσταντινούπολης ένα αντίγραφο της πραγματείας του «Εγχειριδίου αποκρυπτογράφησης κρυπτογραφικών μηνυμάτων», απ' όπου μπορέσαμε να αντλήσουμε σημαντικά αποσπάσματα, όπως το εξής «Ένας τρόπος να λύσουμε ένα κρυπτογραφημένο μήνυμα, αν γνωρίζουμε τη γλώσσα, είναι να βρούμε ένα καθαρό κείμενο γραμμένο σ' αυτή τη γλώσσα, αρκετά μεγάλο, κι έπειτα να υπολογίσουμε πόσες φορές εμφανίζεται κάθε γράμμα. Το γράμμα που εμφανίζεται τις περισσότερες φορές θα ονομάζεται «πρώτο», το επόμενο «δεύτερο» και τούτο καθεξής, ώσπου να εξαντλήσουμε όλα τα γράμματα που εμφανίζονται στο μήνυμα. Στη συνέχεια κάνουμε το ίδιο και στο κείμενο που θέλουμε να αποκωδικοποιήσουμε και κατηγοριοποιούμε τα σύμβολά του με τον ίδιο τρόπο. Κατηγοριοποιώντας τα σύμβολα με φθίνουσα σειρά της συχνότητας εμφάνισης τους, τα αντικαθιστούμε με τα αντίστοιχα γράμματα ώσπου να εξαντλήσουμε όλα τα σύμβολα του κρυπτογράμματος που θέλουμε να αποκρυπτογραφήσουμε».

Είδαμε ότι στη μέθοδο κρυπτογράφησης με αντικατάσταση, ένα γράμμα του μηνύματος «διατηρεί τη θέση του αλλά αλλάζει ρόλο», κι αυτό ακριβώς το γεγονός ότι «διατηρεί τη θέση του» είναι που καθιστά εφαρμόσιμη την κρυπτανάλυση μέσω της μελέτης των συχνοτήτων. Η ιδιοφυΐα του al–Kindi αντέστρεψε τη σχέση δυνάμεων ανάμεσα στους κρυπτογράφους και τους κρυπταναλυτές, δίνοντας, τουλάχιστον μέχρι στιγμής, την εξουσία στα χέρια των κρυπταναλυτών.

10. Ένας λεπτομερές παράδειγμα

Τα γράμματα που εμφανίζονται συχνότερα στα γραπτά κείμενα στα γαλλικά είναι, με φθίνουσα σειρά συχνότητας: E S A I N T R U L O D C P M V Q G F H B X J Y Z K W. Ο παρακάτω πίνακας δίνει τις ποσοστιαίες συχνότητες εμφάνισης κάθε γράμματος.

A 8,01 %	H 0,88 %	O 5,43 %	U 6,00%
B 0,88 %	I 7,35 %	P 2,94 %	V 1,41%
C 3,23 %	J 0,44 %	Q 1,14 %	W 0,02 %
D 3,91 %	K 0,05 %	R 6,69 %	X 0,47 %
E 17,52 %	L 5,77 %	S 8,17 %	Y 0,30 %
F 1,06 %	M 2,90 %	T 7,07 %	Z 0,12 %
G 1,06 %	N 7,22 %		

Αν ένα μήνυμα ήταν κωδικοποιημένο με έναν από τους αλγόριθμους αντικατάστασης που μελετήσαμε προηγουμένως, μπορεί να αποκωδικοποιηθεί δυνάμει τη σχετικής συχνότητας εμφάνισης των χαρακτήρων του πρωτότυπου κειμένου. Αρκεί να υπολογίσουμε τον αριθμό εμφάνισης κάθε κωδικοποιημένου χαρακτήρα και να τον συγκρίνουμε με τον πίνακα συχνοτήτων της γλώσσας στην οποία ήταν γραμμένο. Έτσι, αν ο χαρακτήρας που εμφανίζεται συχνότερα κωδικοποιημένο κείμενο είναι το J, σημαίνει πως το πιθανό γράμμα του πρωτότυπου μηνύματος που του αντιστοιχεί είναι το E. Αν ο δεύτερος συχνότερος χαρακτήρας είναι το Z, ένας ανάλογος συλλογισμός οδηγεί στο ότι το S είναι το πιθανότερο αντίστοιχο γράμμα. Αυτή η διαδικασία επαναλαμβάνεται για όλους τους χαρακτήρες του κωδικοποιημένου μηνύματος για να ολοκληρωθεί η κρυπτανάλυση.

Είναι προφανές ότι αυτή η μέθοδος συχνοτήτων δεν μπορεί να εφαρμοστεί πάντα με τόσο άμεσο τρόπο. Οι συχνότητες του προηγούμενου πίνακα είναι σωστές για το σύνολο της γαλλικής γλώσσας. Οι συχνότητες του προηγούμενου πίνακα είναι σωστές για το σύνολο της γαλλικής γλώσσας. Μικρά κείμενα, όπως, παραδείγματος χάριν, «*En Virginie, et à Vancouver, le vert vif des vallèes verdoyantes est vivifiant*», παρουσιάζουν σχετικές συχνότητες εμφάνισης των γραμμάτων κατά πολύ διαφορετικές από εκείνες που χαρακτηρίζουν συνολικά τη γλώσσα. Στην πραγματικότητα, για κείμενα μικρότερα των 100 χαρακτήρων, αυτή η απλή ανάλυση σπανίως είναι χρήσιμη.

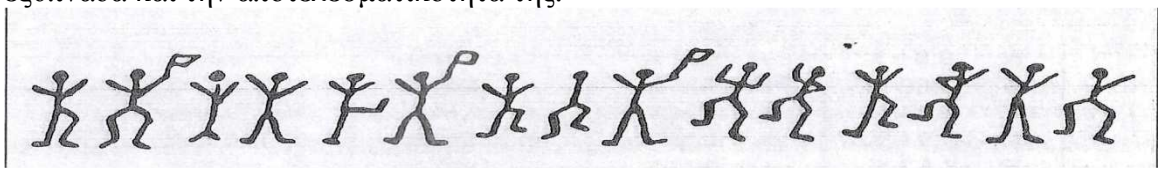
Αντίθετα, η ανάλυση συχνοτήτων δεν έχει λόγο να περιοριστεί μόνο στη μελέτη των γραμμάτων. Ακόμα κι αν δεχτούμε πως είναι απίθανο ο πιο συχνός χαρακτήρας ενός σύντομου κωδικοποιημένου κειμένου να είναι το E, μπορούμε ωστόσο να επιβεβαιώσουμε με μεγάλη σιγουριά πως τα πέντε γράμματα E, S, A, I ή N είναι τα πιο συχνά, χωρίς να γνωρίζουμε με βεβαιότητα αυτά στα οποία αντιστοιχούν. Από τα πέντε πιο συνηθισμένα γράμματα στα ισπανικά (A, E, L και O), αυτό που επαναλαμβάνεται συχνά είναι το L.

Έτσι, αν σε ένα ισπανικό μήνυμα βρούμε έναν από τους πέντε πιο συχνούς χαρακτήρες κι αν επιπλέον μερικές φορές είναι διπλός, τότε μπορούμε να εικάσουμε ότι στο πρωτότυπο κείμενο θα είναι ένα L. Ομοίως, είναι εξίσου πιθανό, ακόμα κι αν το κείμενο είναι μικρό, τα φωνήεντα να τείνουν να εμφανίζονται πριν και μετά από έναν αριθμό χαρακτήρων μεγαλύτερο από εκείνο των συμφώνων, που συνήθως σχετίζονται με άλλα φωνήεντα ή με μικρό αριθμό χαρακτήρων. Κατ' αυτό τον τρόπο μπορούμε μερικές φορές να αναγνωρίσουμε το A, το E και το I. Εφόσον καταφέρουμε να αποκρυπτογραφήσουμε μερικούς χαρακτήρες, εμφανίζονται λέξεις που τους λείπουν μόνο ένα ή δύο γράμματα, κάτι που μας επιτρέπει να κάνουμε υποθέσεις σχετικά με αυτά. Κατά συνέπεια, η ταχύτητα της αποκρυπτογράφησης αυξάνει περισσότερο από την απλή αναλογικότητα του αριθμού αποκρυπτογραφημένων χαρακτήρων. Εφαρμόζοντας αυτές τις ιδιαιτερότητες της συχνότητας εμφάνισης των γραμμάτων και ομάδων γραμμάτων, μπορούμε να επιτύχουμε την αποκρυπτογράφηση ακόμα και ξεκινώντας από ένα πολύ μικρό κείμενο.

11. Sherlock Holmes, ο κρυπταναλυτής

Η αποκρυπτογράφηση συχνοτήτων είναι μια μέθοδος πολύ αποτελεσματική και θεαματική που τράβηξε την προσοχή πολλών μυθιστοριογράφων. Η πιο διάσημη από τις ιστορίες που χτίστηκαν γύρω από την κρυπτανάλυση ενός μηνύματος είναι ίσως εκείνη του

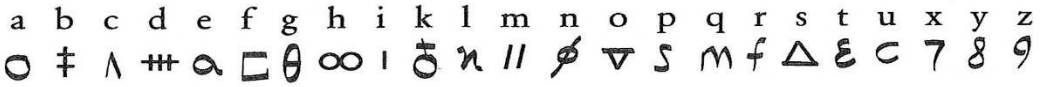
«Χρυσού Σκαραβαίου» που γράφτηκε το 1843 από τον Edgar Allan Poe. Κι άλλοι αφηγητές, όπως ο Ιούλιος Βερν ή ο Arthur Conan Doyle, χρησιμοποίησαν εξίσου παρόμοια μέσα για να προσθέσουν μυστήριο στις ιστορίες τους. Στο «The dancing men», ο Conan Doyle έβαλε τον Sherlock Holmes, αντιμέτωπο με ένα κωδικοποιημένο μήνυμα αντικατάστασης, του οποίου η λύση οδηγούσε τον επιθεωρητή στο να χρησιμοποιήσει την ανάλυση συχνοτήτων. Πάνω από χίλια χρόνια αργότερα, η ιδέα του al–Kindi συνέχισε να συνεπαίρνει το κοινό με την εξυπνάδα και την αποτελεσματικότητά της.



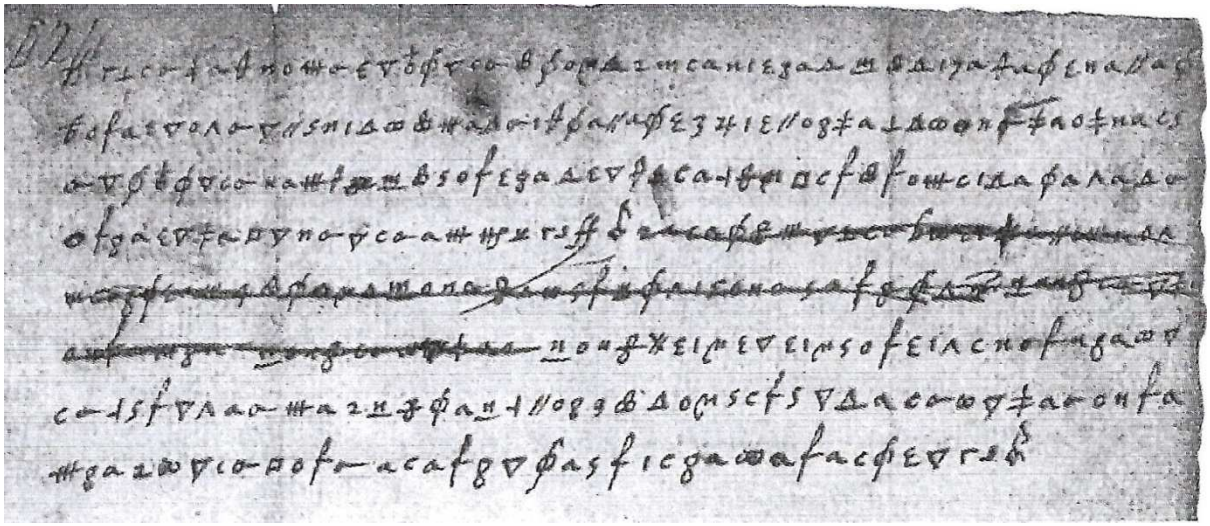
Το 1ο από τα μηνύματα κλειδιού που ο Sherlock Holmes έπρεπε να αποκρυπτογραφήσει στο The dancing men. Οι μικρές σημαίες που κρατούν τα ανθρωπάκια αποτελούν σημαντικό στοιχείο του κλειδιού.

12. Το πολυαλφαβητικό κρυπτογράφημα

Στις **08.02.1587**, η Μαρία, πρώην βασίλισσα της Σκοτίας, αποκεφαλίστηκε στο Λονδίνο, αφότου κρίθηκε ένοχη για έσχατη προδοσία. Η δίκη που προηγήθηκε αυτού του δραματικού γεγονότος είχε αποδείξει, χωρίς την παραμικρή αμφιβολία, τη συνεργασία της Μαρίας με μια ομάδα καθολικών αριστοκρατών με επικεφαλής τους το νεαρό Anthony Babington για τη δολοφονία της βασίλισσας Ελισάβετ της Αγγλίας, ώστε να πάρει η Μαρία τα σκήπτρα της βασιλείας του καθολικού βασιλείου, ενώνοντας τους Άγγλους με τους Σκότους. Οι βασικές αποδείξεις που παρουσιάστηκαν από την υπηρεσία αντικατασκοπείας της βασίλισσας Ελισάβετ υπό τη διεύθυνση του λόρδου Walsingham ήταν μια σειρά επιστολών της Μαρίας προς τον Babington που αποδεικνύουν ότι η νεαρή βασίλισσα γνώριζε το σχέδιο και το ενέκρινε. Οι εν λόγω επιστολές ήταν κρυπτογραφημένες με έναν αλγόριθμο που συνδύαζε κρυπτογράφημα και κώδικα, δηλαδή τα γράμματα όχι μόνο είχαν αντικατασταθεί από άλλους χαρακτήρες, αλλά είχαν χρησιμοποιηθεί και σύμβολα για να αντικαταστήσουν λέξεις που εμφανίζονταν συχνά. Το κωδικοποιημένο αλφάβητο που είχε χρησιμοποιήσει η Μαρία ήταν το ακόλουθο:



Εκτός από το γεγονός της χρήσης συμβόλων στη θέση των γραμμάτων, το κωδικοποιημένο αλφάβητο της Μαρίας δεν ήταν διαφορετικό από όλα εκείνα που έχουν χρησιμοποιηθεί ανά τους αιώνες από τους κρυπτογράφους ολόκληρου του κόσμου. Η νεαρή βασίλισσα και οι συνεργοί της ήταν βέβαιοι πως η κρυπτογράφηση ήταν ασφαλής, αλλά προς μεγάλη τους απογοήτευση, ο καλύτερος κρυπταναλυτής της Ελισάβετ, Thomas Phelippes, γνώριζε τη μέθοδο της ανάλυσης συχνοτήτων και μπόρεσε να αποκωδικοποιήσει τις επιστολές της Μαρίας χωρίς ιδιαίτερη δυσκολία. Η ανατροπή αυτού που ονομάστηκε «συνωμοσία Babington» δεν ήταν παρά μια ηχηρή προειδοποίηση στις κυβερνήσεις και στους πράκτορες ανά την Ευρώπη, ο συμβατικός αλγόριθμος αντικατάστασης δεν ήταν πια ασφαλής. Οι κρυπτογράφοι έμοιαζαν ανίσχυροι μπροστά στην εξουσία των νέων εργαλείων αποκρυπτογράφησης.



Απόσπασμα μιας εκ των επιστολών της Μαρίας της Σκοτίας στο συνωμότη Anthony Babington που θα την καταδικάσουν τελικά σε θάνατο

13. Η συνεισφορά του Alberti

Η λύση στο πρόβλημα που προκάλεσε η ανάλυση συχνοτήτων είχε ήδη δοθεί πριν από έναν αιώνα. Ο εφευρέτης του νέου κρυπτογραφήματος δεν ήταν άλλος από τον Leon Battista Alberti, τον μεγαλοφυή πολυπράγμονα της Αναγέννησης. Γνωστότερος ως αρχιτέκτονας, μαθηματικός και θεωρητικός της προοπτικής, ο Alberti είχε συλλάβει γύρω στο 1460 ένα σύστημα κρυπτογράφησης που συνίστατο στην πρόσθεση ενός δεύτερου αλφάβητου στο συμβατικό αλφάβητο, όπως δείχνει ο ακόλουθος πίνακας:

(1)	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	P	S	T	U	Y	V	X	Y	Z
(2)	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
(3)	M	N	B	V	C	X	Z	T	K	J	H	G	F	D	S	A	P	O	I	U	Y	L	R	E	W	Q

(1) Κανονικό, (2) Κρυπτογραφημένο & (3) Κρυπτογραφημένο αλφάβητο 2.

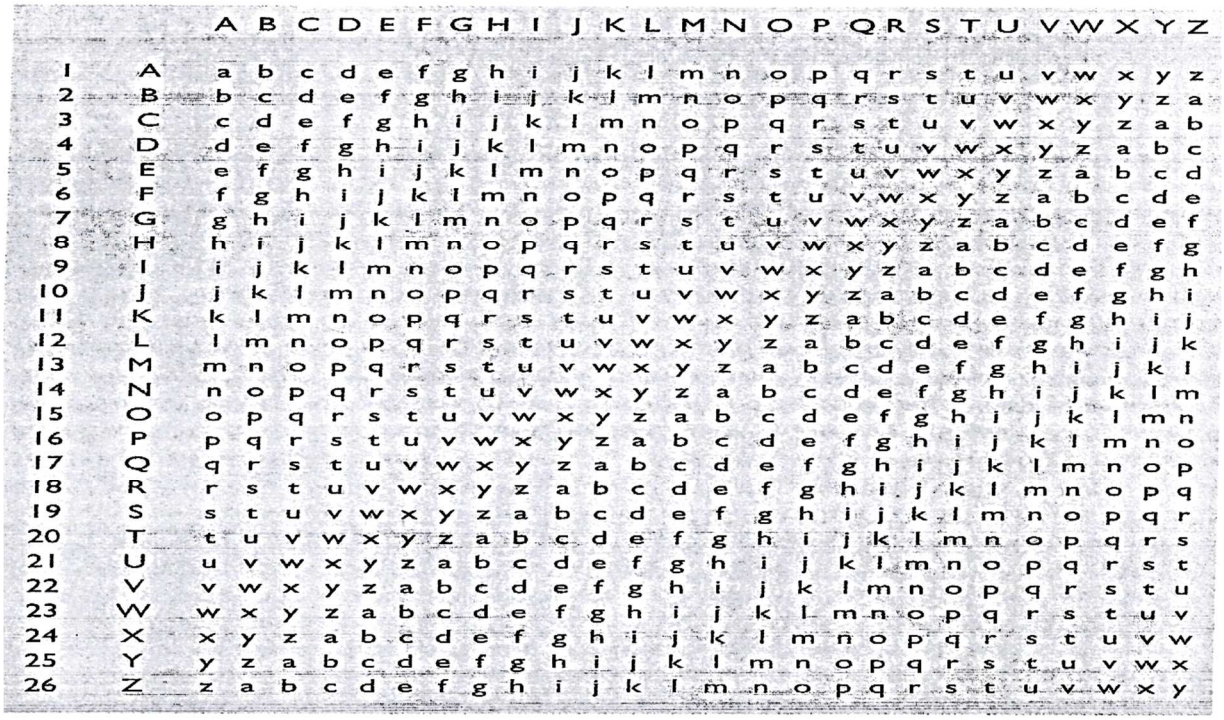
Για την κρυπτογράφηση ενός οποιουδήποτε μηνύματος, ο Alberti πρότεινε τη χρήση ενός κρυπτογραφημένου αλφάβητου εναλλάξ με ένα άλλο. Για παράδειγμα στην περίπτωση της λέξης «ATLAS», το κρυπτογράφημα του πρώτου γράμματος θα βρισκόταν στο πρώτο αλφάβητο (D), εκείνο του δεύτερου στο δέντρο (U) και ούτω καθεξής. Στο παράδειγμά μας το «ATLAS» θα γινόταν «DUOMV». Το πλεονέκτημα αυτού του πολυαλφαβητικού αλγόριθμου κρυπτογράφησης έναντι των προηγούμενων είναι προφανές από την πρώτη ματιά: ένας ίδιος χαρακτήρας Α του κανονικού κειμένου μπορεί να κρυπτογραφηθεί με δυο διαφορετικούς τρόπους, D και M. Και για να μπερδευτεί ακόμα περισσότερο ο κρυπταναλυτής που θα εκφοβιζόταν από ένα κείμενο κωδικοποιημένο με αυτόν τον τρόπο, ο ίδιος κρυπτογραφημένος χαρακτήρας θα μπορεί να αντικαταστήσει δύο χαρακτήρες του κανονικού κειμένου. Η ανάλυση συχνοτήτων χάνει σ' αυτό το σημείο ένα μεγάλο μέρος της χρησιμότητάς της. Ο διαπρεπής Ιταλός δεν θεώρησε ενδιαφέρον να αναπτύξει την ιδέα του και δεν άφησε καμία πραγματεία σχετικά με το θέμα αυτό, αλλά δύο άλλοι πανεπιστημιακοί, σχεδόν σύγχρονοί του, ο Γερμανός Johannes Trihemius και ο Γάλλος Blaise de Vigenere, κάλυψαν αυτό το κενό.

14. Το τετράγωνο του Vigenère

Σε έναν κώδικα του Καίσαρα, το κρυπτογράφημα είναι μονοαλφαβητικό. Στο κανονικό αλφάβητο αντιστοιχεί ένα μόνο κρυπτογραφημένο αλφάβητο, έτσι ώστε σε κάθε

γράμμα να αντιστοιχεί πάντα ο ίδιος κωδικοποιημένος χαρακτήρας (στον κλασικό κώδικα του Καίσαρα, στο γράμμα Α αντιστοιχεί πάντα το γράμμα Δ, στο Β το Ε και ούτω καθεξής).

Αντίθετα, σε μια πολυαλφαβητική κρυπτογράφηση, σε ένα δεδομένο γράμμα ενός μηνύματος, μπορεί να αντιστοιχούν τόσα γράμματα όσα και τα κωδικοποιημένα αλφάβητα που χρησιμοποιούνται. Για να κρυπτογραφήσουμε το κείμενο, περνάμε από το ένα κωδικοποιημένο αλφάβητο στο άλλο, όπως περνάμε και από το ένα γράμμα του κανονικού αλφάβητου στο άλλο. Το πρώτο και το πιο διάσημο από τα πολυαλφαβητικά κρυπτογραφήματα είναι γνωστό με το όνομα «τετράγωνο του Vigenère». Αυτού του είδους το κρυπτογράφημα αποτελείτε από ένα κανονικό αλφάβητο n χαρακτήρων, κάτω από το οποίο τοποθετούνται n κωδικοποιημένα αλφάβητα, εκ των οποίων καθένα μετατοπίζεται κατά ένα γράμμα προς τα αριστερά. Με άλλα λόγια, ένας πίνακας 26 γραμμάτων και 26 στηλών, όπως φαίνεται στο παρακάτω σχήμα.



		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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Πρέπει να επισημάνουμε τη συμμετρία των αντιστοιχιών ανάμεσα στα γράμματα, όπως παραδείγματος χάριν το ζεύγος (A, R)=(R, A), κάτι που ισχύει για όλα τα γράμματα.

Όπως μπορούμε να παρατηρήσουμε αμέσως, το τετράγωνο του Vigenère είναι ένα κανονικό αλφάβητο n χαρακτήρων, σε καθένα εκ των οποίων εφαρμόζεται ένας ομοπαραλληλικός μετασχηματισμός αυξουσών παραμέτρων. Έτσι, το πρώτο κωδικοποιημένο αλφάβητο θα ήταν ένα κρυπτογράφημα του Καίσαρα παραμέτρων a=1 και b=2, το δεύτερο ένα κρυπτογράφημα Καίσαρα με b=3 κ.ο.κ. Όσο για το κλειδί του τετραγώνου του Vigenère, πρέπει να ξέρουμε ποια είναι τα γράμματα του μηνύματος που πρέπει να κρυπτογραφήσουμε και κατά πόσες γραμμές μετατοπίζονται προς τα πίσω για να βρούμε τον αντίστοιχο χαρακτήρα. Ένα πιο απλό κλειδί είναι η μετατόπιση κατά μία γραμμή προς τα πίσω. Για κάθε γράμμα του πρωτότυπου μηνύματος. Έτσι, η φράση «*VENI VIDI VICI*» θα κωδικοποιούνται με τον ακόλουθο τρόπο:

Για να κωδικοποιήσουμε το πρώτο V, ψάχνουμε την αντιστοιχία στη γραμμή 1: είναι το V. Για να κωδικοποιήσουμε το πρώτο N, ψάχνουμε την αντιστοιχία στη γραμμή 1: είναι το P.

Το I (γραμμή 4): L *Το V (γραμμή 5): Z* *Το I (γραμμή 6): N*
Το D (γραμμή 7): J *Το I (γραμμή 8): P* *Το V (γραμμή 9): D*
Το I (γραμμή 10): R *Το C (γραμμή 11): M* *Το I (γραμμή 12): T*

ΠΑΙΖΟΝΤΑΣ ΜΕ ΤΟΥΣ ΔΙΣΚΟΥΣ

Ένας πρακτικός τρόπος να εφαρμόσουμε ένα πολυαλφαβητικό κρυπτογράφημα είναι η χρήση γνωστών μηχανισμών με το όνομα «δίσκοι Arberti». Αυτοί οι φορητοί κρυπτογράφοι έχουν ένα σταθερό πλαίσιο πάνω στο οποίο είναι χαραγμένο ένα συμβατικό αλφάβητο και πάνω σ' αυτό είναι στερεωμένη μια άλλη κυκλική ομόκεντρη και κινητή επιφάνεια, πάνω στην οποία είναι χαραγμένο ένα άλλο αλφάβητο. Ο αποστολέας μπορεί, περιστρέφοντας τον κινητό δακτύλιο, να αντιστοιχίσει το κανονικό αλφάβητο με τόσα κωδικοποιημένα αλφάβητα όσες είναι και οι θέσεις που υπάρχουν, δηλαδή το πολύ όσος είναι ο αριθμός χαρακτήρων του χρησιμοποιούμενου αλφάβητου. Το κρυπτογράφημα που προκύπτει από ένα δίσκο Arberti αντιστέκεται σθεναρά στην ανάλυση συχνοτήτων. Για να μπορέσει να αποκωδικοποιήσει το μήνυμα, ο παραλήπτης χρειάζεται μόνο να περιστρέψει το δίσκο με τον ίδιο τρόπο που το έκανε κι ο αποστολέας. Η ασφάλεια αυτής της κρυπτογράφησης, όπως κι εκείνη άλλων κρυπτογραφήσεων, έγκειται στο μυστικό των κλειδιών, δηλαδή στη σειρά του αλφάβητου του κινητού δακτυλίου, καθώς και της περιστροφής που πραγματοποιείται. Ένας δίσκος Arberti με έναν μόνο κινητό δακτύλιο, όπου είναι χαραγμένο ένα αλφάβητο διατεταγμένο με παραδοσιακό τρόπο, επιτρέπει την εφαρμογή ενός κρυπτογραφήματος του Καίσαρα με περιστροφή. Αυτού του είδους οι μηχανισμοί χρησιμοποιήθηκαν σε πρόσφατες μάχες, όπως σε εκείνη του πολέμου απόσχισης της Βόρειας Αμερικής. Ακόμα σήμερα αποτελούν κομμάτι των παιδικών παιχνιδιών κατασκοπείας.

Δίσκος Alberti που χρησιμοποιήθηκε από τους συμμάχους στον εμφύλιο πόλεμο της Βόρειας Αμερικής.

ΔΙΠΛΩΜΑΤΗΣ ΚΑΙ ΚΡΥΠΤΟΓΡΑΦΟΣ

Ο Blaise de Vigenere γεννήθηκε στη Γαλλία το 1523. Το 1549 εστάλη από τη γαλλική κυβέρνηση σε αποστολή στη Ρώμη όπου ασχολήθηκε με την κρυπτογραφία και με τα κωδικοποιημένα μηνύματα. Το 1585 έγραψε το θεμελιώδες έργο του, *Traite des chiffres,* όπου περιέγραφε μεταξύ άλλων το σύστημα κρυπτογράφησης στο οποίο έδωσε το όνομά του. Αυτό το σύστημα έμεινε απόρθητο για πάνω από δύο αιώνες, ώσπου ο Βρετανός Charles Babbage κατάφερε να το αποκρυπτογραφήσει γύρω στο 1854. Περιέργως, αυτή η προσπάθεια δεν ακολουθήθηκε από καμία άλλη ως το πρώτο μισό του 20ού αιώνα, όταν μια ομάδα ερευνητών επανεξέτασε τις προσωπικές του σημειώσεις.

Η κωδικοποιημένη πρωτότυπη φράση θα ήταν «VFPL ZNJP DRMT». Μπορεί κανείς να παρατήσει εύκολα ότι η συχνότητα των γραμμάτων του πρωτότυπου μηνύματος εξαφανίζεται. Ωστόσο, κάθε κρυπτογράφος ενδιαφέρεται για τα κλειδιά αυτά που μπορεί να θυμάται εύκολα, τόσο για τη διανομή όσο και για την εφαρμογή. Στην περίπτωση του τετράγωνου του Vigenère, αυτό μετατρέπεται σε πιο σύντομα κρυπτογραφήματα με τη μορφή λέξεων–κλειδιών που αποτελούνται από έναν αριθμό γραμμάτων μικρότερο ή ίσο εκείνου του μηνύματος που θέλουμε να κρυπτογραφήσουμε. Η λέξη–κλειδί χρησιμοποιείται ως εξής, γράφουμε τη λέξη κάτω από το κανονικό κείμενο επαναλαμβάνοντάς την όσες φορές χρειάζεται, μετά παίρνουμε τη συντεταγμένη της γραμμής και της στήλης, όπως στο καρτεσιανό σύστημα συντεταγμένων, και έτσι έχουμε το κρυπτογραφημένο μήνυμα. Η αντίστοιχη γραμμή σ' αυτή την περίπτωση είναι εκείνη που αρχίζει με το γράμμα του

χαρακτήρα της σχετικής λέξης-κλειδιού. Για παράδειγμα, αν θέλουμε να κρυπτογραφήσουμε το μήνυμα «*ATTAQUEZ LUNDI*» («*ΕΠΙΤΕΘΕΙΤΕ ΔΕΥΤΕΡΑ*») με το κλειδί «FEVRIER» («ΦΕΒΡΟΥΑΡΙΟΣ»):

Πρωτότυπο μήνυμα	A	T	T	A	Q	U	E	Z	L	U	N	D	I
Κλειδί	F	E	V	R	I	E	R	F	E	V	R	I	E
Κρυπτογραφημένο μήνυμα	F	X	O	R	Y	Y	V	E	P	P	E	L	M

Το κρυπτογραφημένο κείμενο είναι λοιπόν «FXORYYVEPPELM».

Ένα τετράγωνο του Vigenère με τις γραμμές να ορίζονται από τη λέξη-κλειδί «FEVRIER».

Όπως όλα τα συστήματα κλασικής κρυπτογράφησης, η αποκρυπτογράφηση ενός κωδικοποιημένου μηνύματος με ένα τετράγωνο Vigenère είναι συμμετρική σε σχέση με την κρυπτογράφηση. Στην περίπτωση του κωδικοποιημένου μηνύματος «CYCRAQGKE» με τη λέξη–κλειδί «CHAISE»:

Πρωτότυπο μήνυμα	;	;	;	;	;	;	;	;	;
Κλειδί	C	H	A	I	S	E	C	H	A
Κρυπτογραφημένο μήνυμα	C	Y	C	P	A	Q	G	K	E

Στην πρώτη γραμμή ψάχνουμε το άγνωστο «;» που επαληθεύεται (;, C)=C. Για να το βρούμε ψάχνουμε στη γραμμή του C ως τη στήλη όπου εμφανίζεται το C και βλέπουμε ότι είναι το κελί του A. Στη συνέχεια ψάχνουμε το γράμμα «;» που επαληθεύεται (;, H) = Y και καταλήγουμε στο R κ.ο.κ. Το πρωτότυπο κείμενο που αποκαλύπτεται είναι «ARCHIMEDE» («ΑΡΧΙΜΗΔΗΣ»). Η ιστορική σπουδαιότητα του τετραγώνου του Vigenère την οποία μοιράζεται με άλλα πολυαλφαβητικά κρυπτογραφήματα, όπως εκείνο του Gronsfeld (που αναπτύχθηκε την ίδια εποχή) είναι η ανθεκτικότητά του στην ανάλυση των συχνοτήτων. Αν ένας ίδιος χαρακτήρας μπορούσε να κωδικοποιηθεί με πολλούς τρόπους, χωρίς αυτό να καθιστά αδύνατη την τελική αποκρυπτογράφησή του, πώς λοιπόν θα μπορούσε κανείς να καταφέρει την κρυπτανάλυση του; Το ερώτημα παραμένει αναπάντητο για πάνω από 300 χρόνια.

15. Ταξινόμηση των αλφάβητων

Αν και χρειάστηκαν 8 αιώνες για να κάνουν την εμφάνισή τους, πολυαλφαβητικά κρυπτογραφήματα τύπου του τετραγώνου του Vigenère κατάφεραν επιτέλους να ξεγελάσουν

την ανάλυση συχνοτήτων. Περιέργως το πολυαλφαβητικό κρυπτογράφημα χρειάστηκε πολλά χρόνια για να επιβληθεί οριστικά. Τα παραδοσιακά μονοαλφαβητικά συστήματα, παρά τις αδυναμίες τους, είχαν το πλεονέκτημα της εύκολης εφαρμογής. Οι κρυπτογράφοι επιδίδονταν περισσότερο στη βελτιστοποίηση των διαδικασιών και στην τελειοποίηση των τεχνικών των αλγόριθμων, μένοντας όμως ουσιαστικά προσκολλημένοι στα εννοιολογικά πιο απλά κρυπτογραφήματα. Μία από τις πιο τελειοποιημένες παραλλαγές του μονοαλφαβητικού συστήματος είναι το κρυπτογράφημα αντικατάστασης, γνωστό με το όνομα ομοφωνικό κρυπτογράφημα, το οποίο επιδίωκε να εναντιωθεί στη στατιστική κρυπτανάλυση με τη βοήθεια μιας αύξησης του ποσοστού αντικατάστασης των χαρακτήρων με τη μεγαλύτερη συχνότητα εμφάνισης. Έτσι, αν το γράμμα Ε αντιπροσώπευε κατά μέσο όρο το 10% ενός γραπτού κειμένου σε οποιαδήποτε γλώσσα, το ομοφωνικό κρυπτογράφημα αντικατάστασης επιδίωκε να αντιστρέψει την τάση αυτή, αντικαθιστώντας το γράμμα Ε με 10 εναλλακτικούς χαρακτήρες. Η προτίμηση αυτής της μεθόδου και άλλων επιπλέον διατηρήθηκε ως και το πρώτο μισό του 18ου αιώνα. Αυτή η ανθεκτικότητα στην καινοτομία αποδείχτηκε γρήγορα ανώφελη.

Η εμφάνιση των μεγάλων Κρατών και της διπλωματίας που τα συνόδευαν επέφερε δραματική αύξηση της ζήτησης ασφαλών επικοινωνιών. Αυτή η τάση ενισχύθηκε από την εμφάνιση νέων τεχνολογιών επικοινωνίας, όπως του τηλέγραφου, που αύξησαν τον όγκο διακίνησης μηνυμάτων σε δυσθεώρητα ύψη. Τα μεγάλα ευρωπαϊκά έθνη εξοπλίστηκαν με αυτά που ονομάστηκαν «σκοτεινοί θάλαμοι», νευραλγικά κέντρα αφετηρίας των πλέον ευαίσθητων επικοινωνιών και άφιξης των υποκλεμμένων μηνυμάτων του εχθρού.

Η εξειδίκευση των σκοτεινών θαλάμων κατέστησε έτσι αβέβαιη κάθε μορφή μονοαλφαβητικής αντικατάστασης, ακόμα κι αν αυτή ήταν υπερβολικά αλλαγμένη. Σιγά σιγά οι βασικοί πράκτορες ανταλλαγής πληροφοριών κατέφυγαν στους πολυαλφαβητικούς αλγόριθμους. Στερούμενοι το πιο ισχυρό τους όπλο, την ανάλυση συχνοτήτων, οι κρυπταναλυτές έμειναν άπραγοι μπροστά στο χτύπημα των κρυπτογράφων.

ΟΙ ΚΡΥΠΤΟΓΡΑΦΟΙ ΤΟΥ ΒΑΣΙΛΙΑ ΗΛΙΟΥ

Παρότι λίγοι είναι αυτοί που γνωρίζουν την ύπαρξή τους, έξω από τον κύκλο της αυλής του Λουδοβίκου XIV, οι αδελφοί Antoine και Bonaventure Rossignol ήταν δύο από τους πιο ανήσυχους πολίτες στην ταραγμένη Ευρώπη του 17ου αιώνα. Η ικανότητά τους να αποκρυπτογραφούν τα μηνύματα των εχθρών της Γαλλίας κι επιπλέον ενός προσωπικού εχθρού του μονάρχη συνδυαζόταν με την εφευρετικότητά τους ως κρυπτογράφων. Σ' αυτούς οφείλουμε το «Μεγάλο Κρυπτογράφημα», ένα σύνθετο αλγόριθμο αντικατάστασης συλλαβών που χρησιμοποιήθηκε για την κρυπτογράφηση των εξαιρετικά σημαντικών μηνυμάτων που έγραφε ο βασιλιάς. Ωστόσο με το θάνατο των δύο αδελφών, το κρυπτογράφημα έπεσε σε αχρηστία και τελικά η λειτουργία του εξαφανίστηκε. Μόλις το 1890 ένας ειδικός στην κρυπτογραφία, ο εν αποστρατεία στρατιωτικός Etienne Bazeries, ανέλαβε το δύσκολο έργο να αποκρυπτογραφήσει τα κωδικοποιημένα έγγραφα κι έγινε ο ανυποψίαστος παραλήπτης των μυστικών μηνυμάτων του Βασιλιά Ήλιου.

Λουδοβίκος XIV, πορτρέτο του Mignard.

16. Ο ανώνυμος κρυπταναλυτής

Ο Βρετανός Charles Babbage (1791–1871) υπήρξε μια από τις πιο αξιοθαύμαστες επιστημονικές προσωπικότητες του 19ου αιώνα. Εφευρέτης ενός επαναστατικού για την

εποχή του υπολογιστή, της «διαφορικής μηχανής», ενδιαφερόταν γενικά για τα μαθηματικά και την τεχνολογία της εποχής του. Γνωρίζουμε μέσα από την ανταλλαγή επιστολών με ένα φίλο του, ότι ο Babbage αποφάσισε να εξασκήσει τις γνώσεις του στην αποκρυπτογράφηση πολυαλφαβητικών αλγόριθμων με το τετράγωνο του Vigenère. Για το σκοπό αυτό επικεντρώθηκε σε ένα χαρακτηριστικό αυτού του κρυπτογραφήματος.

Στην περίπτωση του κρυπτογραφήματος του Vigenère το μήκος της επιλεγμένης λέξης-κλειδιού καθόριζε τον αριθμό των χρησιμοποιούμενων κρυπτογραφημένων αλφάβητων. Έτσι, αν η λέξη–κλειδί ήταν «PAGE», κάθε χαρακτήρας του πρωτότυπου μηνύματος θα κωδικοποιούνταν το πολύ με τέσσερις διαφορετικούς τρόπους. Το ίδιο ίσχυε και με τις λέξεις. Σ' αυτό ήταν που βασίστηκε ο Babbage για να μελετήσει το πολυαλφαβητικό κρυπτογράφημα. Ας εξετάσουμε το παρακάτω παράδειγμα ενός κρυπτογραφημένου μηνύματος με τη βοήθεια του τετραγώνου του Vigenère.

Πρωτότυπο μήνυμα	L	E	V	E	R	T	E	T	L	E	R	O	S	E
Κλειδί	P	A	G	E	P	A	G	E	P	A	G	E	P	A
Κρυπτογραφημένο μήνυμα	A	E	B	I	G	T	K	X	A	E	X	S	H	E

Αμέσως παρατηρούμε ότι η συλλαβή «LE» του πρωτότυπου μηνύματος κωδικοποιείται με τους ίδιους χαρακτήρες, «AE» και στις δυο περιπτώσεις. Αυτό οφείλεται στο ότι ο διαχωρισμός των δύο συλλαβών του πρωτότυπου μηνύματος (8 γράμματα) είναι πολλαπλάσιος του αριθμού χαρακτήρων του χρησιμοποιούμενου κλειδιού (τέσσερα γράμματα). Με αυτή την πληροφορία κι ένα δεδομένο πρότυπο κείμενο επαρκούς μεγέθους, είναι δυνατό να εικάσουμε το μήκος της λέξεις–κλειδιού. Η διαδικασία έχει ως εξής: κάνουμε μια λίστα όλων των χαρακτήρων που επαναλαμβάνονται και του κενού που υπάρχει μεταξύ τους, έπειτα ψάχνουμε ακέραιους διαιρέτες των αριθμών των χαρακτήρων των κενών. Το μήκος της λέξεις κλειδιού είναι ένας από τους κοινούς διαιρέτες. Έστω ότι ο πιο πιθανός κοινός διαιρέτης, επειδή εμφανίζεται περισσότερο, είναι το 5. Πρέπει να μαντέψουμε σε ποιους χαρακτήρες αντιστοιχεί τώρα καθένα από τα πέντε γράμματα της λέξης κλειδιού.

Αν θυμηθούμε τη διαδικασία κρυπτογράφησης, κάθε γράμμα της λέξης του τετραγώνου του Vigenère καθορίζει ένα μονοαλφαβητικό κρυπτογράφημα του χαρακτήρα που αντιστοιχεί στο πρωτότυπο μήνυμα. Στην περίπτωση της υπόθεσής μας σχετικά με ένα κλειδί πέντε χαρακτήρων (C1, C2, C3, C4, C5), έκτος χαρακτήρας C6 κρυπτογραφείται με το ίδιο αλφάβητο με εκείνο που κρυπτογραφήθηκε ο $1^{ος}$ χαρακτήρας C1, ο $7^{ος}$ με εκείνο που κρυπτογραφήθηκε ο $2^{ος}$ C2 κ.ο.κ. Έτσι ο κρυπταναλυτής βρίσκεται στην πραγματικότητα μπροστά σε 5 μονοαλφαβητικά κρυπτογραφήματα, εκ των οποίων όλα μπορούν να υποβληθούν σε κρυπτανάλυση.

Η διαδικασία ολοκληρώνεται με τη σύνταξη πινάκων συχνοτήτων για όλους τους χαρακτήρες του κειμένου που είναι κρυπτογραφημένοι με τον ίδιο χαρακτήρα της λέξης–κλειδιού (C1, C6, C11... και C2, C7, C12... ώσπου να ολοκληρωθούν οι πέντε ομάδες χαρακτήρων ως το τέλος του μηνύματος) και στη συνέχεια με τη σύγκριση των πινάκων αυτών μ' εκείνους που χαρακτηρίζουν τη γλώσσα του μηνύματος. Αν αυτοί δεν συμπίπτουν, αφήνουμε αυτή την τιμή του μήκους του κλειδιού και παίρνουμε τη δεύτερη πιο πιθανή τιμή. Επαναλαμβάνοντας αυτή τη διαδικασία, μπορούμε να αναγνωρίσουμε τουλάχιστον μια πιθανή λέξη-κλειδί και έτσι μένει μόνο να αποκωδικοποιήσουμε το μήνυμα.

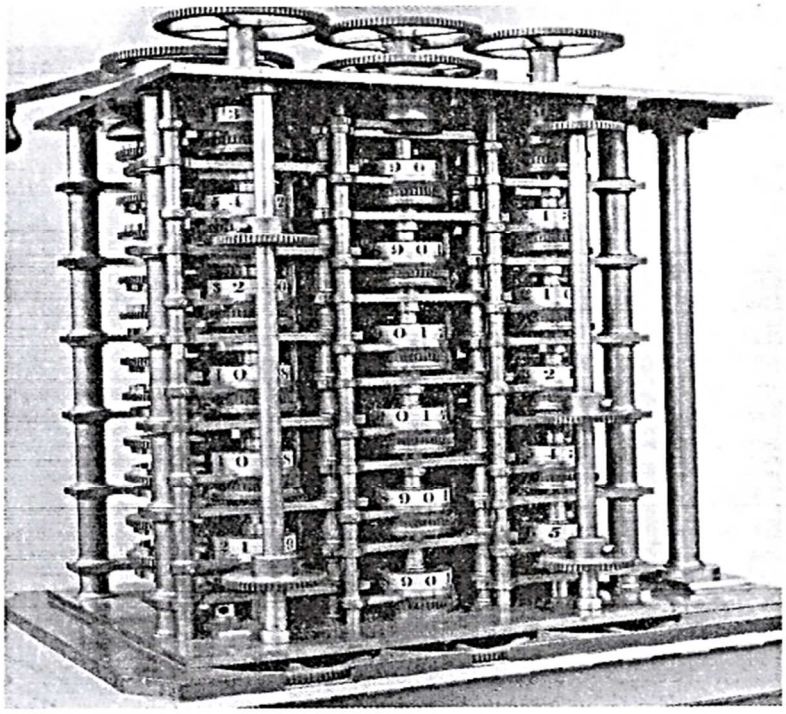
Το πολυαλφαβητικό κλειδί έσπασε. Αυτή η συναρπαστική άσκηση που πραγματοποίησε ο Babbage γύρω στο 1854 έμελλε να μείνει ωστόσο στην αφάνεια. Στην πραγματικότητα, η εκκεντρική αυτή διάνοια δεν δημοσίευσε ποτέ τις ανακαλύψεις του, και μόλις πρόσφατα, μετά από εξέταση των σημειώσεών του, αναγνωρίστηκε ως πρωτοπόρος στην αποκρυπτογράφηση του πολυαλφαβητικού κλειδιού. Κατά τύχη για τους

κρυπταναλυτές όλου του κόσμου, ο πρώσος αξιωματούχος Friedrich Krasinski δημοσίευσε μια παρόμοια μέθοδο μετά από λίγα χρόνια, το 1863. Ανεξάρτητα από το αν γνωρίζουμε ή όχι ποιος ήταν ο πρώτος που τα είχε καταφέρει, ήταν σαφές από δω και στο εξής ότι το πολυαλφαβητικό κρυπτογράφημα δεν ήταν πλέον ανεξιχνίαστο.

Από αυτή τη στιγμή, η δύναμη ενός κρυπτογραφήματος δεν θα εξαρτιόταν τόσο από τις μεγάλες καινοτομίες στον κλάδο των κρυπτογραφικών αλγόριθμων, αλλά από τον αριθμό των πιθανών κρυπτογραφημένων αλφάβητων, ο οποίος έπρεπε να είναι αρκετά μεγάλος για να καθιστά εντελώς άχρηστη την ανάλυση συχνοτήτων και των παραλλαγών της. Από την άλλη πλευρά της ροής πληροφοριών, ο στόχος ήταν η κατοχή μηχανισμών που να επιτρέπουν την επίσπευση της κρυπτανάλυσης. Αυτά τα δύο ερευνητικά ρεύματα συνέκλιναν προς έναν κοινό τόπο και έτσι δημιούργησαν μια ίδια διαδικασία, τη μηχανοποίηση.

17. Μηχανές που κωδικοποιούν

Ο 19ος αιώνας είδε τη χρησιμότητα των κωδίκων να ξεπερνά κατά πολύ την κρυπτογραφία. Η εφεύρεση του τηλέγραφου την τρίτη δεκαετία του αιώνα και η ανάπτυξη του διπλού τηλεγράφου, 30 χρόνια αργότερα, από τον Thomas Alva Edison, έφεραν επανάσταση στις επικοινωνίες και τελικά στον κόσμο ολόκληρο. Παρότι ο τηλέγραφος λειτουργούσε με ηλεκτρικές ωθήσεις, έπρεπε να χρησιμοποιηθεί ένα σύστημα που να μεταφράζει το περιεχόμενο των μηνυμάτων σε μια γλώσσα «κατανοητή» από τη μηχανή, δηλαδή έπρεπε να καθιερωθεί ένας κώδικας. Από όλες τις δυνατότητες που προσφέρονταν, αυτό ήταν ένα σύστημα από παύλες και τελείες, το οποίο συνέλαβε ένας Βορειοαμερικάνος ζωγράφος και ο φυσικός, ο Samuel Morse. Ο Κώδικας Morse μπορεί να θεωρηθεί ως πρόγονος των κωδίκων που, δεκάδες χρόνια αργότερα, θα επέτρεπαν στους χρήστες τους να εισάγουν την πληροφορία στους υπολογιστές και να την εξάγουν.



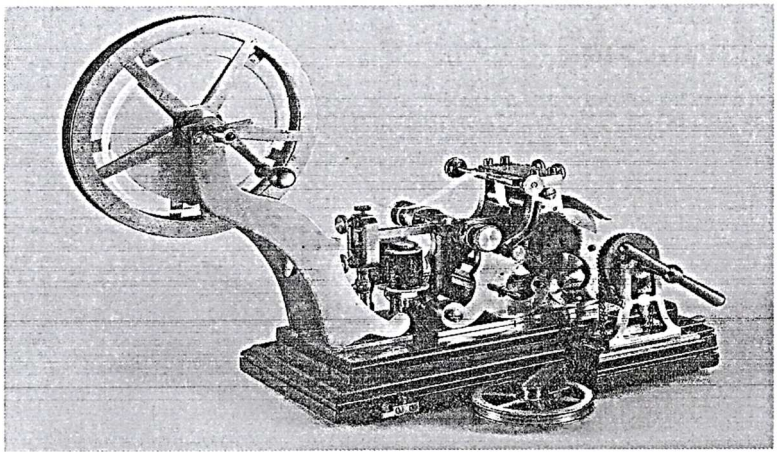
Η διαφορική μηχανή του Babbage που κατασκευάστηκε το 1991 σύμφωνα με τα σχέδια του εφευρέτη. Επιτρέπει την προσέγγιση λογαριθμικών και τριγωνομετρικών συναρτήσεων και την ταυτόχρονη χρήση των αστρολογικών πινάκων. Ο Babbage δεν κατάφερε να τη δει να λειτουργεί όσο ζούσε.

18. Ο κώδικας Morse

Ο κώδικας Morse αναπαριστά τα γράμματα του αλφαβήτου, τους αριθμούς και άλλα σύμβολα, μέσω ενός συνδυασμού τελειών, παυλών και κενών. Με αυτό τον τρόπο, επιτρέπει τη μετάφραση διάφορων συμβολικών αλφάβητων σε ένα μόνο, ικανό να περιγραφεί με τη

βοήθεια απλών, φωτεινών, ηχητικών ή ηλεκτρικών σημάτων. Κάθε τελεία αναπαριστά μία μονάδα χρόνου μέσης διάρκειας 1/25 του δευτερολέπτου, ενώ κάθε παύλα 3 μονάδες.

Τα κενά ανάμεσα στα γράμματα είναι 3 τελείες και ανάμεσα στις λέξεις 5. Αρχικά η ευρεσιτεχνία του Morse δεν είχε γίνει δεκτή στις ΗΠΑ ούτε στην Ευρώπη, ώσπου το 1843 πήρε κυβερνητική χρηματοδότηση, για να κατασκευάσει μια τηλεγραφική γραμμή μεταξύ Ουάσιγκτον και Βαλτιμόρης. Η πρώτη αναμετάδοση πραγματοποιήθηκε το 1844 και λίγο αργότερα ιδρύθηκε μια εταιρεία με σαφή στόχο την κάλυψη ολόκληρης της Βόρειας Αμερικής με τηλεγραφικές γραμμές. Όταν το 1860 ο Ναπολέων Γ του απένειμε βραβεία αναγνώρισης, πολλά τηλεγραφικά καλώδια διέτρεχαν ήδη τις ΗΠΑ και την Ευρώπη προς όλες τις κατευθύνσεις. Έως το θάνατο του Morse το 1872, την αμερικανική ήπειρο διέσχιζαν γραμμές μήκους πάνω από 300.000 km. Για τη μετάδοση και την παραλαβή τηλεγραφικών μηνυμάτων, χρησιμοποιούνταν αρχικά μια απλή συσκευή που είχε εφεύρει ο ίδιος ο Morse το 1844. Αυτή η συσκευή αποτελούνταν από ένα πλήκτρο μετάδοσης, που λειτουργούσε παράλληλα ως διακόπτης του ηλεκτρικού ρεύματος και ως ηλεκτρομαγνήτης που δεχόταν σήματα. Κάθε φορά που κάποιος πατούσε το πλήκτρο προς τα πίσω, γενικά με το δέκτη ή τον μέσο, πραγματοποιούνταν μια ηλεκτρική επαφή. Οι περιοδικές ωθήσεις που παράγονταν πιέζοντας το πλήκτρο στέλνονταν σε ένα ηλεκτρικό καλώδιο, αποτελούμενο από δύο χάλκινα νήματα. Αυτά τα καλώδια που στηρίζονταν από ξύλινους στύλους ένωναν τους διάφορους τηλεγραφικούς σταθμούς και συχνά εκτείνονταν για εκατοντάδες χιλιόμετρα χωρίς διακοπή.



Η συσκευή–παραλήπτης αποτελούνταν από έναν ηλεκτρομαγνήτη, με ένα κουβάρι χάλκινου νήματος γύρω από ένα σιδερένιο πυρήνα. Όταν το καλώδιο δεχόταν τις ωθήσεις ηλεκτρικού ρεύματος που αντιστοιχούσαν σε τελείες και παύλες, ο σιδερένιος πυρήνας μαγνητιζόταν και έλκυε ένα κινητό μέρος, επίσης από σίδερο, που εξέπεμπε έναν ξηρό, πολύ χαρακτηριστικό ήχο όταν χτυπούσε πάνω του που έμοιαζε με τακ. Το κενό που μεσολαβούσε ανάμεσα στα τακ ήταν σύντομο όταν επρόκειτο για τελεία και πιο μακρύ όταν επρόκειτο για παύλα. Για τη μετάδοση παραδοσιακών τηλεγραφημάτων, χρειαζόταν ένας χειριστής για να χτυπήσει την κωδικοποιημένη εκδοχή του μηνύματος και ένας άλλος για να τη διαβάσει.

Η μετάφραση των συμβατικών χαρακτήρων στον κώδικα Morse γινόταν βάσει του παρακάτω πίνακα:

ΣΗΜΑ	ΚΩΔΙΚΑΣ	ΣΗΜΑ	ΚΩΔΙΚΑΣ	ΣΗΜΑ	ΚΩΔΙΚΑΣ	ΣΗΜΑ	ΚΩΔΙΚΑΣ	ΣΗΜΑ	ΚΩΔΙΚΑΣ	ΣΗΜΑ	ΚΩΔΙΚΑΣ
A	• -	G	- - •	N	- •	T	-	0	- - - -	7	- - • •
B	- • • •	H	• • • •	Ñ	- - • - -	U	• • -	1	• - - - -	8	- - - • •
C	- • - •	I	• •	O	- - -	V	• • • -	2	• • - - -	9	- - - - •
CH	- - - -	J	• - - -	P	• - - •	W	• - -	3	• • • - -	.	• - • - •

											-
D	- • •	K	- • -	Q	- - • -	X	- • • -	4	• • • • -	,	- - • - -
E	•	L	• - • •	R	• - •	Y	- • - -	5	• • • • •	?	• • - - • •
F	• • - •	M	- -	S	• • •	Z	- - • •	6	- • • • •	“	• - • • - •

Έτσι το μήνυμα «Je t’aime» (Σε αγαπώ) θα μεταφραζόταν:

J	E	T	A	I	M	E
.---	.	-	.-	..	--	.

Ο Κώδικας Morse αποτελεί από μια άποψη μια πρώτη εκδοχή των μελλοντικών συστημάτων αριθμητικών επικοινωνιών. Για να εξηγήσουμε αυτή την ιδέα, αρκεί να δώσουμε την τιμή 1 στην τελεία και την τιμή 0 στην παύλα. Στις αρχές του 20ου αιώνα, η παραδοσιακή τηλεγραφία είχε ήδη αντικατασταθεί από την επικοινωνία χωρίς καλώδιο, η οποία ενισχύθηκε από την εφεύρεση του ραδιοφώνου και έτσι οι τηλεγραφητές ονομάστηκαν ραδιοτηλεγραφητές. Αυτή η νέα τεχνολογία επέτρεψε επιπλέον την πολύ γρήγορη μετάδοση.

Μεταδιδόμενα με τη μορφή ηλεκτρομαγνητικών κυμάτων, τα μηνύματα που εκπέμπονταν από το ραδιόφωνο μπορούσαν να υποκλαπούν σχετικά εύκολα. Αυτό εφοδίασε τους κρυπταναλυτές με τεράστιο όγκο κωδικοποιημένου υλικού, με το οποίο μπορούσαν να δουλέψουν και να παγιώσουν την ισχυρή θέση τους, δεδομένου ότι η πλειοψηφία των κρυπτογραφημάτων, ακόμα και των πιο ευαίσθητων, που χρησιμοποιούσαν οι κυβερνήσεις και οι μυστικοί πράκτορες βασιζόταν σε ήδη γνωστούς αλγορίθμους.

Για παράδειγμα, το κρυπτογράφημα Playfair που συνέλαβαν από κοινού δύο Βρετανοί, ο βαρόνος Lyon Playfair και ο Sir Charles Wheatstone, είναι μια μεγαλοφυής παραλλαγή του κρυπτογραφήματος του Πολύβιου, χωρίς όμως να είναι κάτι παραπάνω. Παρά τη μεγάλη ιδιοφυΐα των δημιουργών του, η αποκρυπτογράφηση αυτού του «ανακυκλωμένου» κρυπτογραφήματος δεν είναι τελικά παρά θέμα χρόνου και ικανότητας υπολογισμού. Η ιστορία της κρυπτογραφίας στον Α΄ Παγκόσμιο Πόλεμο το απεικονίζει τέλεια. Είδαμε προηγουμένως την αδυναμία του γερμανικού διπλωματικού κρυπτογραφήματος με αφορμή το «τηλεγράφημα Zimmermann». Αυτό που ακόμη και οι Γερμανοί δεν είχαν φανταστεί ήταν ότι ένα άλλο κρυπτογράφημά τους εκείνης της εποχής, γνωστό με το όνομα ADFGVX, που χρησιμοποιούνταν για την κωδικοποίηση των πιο ευαίσθητων μηνυμάτων από το μέτωπο θα γινόταν επίσης λεία των αντίπαλων κρυπταναλυτών, παρόλη την υποτιθέμενη άτρωτη δομή του. Το διπλό γερμανικό φιάσκο στον Α΄ Παγκόσμιο έκανε τους πάντες να συνειδητοποιήσουν την αναγκαιότητα μίας επιπλέον πιο ασφαλούς κρυπτογράφησης. Αυτός ο σκοπός έγινε θεμελιώδης προτεραιότητα, κάνοντας ακόμη πιο δύσκολη την κρυπτανάλυση. Η σύγκρουση ανάμεσα σε κρυπτογράφους και κρυπταναλυτές αποτελεί έναν μυστικό πόλεμο που διεξήχθη παράλληλα με τις παγκόσμιες αιματηρές συμπλοκές στο 1ο μισό του περασμένου αιώνα.

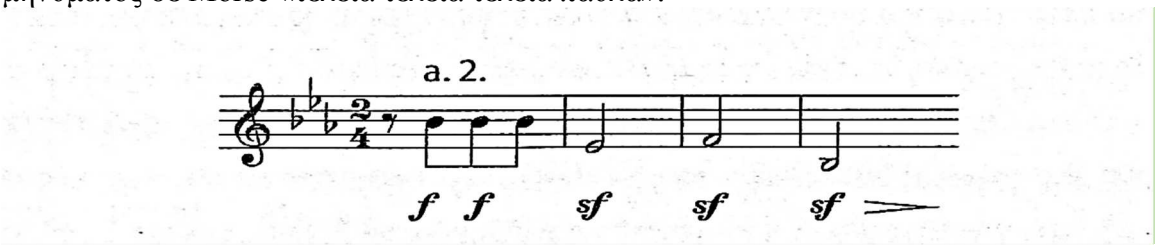
18.1 Σώστε την ψυχή μας

Η πιο γνωστή λέξη του κώδικα Morse είναι το σήμα της κλήσης σε βοήθεια SOS. Επιλέχθηκε για τον σκοπό αυτόν από μια επιτροπή ευρωπαϊκών χωρών για την απλότητα της μετάδοσής του (τρεις τελείες, τρεις παύλες, τρεις τελείες). Η λαϊκή κουλτούρα τού απέδωσε διάφορες έννοιες, μεταξύ άλλων, αυτή του «σώστε την ψυχή μας» (από το αγγλικό Save Ours Souls). Αργότερα, και λόγω της συχνής χρήσης του στη ναυσιπλοΐα, του αποδόθηκε η έννοια «σώστε το πλοίο μας» (από το αγγλικό Save Our Ship).

18.2 Συμφωνία σε V ματζόρε

Ο Beethoven ήταν άλλος ένας διάσημος κωφός που σχετίζεται με τον τηλέγραφο, αν και στη δική του περίπτωση εντελώς έμμεσα. Γεγονός είναι ότι τα πρώτα ακόρντα της 5ης

Συμφωνίας του μεγαλοφυούς συνθέτη αντιπροσώπευαν ένα ρυθμό παρόμοιο με εκείνον του μηνύματος σε Morse «τελεία τελεία τελεία παύλα».



Αυτή η ακολουθία τελείας και παύλας αντιστοιχεί στο γράμμα V, το πρώτο γράμμα της αγγλικής λέξης victory (νίκη). Για το λόγο αυτόν ο βρετανικός ραδιοφωνικός σταθμός BBC τη χρησιμοποίησε ως μουσικό σήμα των εκπομπών του προς την κατεχόμενη Ευρώπη κατά το Β' Παγκόσμιο Πόλεμο.

18.3 Μη προφορικές επικοινωνίες

Λόγω της κώφωσής του ο Thomas Alva Edison (1847–1931), επικοινωνούσε με τη σύζυγό του, Mary Stilwell, με τον Κώδικα Morse. Όταν ήταν ακόμη αρραβωνιασμένοι, ο Edison τη ζήτησε σε γάμο χτυπώντας τα σήματα πάνω στην παλάμη του και εκείνη του απάντησε με τον ίδιο τρόπο. Ο τηλεγραφικός κώδικας έγινε το συνηθισμένο μέσο επικοινωνίας ανάμεσα στο ζευγάρι, στο βαθμό που παρακολουθούσαν μια θεατρική παράσταση, ο Edison έβαζε το χέρι του επάνω στο γόνατο της Mary για να του «τηλεγραφεί» τους διαλόγους των ηθοποιών.

19. Ογδόντα km από το Παρίσι

Τον Ιούνιο του 1918, τα γερμανικά στρατεύματα ετοιμάζονταν να επιτεθούν στη γαλλική πρωτεύουσα. Για τους Συμμάχους, ήταν κομβικής σημασίας να υποκλέπτουν τις επικοινωνίες και να προβλέπουν πού θα γίνονταν οι συγκρούσεις. Τα γερμανικά μηνύματα που προορίζονταν για το μέτωπο κωδικοποιούνταν με το γνωστό κρυπτογράφημα ονόματι ADFGVX, που θεωρείτο άτρωτο. Το ενδιαφέρον αυτού του κρυπτογραφήματος έγκειται στο γεγονός ότι χρησιμοποιεί αλγόριθμους αντικατάστασης και μετάθεσης. Πρόκειται για μία από τις πιο άρτιες μεθόδους της κλασικής κρυπτογραφίας. Από το Μάρτιο του 1918, που υιοθετήθηκε από τους Γερμανούς, οι Γάλλοι προσπάθησαν απεγνωσμένα να το αποκρυπτογραφήσουν μόλις έμαθαν την ύπαρξη του. Κατά τύχη, ένας ταλαντούχος κρυπταναλυτής, ονόματι George Painvin, δούλευε στο κεντρικό γραφείο κρυπτογραφημάτων και αφοσιώθηκε νυχθημερόν σε αυτή τη δουλειά.

Το βράδυ της **02.06.1918**, ο Painvin κατάφερε να αποκρυπτογραφήσει το πρώτο μήνυμα. Το φρικτό του περιεχόμενο αφορούσε μια διαταγή προς το μέτωπο: «Στείλτε γρήγορα πολεμοφόδια. Ακόμη και σήμερα, αν δεν σας βλέπουν». Πριν από το μήνυμα, αναφερόταν ότι είχε σταλεί από ένα μέρος ανάμεσα στο Montdidier και στο Compiegne, περίπου 80 km βόρεια του Παρισιού. Το κατόρθωμα του Painvin επέτρεπε στους Γάλλους να εμποδίσουν την επίθεση, και έτσι μπόρεσαν να αναχαιτίσουν την πορεία του γερμανικού στρατού. Το κρυπτογράφημα ADFGVX, όπως αποκαλείται, γίνεται με δύο πράξεις: αντικατάσταση και μετάθεση. Σε πρώτο χρόνο, όσον αφορά στην αντικατάσταση, χρησιμοποιείται ένας πίνακας από επτά γραμμές και επτά στήλες, του οποίου η πρώτη γραμμή και η πρώτη στήλη συμπληρώνονται από τους χαρακτήρες ADFGVX. Στη συνέχεια, ο πίνακας συμπληρώνεται με 36 στοιχεία, αποτελούμενα από 26 γράμματα και 10 πρώτους αριθμούς, τοποθετημένα με τυχαίο τρόπο. Η διάταξη των στοιχείων αποτελεί το κλειδί του κρυπτογραφήματος και ο αποστολέας, προφανώς, χρειάζεται αυτή την πληροφορία για να αποκρυπτογραφήσει το μήνυμα. Ας υποθέσουμε ότι χρησιμοποιείται ο ακόλουθος πίνακας

	A	D	F	G	V	X
A	O	P	F	0	Z	C
D	G	3	B	H	4	K
F	A	I	7	J	R	2
G	5	6	L	D	E	T
V	V	M	S	N	Q	I
X	U	W	9	X	Y	8

Η κρυπτογράφηση συνίσταται στη μετάφραση κάθε χαρακτήρα του μηνύματος με ένα ζεύγος γραμμάτων από την ομάδα ADFGVX, σύμφωνα με την καρτεσιανή του αντιστοιχία. Γράφουμε πρώτα το γράμμα που αντιστοιχεί στη γραμμή και μετά το γράμμα που αντιστοιχεί στη στήλη. Με αυτό τον τρόπο, αν θέλουμε να κωδικοποιήσουμε τον αριθμό 4, θα γράψουμε «DV». Το μήνυμα «*Objectif Paris*» («*Στόχος Παρίσι*») θα κρυπτογραφούταν ως εξής:

O	b	j	e	t	i	f	P	a	r	i	S
AA	DF	FG	GV	GX	VX	AF	AD	FA	FV	VX	VF

Έως εδώ πρόκειται για απλή αντικατάσταση και για την αποκρυπτογράφηση του μηνύματος θα αρκούσε μια ανάλυση συχνοτήτων. Αλλά αυτή η κρυπτογράφηση περιέχει και μια δεύτερη φάση, χρησιμοποιώντας αυτή τη φορά τη μετάθεση. Η μετάθεση εξαρτάται από μια λέξη–κλειδί, συμφωνημένη από τον αποστολέα και τον παραλήπτη. Αυτή η δεύτερη φάση κρυπτογράφησης εφαρμόζεται με τον ακόλουθο τρόπο. Καταρχάς, δημιουργείται ένας πίνακας με τόσες στήλες όσα και τα γράμματα που περιέχει η λέξη–κλειδί.

Έπειτα συμπληρώνονται τα κελιά με το κρυπτογραφημένο κείμενο. Τα γράμματα της λέξης-κλειδί γράφονται στην πάνω γραμμή του νέου πίνακα. Στο παράδειγμά μας, θα χρησιμοποιήσουμε ως κλειδί τη λέξη BETA. Φτιάχνουμε έναν άλλο πίνακα, του οποίου η πρώτη γραμμή περιέχει αυτή τη λέξη και οι επόμενες τους χαρακτήρες του κρυπτογραφημένου μηνύματος με αντικατάσταση. Τα υπόλοιπα κελιά συμπληρώνονται από τους χαρακτήρες του αριθμού 0, που σύμφωνα με τον πρώτο πίνακα, κωδικοποιείται ως «AG». Όλη η διαδικασία είναι η περίπτωση του μηνύματος «*Objectif Paris*». Υπενθυμίζουμε το αποτέλεσμα της κρυπτογράφησης με αντικατάσταση:

AA	DF	FG	GV	AX	GX	VA	AF	AD	FA	FV	VX	VF

Ας πάρουμε το BETA ως λέξη–κλειδί, και ιδού ο νέος πίνακας:

B	E	T	A
A	A	D	F
F	G	G	V
A	X	G	X
V	X	A	F
A	D	F	A
F	V	V	X
V	F	A	G

Ας συνεχίσουμε με την κρυπτογράφηση μετάθεσης και ας αλλάξουμε τις στήλες με τέτοιο τρόπο ώστε τα γράμματα του κλειδιού να τοποθετηθούν με αλφαβητική σειρά. Τότε έχουμε τον παρακάτω πίνακα:

A	B	E	T
F	A	A	D
V	F	G	G
X	A	X	G
F	V	X	A
A	A	D	F
X	F	V	V
G	V	F	A

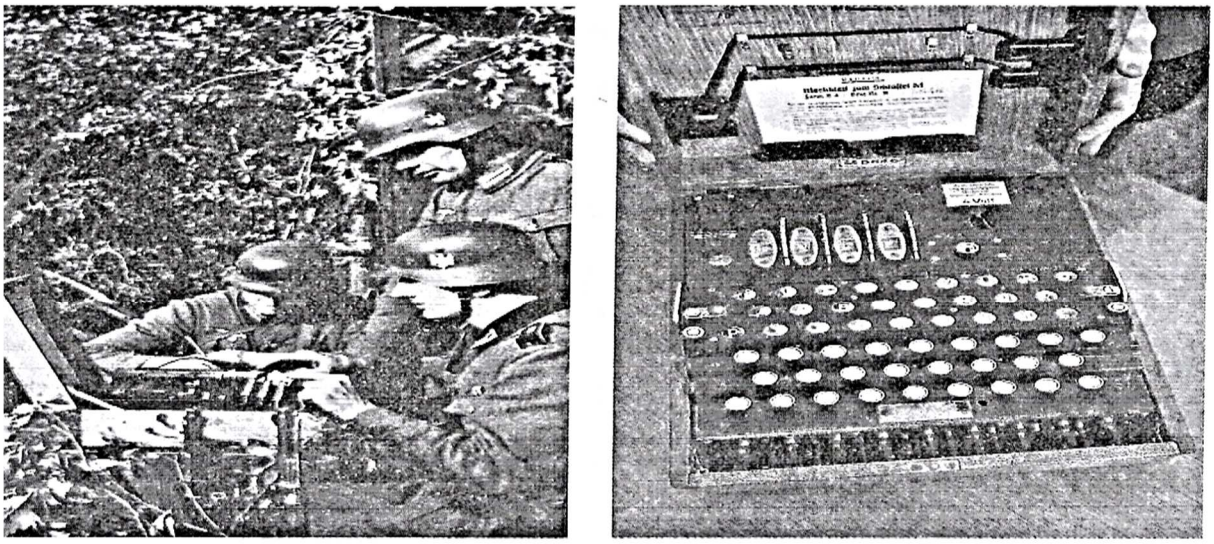
Φτιάχνουμε το κρυπτογραφημένο μήνυμα παίρνοντας τα γράμματα του πίνακα ανά στήλες. Στο παράδειγμα μας, αυτό γίνεται FVXFAXGAFAVAFVAGXXDVFDGGAFVA. Το μήνυμα είναι ένα τυχαίο συνονθύλευμα των χαρακτήρων A, D, F, G, V και X. Προφανώς, πρόκειται για ένα παράδειγμα ex professo που προέκυψε από τον αρχικό πίνακα. Οι Γερμανοί επέλεξαν αυτούς τους έξι χαρακτήρες, επειδή οι αντίστοιχες μεταφράσεις τους σε σήματα Morse διέφεραν πολύ, γεγονός που επέτρεπε στον αποδέκτη του μηνύματος να ανιχνεύσει πιθανά σφάλματα μετάδοσης. Επιπλέον, καθώς αποτελούνταν από έξι μόνο χαρακτήρες, η τηλεγραφική μετάδοση ήταν απλή και εύκολη ακόμη και για αρχάριους χειριστές. Ρίχνοντας μια ματιά στον πίνακα του κώδικα Morse στην αρχή αυτού του κεφαλαίου, παρατηρούμε ότι η αντιστοιχία κάθε χαρακτήρα του κρυπτογραφήματος ADFGVX είναι η εξής A= . – D=–.. F=..–. G=– –. V=…- X=–..– Ο παραλήπτης δεν χρειάζεται παρά την τυχαία κατανομή των χαρακτήρων του πίνακα βάσης και της λέξης–κλειδί για να αντιστρέψει την κωδικοποίηση και να βρει το μήνυμα.

20. Η μηχανή Enigma

Το 1923, ο Γερμανός μηχανικός Arthur Scherbius πατεντάρισε μια μηχανή με στόχο τη διευκόλυνση των προστατευμένων επικοινωνιών. Η ονομασία της Enigma, έγινε συνώνυμη του στρατιωτικού απορρήτου και παραπέμπει σε εικόνες υπόγειων εργαστηρίων και μηχανών περίπλοκης δομής. Παρ' όλη την επιτήδευση της, η μηχανή Enigma δεν είναι στην ουσία παρά μια βελτιωμένη παραλλαγή του δίσκου του Alberti. Λόγω της σχετικής ευκολίας της χρήσης της και της πολυπλοκότητας που επιτρέπει στην κρυπτογράφηση, η μηχανή Enigma επιλέχθηκε από τη γερμανική κυβέρνηση ως βάση κωδικοποίησης ενός μεγάλου μέρους των στρατιωτικών της επικοινωνιών κατά τη διάρκεια του Β΄ Παγκοσμίου Πολέμου. Η αποκρυπτογράφηση του Enigma έγινε, έτσι, απόλυτη προτεραιότητα για τις κυβερνήσεις που αντιστέκονταν στη ναζιστική Γερμανία.

Όταν τελικά επιτεύχθηκε αυτός ο στόχος, τα μηνύματα που υπέκλεπταν και αποκρυπτογραφούσαν οι συμμαχικές υπηρεσίες πληροφοριών ήταν θεμελιώδους σημασίας ως προς τη λήψη των τελικών αποφάσεων για την έκβαση της μάχης. Η ιστορία της αποκρυπτογράφησηw του Enigma είναι συναρπαστική, με τους βασικούς πόλους να διαδραματίζονται κυρίως από τις υπηρεσίες πληροφοριών της Πολωνίας και του Ηνωμένου Βασιλείου. Ανάμεσα στους ήρωες της, ένας ιδιοφυής μαθηματικός, ο Alan Turning, είναι ο άνθρωπος που θεωρείται ο πατέρας της σύγχρονης πληροφορικής. Η περιπέτεια που διαδραματίστηκε μέχρι να σπάσει ο κώδικας Enigma είχε ως αποτέλεσμα επιπλέον τον πρώτο υπολογιστή της ιστορίας – κάτι που μπορεί να θεωρηθεί ως το πιο θεαματικό επεισόδιο της μακρόχρονης και γραφικής ιστορίας της στρατιωτικής κρυπτανάλυσης. Η μηχανή Enigma ήταν μια ηλεκτρομαγνητική μηχανή παρόμοια με μια γραφομηχανή. Αποτελούνταν από ένα πληκτρολόγιο και ένα φωτεινό πίνακα 26 γραμμάτων, από τρείς αναδιατάκτες επάνω σε άξονες, με 26 πιθανές θέσεις, και από έναν πίνακα βυσμάτων ανάμεσα στο πληκτρολόγιο και στον πρώτο αναδιατάκτη, του οποίου ο ρόλος ήταν να πραγματοποιεί μια πρώτη ανταλλαγή γραμμάτων, ανάλογα με τον τρόπο που ήταν τοποθετημένα τα βύσματα. Η φυσική διαδικασία κρυπτογράφησης ήταν σχετικά απλή.

Κατ' αρχάς, ο αποστολέας διέθετε τα βύσματα και τους αναδιατάκτες στη θέση εξόδου που καθοριζόταν από το βιβλίο των κλειδιών που ίσχυαν τη συγκεκριμένη στιγμή. Στη συνέχεια, εισάγει στο πληκτρολόγιο το πρώτο γράμμα του καθαρού μηνύματος και η μηχανή δημιουργούσε με αυτόματο τρόπο ένα άλλο γράμμα, που εμφανιζόταν στο φωτεινό πίνακα, το πρώτο γράμμα του κρυπτογραφημένου μηνύματος.

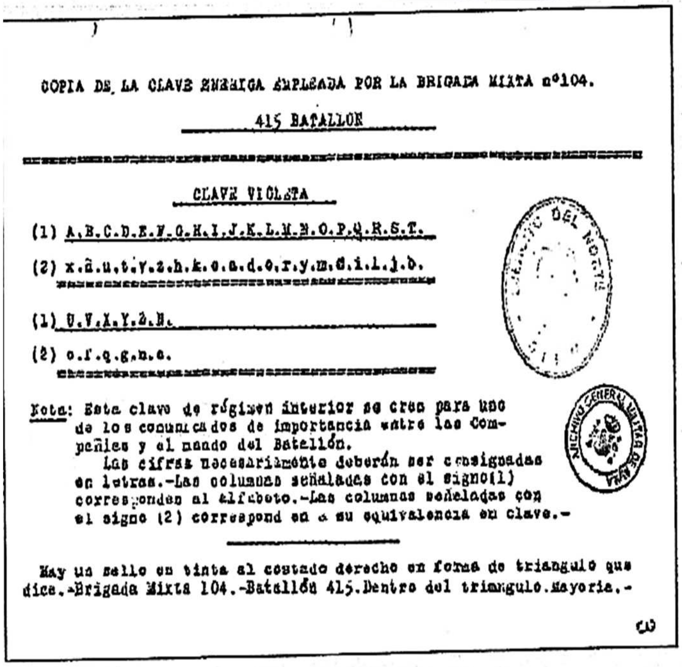


Γερμανοί στρατιώτες μεταγράφουν κρυπτογραφημένα μηνύματα με τη βοήθεια της μηχανής Αίνιγμα κατά το Β΄ Παγκόσμιο Πόλεμο. Δεξιά, μια μονάδα με τέσσερις αναδιατάκτες.

21. Η λεγόμενη «κρυπτογράφηση των χαρακωμάτων»

A	B	C	D	E	F	G	H	Y	I
53-91	12-70	40-86	31	27-43	24	16	11	40-59	22
L	M	N	O	P	Q	R	S	T	U
13	15	96-66	84-39	75	71	28-54	28-54	19	74-44

Στο μέτωπο, η χρήση κρυπτογραφημάτων τόσο πολύπλοκων όσο και το σύστημα ADFGVX ήταν μερικές φορές κοπιαστική. Κατά τη διάρκεια του ισπανικού εμφύλιου του 1936–1939, χρησιμοποιούνταν πολλοί στοιχειώδεις αλγόριθμοι αντικατάστασης, όπως ο εξής: Πολλά γράμματα έχουν πάνω από μία κρυπτογραφημένη εκδοχή. Το R, παραδείγματος χάρη, αντικαθίσταται είτε από το 28 είτε από το 54. Η λέξη «*GUERRE*» («*ΠΟΛΕΜΟΣ*») θα κωδικοποιούνταν σύμφωνα με αυτό το ν πίνακα ως 167427285453. Αυτοί οι κώδικες για ακριβείς κωδικοποιήσεις. Το εθνικιστικό στρατόπεδο, υπό το στρατηγό Φράνκο, διέθετε για τις πιο σημαντικές επικοινωνίες του ένα άλλο όπλο, 30 μηχανές Enigma, που του είχε προμηθεύσει το Ράιχ. Αυτή αποτελεί την πρώτη εντατική χρήση του ευφυούς κρυπτογραφήματος που θα χρησιμοποιούσε η Γερμανία στο Β΄ Παγκόσμιο Πόλεμο. Οι Βρετανοί θα προσπαθήσουν να «σπάσουν» το κρυπτογράφημα, αλλά ανεπιτυχώς.



COPIA DE LA CLAVE ENEMIGA EMPLEADA POR LA BRIGADA MIXTA nº104.

415 BATALLON

CLAVE VIOLETA

(1) A.B.C.D.E.F.G.H.I.J.K.L.M.N.O.P.Q.R.S.T.

(2) x.ã.u.t.y.z.h.k.e.a.d.o.r.y.m.d.i.l.j.b.

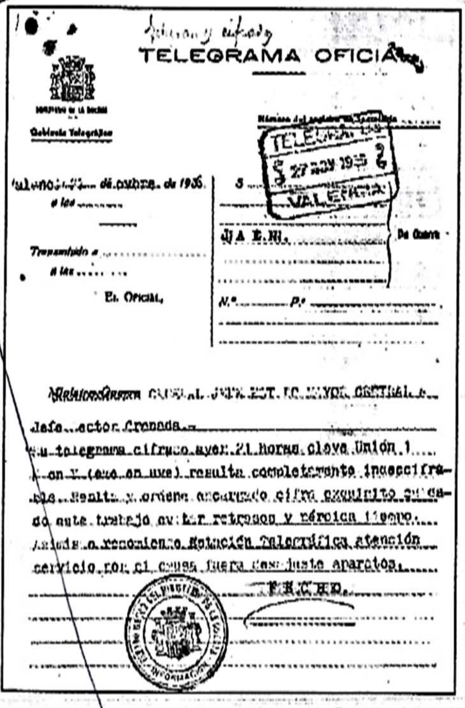
(1) U.V.X.Y.Z.N.

(2) o.f.q.g.n.e.

Nota: Esta clave de régimen interior se creo para uso de los comunicados de importancia entre las Compañias y el mando del Batallón.
Las cifras necesariamente deberán ser consignadas en letras.-Las columnas señaladas con el signo(1) corresponden al alfabeto.-Las columnas señaladas con el signo (2) correspond en a su equivalencia en clave.-

Hay un sello en tinta al costado derecho en forma de triangulo que dice.-Brigada Mixta 104.-Batallón 415.Dentro del triangulo.Mayoria.-

Κλειδί Βιολέτα που χρησιμοποιήθηκε από το απόσπασμα 415, δημοκρατική ταξιαρχία 104, και υποκλάπηκε από το εθνικιστικό στρατόπεδο: «Τα κρυπτογραφήματα θα πρέπει να καταχωριστούν με γράμματα. Οι στήλες με το σήμα (1) αντιστοιχούν στο αλφάβητο. Οι στήλες με το σήμα (2) αντιστοιχούν στο κρυπτογραφημένο αντίστοιχό τους».



TELEGRAMA OFICIAL

Gabinete Telegráfico

Valencia ... de octubre de 1936.

á las ...

Transmitido a ...

á las ...

El Oficial,

JJ A E.M.

De Guerra

N.º ... P.º ...

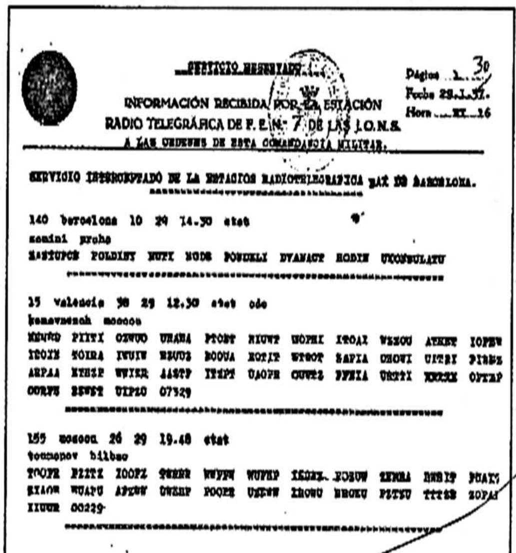
[illegible] GENERAL JEFE EST. DO MAYOR CENTRAL a

Jefe sector Granada.

Su telegrama cifrado ayer 21 horas clave Unión 1 ... on ... resulta completamente indescifrable. Ruego ordene encargado cifra exquisito cuidado este trabajo evitar retrasos y pérdida tiempo. ... Telegráfica atención servicio ... causa fuera ... aparatos.

FECHO.

27 Οκτωβρίου 1936. Στον επικεφαλής του (δημοκρατικού) τομέα χειροβομβίδων: «Το χθεσινό κρυπτογραφημένο τηλεγράφημά σας... παραμένει μη αποκρυπτογραφημένο».



SERVICIO RESERVADO

INFORMACIÓN RECIBIDA POR LA ESTACIÓN RADIO TELEGRÁFICA DE F. E. Nº 7 DE LAS J.O.N.S.

A LAS ORDENES DE ESTA COMANDANCIA MILITAR.

Página 1 30

Fecha 29.I.37.

Hora ... 16

SERVICIO INTERCEPTADO DE LA ESTACION RADIOTELEGRAFICA ... DE BARCELONA.

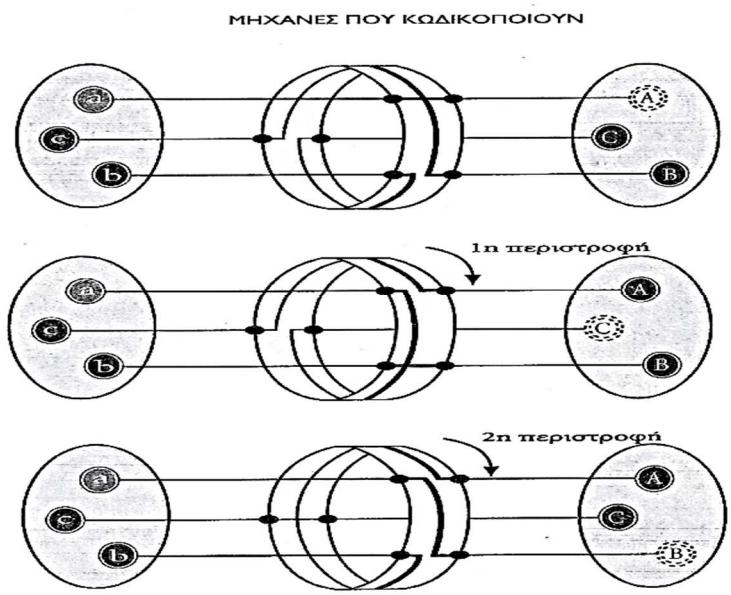
140 barcelona 10 29 14.30 etat
somini proho
ZASTUPCE POLDINY NUTI NODE POSUELI DVANACT HODIN UKONSULATU

15 valencia 30 29 12.30 etat odo
komavnezah moscou
MENUO PIITI OZWUO URANA PTOBT NIUWT UOPHI ITOAI WEZOU ATHET IOPEW
ITOIE TOIRA IWUIW ESUOZ BOOUA EOTIT WTEOT SAPIA OHOWI UITEI PIREZ
ARPAA ETHIP WWIER AASTP ITTPT UAOPE OUWTZ PYNIA URTTI NERRE OPTAP
OURVS ZEWET UIPZO 07329

155 moscou 26 29 19.48 etat
tovmonov bilbao
TOOPE PZITZ IOOPZ TEENE WWYPN WUPEP IEUEE EOZUW ZENEA DNEIP PUAT
EIAOE WUATU APZEW UWEEP POOPE UEEWW IEOWU NEOEU PZTEU TTTEE ZOPA
IIUUR 00229-

29 Ιανουαρίου 1936. Μηνύματα δημοκρατικών που υποκλάπηκαν από την ισπανική φάλαγγα των JONS στα Κανάρια Νησιά.

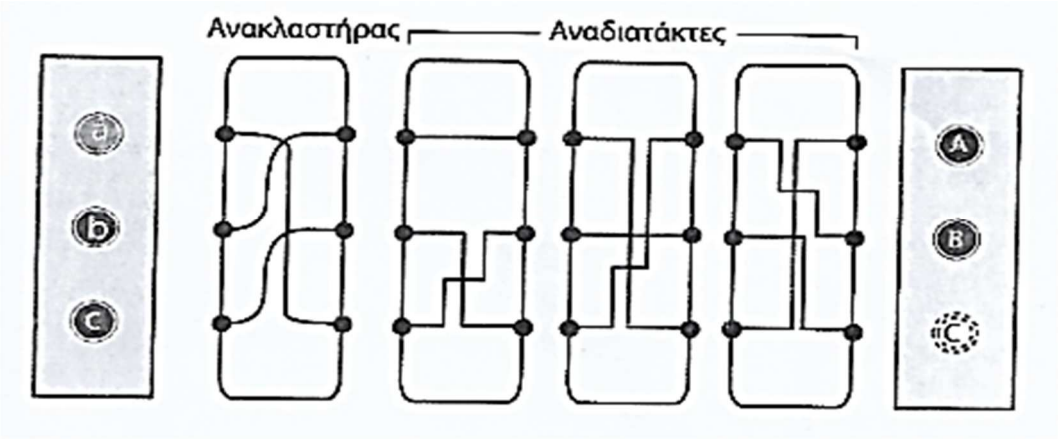
Το ακόλουθο σχήμα παρουσιάζει σχηματικά και με πολύ απλοποιημένο τρόπο το μηχανισμό κρυπτογράφησης των αναδιατακτών, με ένα αλφάβητο 3 μόνο γραμμάτων και με ένα μόνο αναδιατάκτη, δηλαδή με τρεις πιθανές θέσεις. Όταν ο αναδιατάκτης βρίσκεται στην αρχική του θέση, κάθε γράμμα του πρωτότυπου μηνύματος αντικαθίσταται από ένα άλλο διαφορετικό, εκτός από το Α, που μένει το ίδιο. Μετά την κρυπτογράφηση του πρώτου γράμματος, ο αναδιατάκτης μετατοπίζεται κατά το 1/3 της περιστροφής. Σε αυτή τη νέα θέση, τα γράμματα αντικαθίστανται από άλλα γράμματα, διαφορετικά από εκείνα της πρώτης κρυπτογράφησης. Η διαδικασία ολοκληρώνεται με το τρίτο γράμμα και, σε αυτό το σημείο, ο αναδιατάκτης επιστρέφει στην αρχική του θέση, και η ακολουθία κρυπτογράφησης επαναλαμβάνεται.



Οι αναδιατάκτες του Enigma είχαν 26 θέσεις, μία για κάθε γράμμα του αλφαβήτου. Έτσι, ένας αναδιατάκτης μπορούσε να ολοκληρώσει 26 διαφορετικά κρυπτογραφήματα. Η αρχική θέση του αναδιατάκτη είναι επομένως το κλειδί. Για να αυξηθεί ο αριθμός των πιθανών κλειδιών, το Enigma μπορούσε να έχει έως και τρεις αναδιατάκτες, μηχανικά συνδεδεμένους μεταξύ τους. Έτσι, όταν ο πρώτος αναδιατάκτης πραγματοποιούσε μια πλήρη περιστροφή, ο επόμενος ξεκινούσε μια άλλη, κ.ο.κ., ώσπου να ολοκληρωθούν οι πλήρεις περιστροφές των τριών αναδιατακτών, δηλαδή ένα σύνολο 26x26x26=17.576 πιθανά κρυπτογραφήματα.

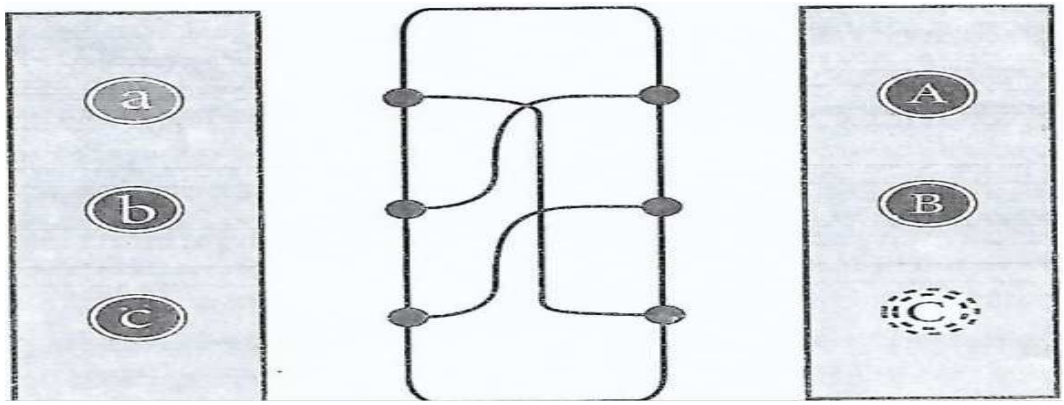
Επιπλέον, η σύλληψη του Scherbius επέτρεπε την αντιστροφή της σειράς των αναδιατακτών, κάτι που αύξανε ακόμη τον αριθμό κλειδιών, όπως θα δούμε παρακάτω. Εκτός από τρεις αναδιατάκτες, το Enigma διέθετε κι έναν πίνακα βυσμάτων, τοποθετημένο ανάμεσα στον πρώτο αναδιατάκτη και στο πληκτρολόγιο. Αυτός ο πίνακας βυσμάτων επέτρεπε την αντιστροφή των ζευγών γραμμάτων πριν από τη σύνδεση στον αναδιατάκτη, κάτι που αύξανε αξιοσημείωτα τον αριθμό των επιπρόσθετων κλειδιών της κρυπτογράφησης.

Η πρότυπη μηχανή Enigma διέθετε 6 κορδόνια βυσμάτων, με τα οποία μπορούσε κανείς να αντιστρέψει έως και 6 ζεύγη γραμμάτων. Το σχήμα δείχνει τη λειτουργία του πίνακα βυσμάτων, το οποίο και πάλι είναι απλοποιημένο, καθότι υπάρχουν μόνο τρία γράμματα και τρία βύσματα. Με αυτό τον τρόπο, το Α αντιστρεφόταν με το C, το Β με το Α και το C με το Β. Προσθέτοντας έναν ανακλαστήρα, μια απλοποιημένη μηχανή Enigma τριών γραμμάτων, θα ήταν ως εξής: Πόσα επιπλέον κλειδιά παρέχει ο ανακλαστήρας, με μια προφανώς ασήμαντη πρόσθεση; Για να απαντήσουμε, πρέπει να αναλογιστούμε τον αριθμό των τρόπων καλωδίωσης έξι ζευγών γραμμάτων από τα 26.



Γενικά, ο αριθμός πιθανών μετασχηματισμών n ζευγών ενός αλφαβήτου N χαρακτήρων υπολογίζεται με τη βοήθεια του τύπου: $\frac{N!}{(N-2n)!n!2^n}$. Στο παράδειγμα μας, N=26 και n=6, κάτι που μας δίνει τον ασύλληπτο αριθμό των 100.391.791.500 συνδυασμών. Κατά συνέπεια, ο συνολικός αριθμός πιθανών κλειδιών που προσφέρει η μηχανή Enigma τριών αναδιατακτών 26 γραμμάτων και ενός πίνακα βυσμάτων έξι σειρών είναι ο ακόλουθος: Όσον αφορά στις περιστροφές των αναδιατακτών, 26^3=26x 26x26=17.576 συνδυασμοί. Ομοίως, οι τρεις αναδιατάκτες (1,2,3) μπορούσαν να εναλλαχθούν μεταξύ τους και να πάρουν τις θέσεις 1–2–3, 1–3–2, 2–1–3, 3–1–2, 3–2–1, κάτι που μας δίνει σε αυτή την περίπτωση έξι επιπλέον πιθανούς συνδυασμούς σε σχέση με τη διάταξη των αναδιατακτών. Τέλος, υπολογίσαμε ότι οι έξι σειρές του αρχικού πίνακα των βυσμάτων πρόσθεταν από μόνες τους 100.391.791.500 επιπλέον κρυπτογράμματα.

Ο συνολικός αριθμός κλειδιών λαμβάνει πολλαπλασιάζοντας τους παραπάνω διαφορετικούς συνδυασμούς: 6·17.576·100.391.7915000=10.586.916.764.424.000. Συνεπώς, οι μηχανές Enigma μπορούσαν να κρυπτογραφήσουν ένα κείμενο χρησιμοποιώντας πάνω από δέκα χιλιάδες δισεκατομμύρια διαφορετικού συνδυασμούς. Το Ράιχ μπορούσε να είναι ήσυχο και βέβαιο ότι οι άκρως σημαντικές επικοινωνίες του θα ήταν απολύτως ασφαλείς. Μέγα λάθος!



22. Αποκρυπτογράφηση του κώδικα Enigma

Ένα οποιοδήποτε κλειδί του Enigma προσδιόριζε τη θέση του πίνακα βυσμάτων για καθεμία από τις έξι ανταλλαγές πιθανών γραμμάτων (πχ B/Z, F/Y, R/C, T/H, E/O και L/J, για να φανεί ότι η πρώτη ανταλλαγή ήταν μεταξύ των γραμμάτων B και Z, και ούτω καθεξής), τη διάταξη των αναδιατακτών (πχ 2–3–1) και τον προσανατολισμό εκκίνησης (πχ R,V,B για να οριστεί ποιο γράμμα ήταν πρώτο). Αυτές οι ενδείξεις ήταν καταγεγραμμένες σε

βιβλία κλειδιών, που με τη σειρά τους μεταδίδονταν με κωδικοποιημένο τρόπο και μπορούσαν να αλλάζουν καθημερινά ή δυνάμει άλλων περιστάσεων, όπως για παράδειγμα της φύσης του μηνύματος. Για να αποφεύγουν να επαναλαμβάνουν το ίδιο κλειδί όλη τη μέρα, κατά τη διάρκεια της οποίας μπορεί να στέλνονταν χιλιάδες μηνύματα, οι χειριστές της μηχανής Enigma κατέφευγαν σε μεγαλοφυή τεχνάσματα για τη μετάδοση νέων κλειδιών περιορισμένης χρήσης, χωρίς να πρέπει να αλλάξουν το βιβλίο των κοινών κλειδιών.

Έτσι, ο αποστολέας κωδικοποιούσε σύμφωνα με το σχετικό κλειδί της μέρας ένα μήνυμα έξι γραμμάτων, που υποδήλωνε στην ουσία μια νέα διάταξη των αναδιατακτών, για παράδειγμα T–Y–J (και για μεγαλύτερη ασφάλεια, κωδικοποιούσε δύο φορές αυτές τις τρεις ενδείξεις, εξ ου τα έξι γράμματα). Στη συνέχεια, κωδικοποιούσε το πραγματικό μήνυμα σύμφωνα με αυτή τη νέα διάταξη. Ο παραλήπτης λάμβανε ένα μήνυμα που δεν μπορούσε να αποκρυπτογραφήσει με το κλειδί της μέρας, αλλά ήξερε ότι οι έξι πρώτοι χαρακτήρες ήταν στην ουσία οι οδηγίες διάταξης των αναδιατακτών. Ο παραλήπτης έκανε αυτές τις αλλαγές χωρίς να τροποποιεί τον πίνακα των βυσμάτων ούτε τη σειρά των αναδιατακτών, κι έτσι μπορούσε να αποκρυπτογραφήσει το μήνυμα με το σωστό τρόπο. Οι Σύμμαχοι πήραν την πρώτη έγκυρη πληροφορία σχετικά με τη μηχανή Αίνιγμα από τα χέρια ενός Γερμανού κατασκόπου, του Hans-Thilo Schmidt, η οποία αποτελούνταν από πολλά εγχειρίδια πρακτικής εφαρμογής της μηχανής. Η επαφή με τον Schmidt έγινε από την πολωνική υπηρεσία πληροφοριών, που εκείνη την περίοδο ένιωθε πολύ έντονα την ανάσα μιας Γερμανίας ολοένα και πιο απειλητικής. Η πολωνική υπηρεσία κρυπτανάλυσης, γνωστή με το όνομα **Byuro Szyfrow**, βάλθηκε να δουλεύει τα έγγραφα του Schmidt και κατέληξε σε πολλά δείγματα της μηχανής Enigma, άγνωστα στους Γερμανούς.

Και, κάτι καινούργιο για την εποχή εκείνη, η υπηρεσία αποφάσισε να επανδρώσει την ομάδα των κρυπταναλυτών με έναν αξιόλογο αριθμό μαθηματικών. Μεταξύ τους υπήρχε ένας νέος ταλαντούχος άντρας, 23 ετών, εσωστρεφής και ντροπαλός, ονόματι **Marian Rejewski**. Αυτός ρίχτηκε αμέσως στη δουλειά και επικέντρωσε όλες του τις προσπάθειες συγκεκριμένα στο κλειδί του μηνύματος έξι γραμμάτων, που προηγούνταν πολλών μηνυμάτων που αντάλλασσαν καθημερινά οι Γερμανοί. Ο Rejewski ήξερε ότι τα τελευταία τρία κρυπτογράμματα του κλειδιού ήταν τα τρία πρώτα κρυπτογραφημένα εκ νέου και ήξερε λοιπόν ότι το τέταρτο, το πέμπτο και το έκτο μπορεί να αποτελούσαν τη βάση της περιστροφής των αναδιατακτών. Με αφετηρία αυτή τη διαπίστωση, όσο ασήμαντη και αν φαίνεται, ο Rejewski κατέληξε σε έναν εκπληκτικό αριθμό αποτελεσμάτων, τα οποία θα του επέτρεπαν τελικά να «σπάσει» τον κώδικα Enigma. Είναι γεγονός ότι, έπειτα από μερικούς μήνες, ο Rejewski είχε καταφέρει να μειώσει τον αριθμό πιθανών κλειδιών από δέκα χιλιάδες δισεκατομμύρια πιθανά αρχικά στα μόλις 105.456, που προκύπτανε από διαφορετικούς συνδυασμούς της σειράς των αναδιατακτών και των διάφορων περιστροφών τους. Έτσι, ο Rejewski κατασκεύασε ένα μηχάνημα λειτουργίας παρόμοιας με εκείνης του Enigma, ονόματι **Bomba**, ικανό να παράγει όλες τις πιθανές θέσεις των τριών αναδιατακτών, αναζητώντας το κλειδί της ημέρας. Ήδη το 19234, η υπηρεσία Byuro Szyfrow είχε καταφέρει να «σπάσει» το Enigma και ήταν ικανή να αποκρυπτογραφήσει οποιοδήποτε μήνυμα μέσα σε 24 ώρες.

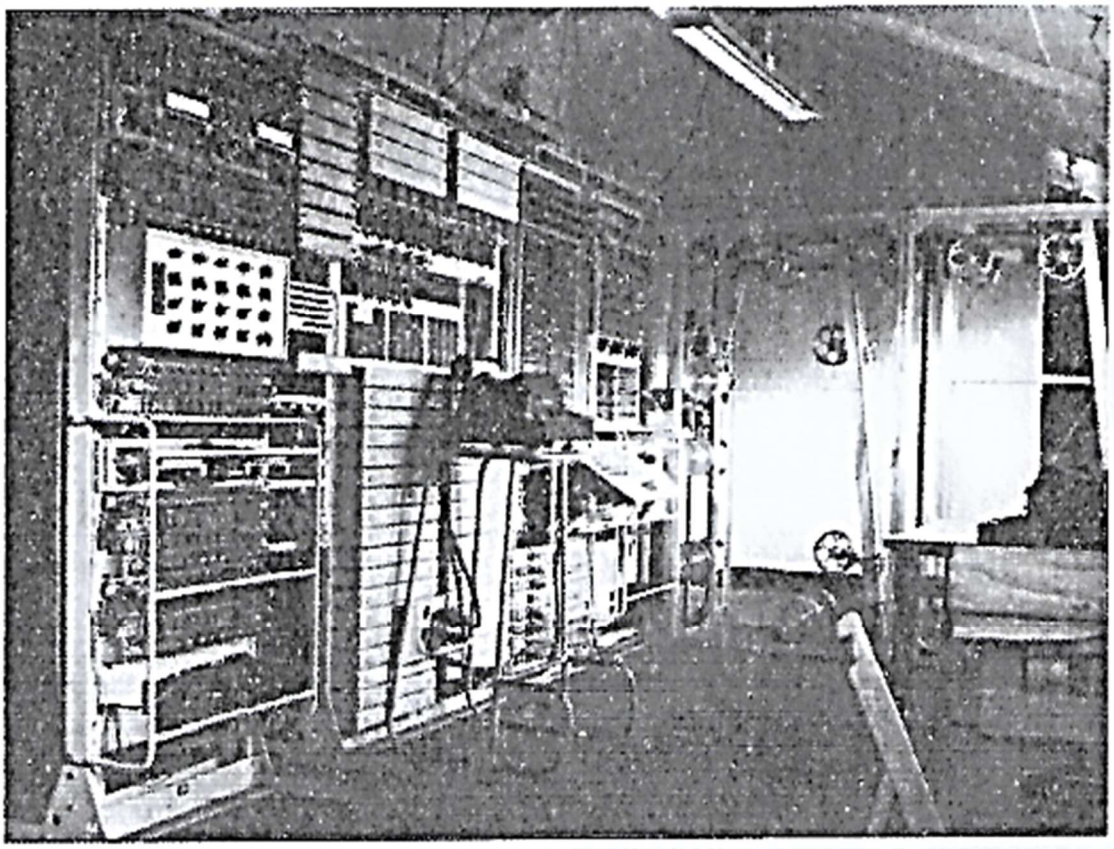
Οι Γερμανοί δεν ήξεραν ότι οι Πολωνοί είχαν παραβιάσει την ασφάλεια του Enigma, ωστόσο δεν σταμάτησαν να επιφέρουν βελτιώσεις σε ένα σύστημα που τελικά λειτουργούσε ήδη εδώ και δέκα χρόνια. Το 1938 οι χειριστές του Enigma προσπάθησαν δύο ακόμη αναδιατάκτες στους τρεις ήδη υπάρχοντες στην πρότυπη μηχανή, ενώ λίγο καιρό αργότερα δημιουργήθηκαν καινούργια μοντέλα της μηχανής με πίνακες βυσμάτων δέκα σειρών.

Έτσι, ο αριθμός των πιθανών κλειδιών αυξήθηκε αμέσως στα σχεδόν 159 τρισεκατομμύρια. Η προσθήκη και μόνο των δύο αναδιατακτών στην περιστροφή των τροποποιητών αύξησε τους πιθανούς συνδυασμούς από 6 σε 60: ένας οποιοσδήποτε από τους πέντε αναδιατάκτες στην πρώτη θέση (5 δυνατότητες) x, ένας από τους τρεις αναδιατάκτες

στην τρίτη θέση (τρεις δυνατότητες)=5x4x3=60. Ακόμη και αν ήξερε πώς να αποκρυπτογραφήσει τον κώδικα, η υπηρεσία Buyro Szyfrow δεν διέθετε τα απαραίτητα μέσα για να αναλύσει σειριακά έναν αριθμό σχηματισμών των αναδιατακτών 10 φορές μεγαλύτερο.

23. Οι Βρετανοί παίρνουν τη σκυτάλη

Η βελτίωση του Enigma δεν ήταν τυχαία. Η Γερμανία είχε αρχίσει ήδη την επιθετική της επέκταση στην Ευρώπη, προσαρτώντας την Τσεχοσλοβακία και την Αυστρία, ενώ σχεδίαζε να εισβάλει στην Πολωνία. Το 1939, ενώ ο πόλεμος διεξαγόταν στην καρδιά της Ευρώπης και στις ήδη κατακτημένες χώρες της, οι Πολωνοί εμπιστεύθηκαν τις μηχανές Enigma που είχαν φτιάξει στους Βρετανούς συμμάχους, οι οποίοι τον Αύγουστο του ίδιου έτους αποφάσισαν να ανασυγκροτήσουν τις διάσπαρτες ομάδες κρυπτανάλυσης που διέθεταν. Το μέρος που επέλεξαν ήταν ένα σπίτι στα προάστια του Λονδίνου, σε μια ιδιοκτησία ονόματι **Bletchley Park**. Ένας από τους πιο λαμπρούς κρυπταναλυτές που είχε επιστρατεύσει η κυβέρνηση για την ομάδα του Bletchley Park ήταν ο νεαρός μαθηματικός Alan Turing. Ο Turing ήταν μια παγκοσμίως αναγνωρισμένη αυθεντία της πληροφορικής, η οποία εκείνη την εποχή ήταν ένας ανεκμετάλλευτος κλάδος της επιστήμης, ανοιχτός σε νέες, ακόμη και επαναστατικές, εξελίξεις. Οι γνώσεις του υπήρξαν θεμελιώδης ως προς την αποκρυπτογράφηση της βελτιωμένης μηχανής Enigma.

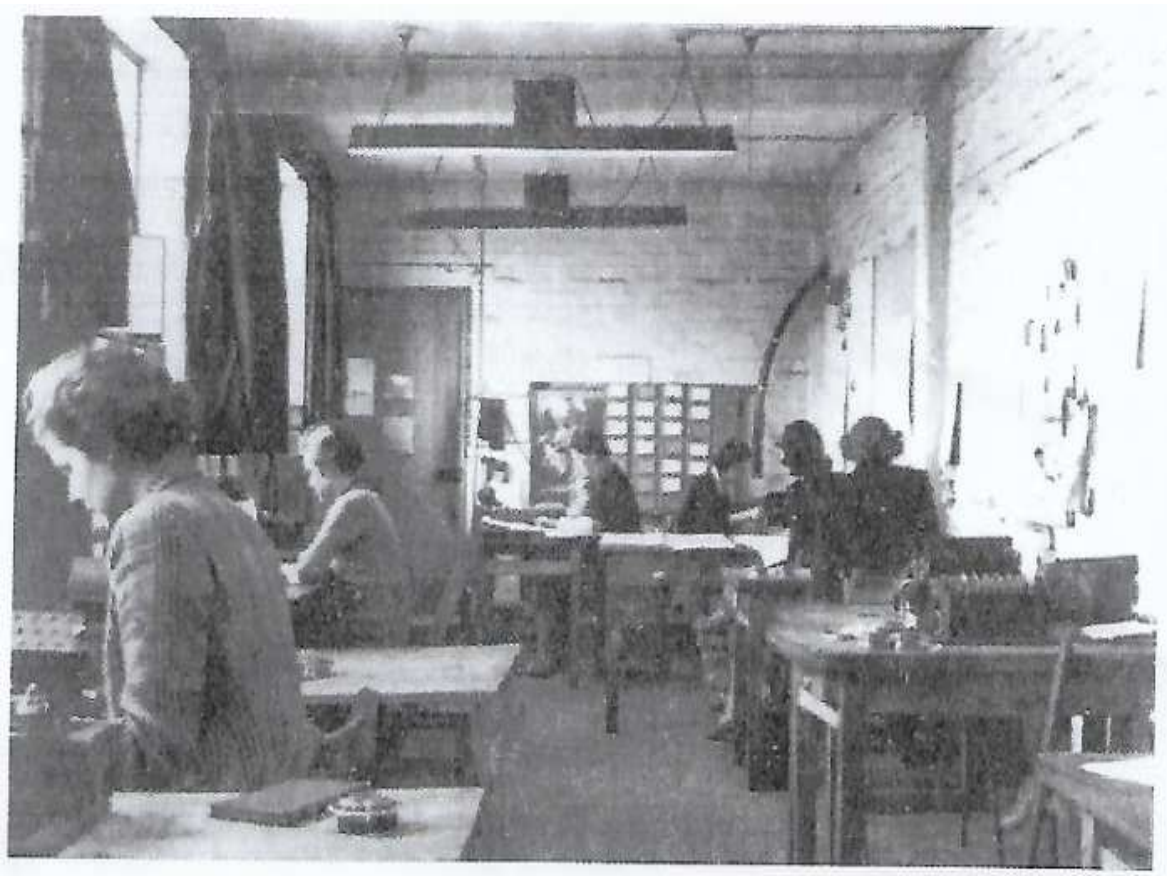


Ο Colossus, πρωτότυπο του σύγχρονου υπολογιστή, που κατασκευάστηκε στο Bletchley Park. Η φωτογραφία τραβήχτηκε το 1943 και δείχνει τον πίνακα ελέγχου αυτής της πολύπλοκης μηχανής.

Οι ειδικοί του Bletchley Park επικεντρώθηκαν σε σύντομα αποσπάσματα κρυπτογραφημένων κειμένων, των οποίων πίστευαν ότι γνώριζαν την καθαρή αντιστοιχία. Για παράδειγμα, χάρη στη δουλειά των κατασκόπων, ήξεραν ότι οι Γερμανοί είχαν τη συνήθεια να μεταδίδουν ένα κωδικοποιημένο μήνυμα σχετικά με τις μετεωρολογικές

συνθήκες διάφορων σημείων του μετώπου, και αυτό γινόταν κάθε μέρα γύρω στις 6 το απόγευμα. Κατά συνέπεια, ήταν λογικά σίγουροι ότι ένα υποκλεμμένο μήνυμα λίγα λεπτά μετά την ώρα αυτή περιείχε την κωδικοποιημένη εκδοχή λέξεων όπως «καιρός» ή «βροχή» στο καθαρό κείμενο. Ο Turing επινόησε μια ηλεκτρική συσκευή που επέτρεπε την αναπαραγωγή όλων των 1.054.650 πιθανών συνδυασμών σε σειρά και σε θέση των τριών αναδιατακτών. Αυτή η συσκευή λάμβανε τις κρυπτογραφημένες λέξεις που , από το μήκος ή άλλες ενδείξεις, θεωρούνταν ότι αντιπροσώπευαν τμήματα καθαρού κειμένου, όπως, για παράδειγμα, οι λέξεις «καιρός» ή «βροχή».

Έστω ότι το κρυπτογραφημένο κείμενο FGRTY είναι η κρυπτογραφημένη εκδοχή της λέξης «καιρός». Εισήγαν το κρυπτογράφημα στη μηχανή και αν υπήρχε ένας συνδυασμός αναδιατακτών που έδινε ως αποτέλεσμα τη λέξη «καιρός», οι κρυπταναλυτές ήξεραν ότι είχαν βρει, από όλα τα κλειδιά, εκείνο που αντιστοιχούσε στο σχηματισμό των αναδιατακτών. Στη συνέχεια, ο χειριστής εισήγε το κρυπτογραφημένο κείμενο στην πραγματική μηχανή Enigma, με τους αναδιατάκτες στη θέση που υποδείκνυε το κλειδί. Αν η μηχανή έδινε ένα αποκρυπτογραφημένο κείμενο TMPES, για παράδειγμα, ήταν προφανές ότι το μέρος του κλειδιού που είχε να κάνει με τη θέση των καλωδίων έδειχνε τη μετατόπιση των γραμμάτων Μ και Ε. Με αυτό τον τρόπο, είχαν βρει ολόκληρο το κλείδι. Έτσι, αποκαλύπτονταν πλήρως τα μυστικά της μηχανής Enigma. Κατά τη διαδικασία ανάπτυξης και βελτίωσης των αναλυτικών μηχανών που περιγράφουμε εδώ, η ομάδα του Bletchley Park κατέληξε να δημιουργήσει τον πρώτο πρωτότυπο υπολογιστή στην ιστορία, ο οποίος ονομάστηκε Colossus.



Εγκαταστάσεις του Bletchley Park, όπου εργάζονταν οι ειδικοί που αποκρυπτογράφησαν τον κώδικα Αίνιγμα.

24. Άλλοι κώδικες του Β΄ Παγκοσμίου Πολέμου

Η Ιαπωνία ανέπτυξε τα δικά της συστήματα κωδικοποίησης: ο λεγόμενος κώδικας «**Purple**» και ο JH-25. Ο πρώτος χρησιμοποιήθηκε για τις διπλωματικές επικοινωνίες και δεύτερος για τη μετάδοση μηνυμάτων στρατιωτικού χαρακτήρα. Και τα δύο κρυπτοσυστήματα λειτουργούσαν με τη βοήθεια μηχανικών συσκευών. Ο JN-25, για παράδειγμα, αποτελούνταν από έναν αλγόριθμο αντικατάστασης που μετέφραζε τα ιδεογράμματα της ιαπωνικής γλώσσας (30.000) σε μια ακολουθία αριθμών βάσει τυχαίων πινάκων πέντε στοιχείων. Παρά τις προφυλάξεις που έπαιρναν οι Ιάπωνες, οι Βρετανοί και οι Αμερικάνοι αποκρυπτογράφησαν τον κώδικα Purple και τον JN–25, τη στιγμή των ουσιαστικών αποφάσεων για τις κρίσιμες μάχες στον ειρηνικό ωκεανό και ιδιαίτερα για εκείνες στην Θάλασσα των Κοραλλιών και στο Μίντγουεϊ που πραγματοποιήθηκαν το 1942, καθώς και για τη λήψη απίστευτων μέτρων, όπως της δολοφονίας του ναυάρχου Γιαμαμότο, ένα χρόνο μετά. Το περιεχόμενο της υποκλοπής των κρυπτοσυστημάτων Purple και JN–25 ονομάστηκε **Magic**.

25. Ένας αυθεντικός «εξαιρετικός» άνθρωπος

Ο Alan Turing γεννήθηκε στην Αγγλία το 1912. Μαθητής ιδιαίτερων ικανοτήτων, έδειξε από πολύ μικρή ηλικία μεγάλη κλίση στα μαθηματικά και στη φυσική. Το 1931 μπήκε στο Cambridge, όπου ασχολήθηκε με τη δουλειά του επιστήμονα της λογικής Kurt Gödel πάνω στο γενικό πρόβλημα της εγγενούς μη πληρότητας κάθε λογικού συστήματος.

Τρία χρόνια πριν, είχε εκδώσει μια μελέτη σχετικά με την πιθανότητα κατασκευής μηχανών που θα ήταν ικανές να υπολογίσουν διάφορους αλγορίθμους, όπως το άθροισμα, ο πολλαπλασιασμός κλπ. Ωθούμενος από τη δουλειά του Gödel, προχώρησε ακόμη παραπέρα την ιδέα του και προσδιόρισε το 1937 τις αρχές μιας «παγκόσμιας μηχανής», ικανής να υπολογίζει κάθε είδους αλγόριθμο. Έτσι, τέθηκε ένα από τα θεμέλια του θεωρητικού οικοδομήματος της σύγχρονης πληροφορικής. Δύο χρόνια πριν από την επαναστατική του συνεισφορά, ο Turing ήρθε σε επαφή με το μεγάλο Ούγγρο μαθηματικό **John von Neumann,** που τότε βρισκόταν εξόριστος στις Ηνωμένες Πολιτείες.

Ο Von Neumann, που θεωρούνταν ο άλλος «πατέρας» της πληροφορικής, του πρόσφερε μια θέση στο Princeton, με πολύ καλή αμοιβή και εξαιρετικό κύρος. Ωστόσο, ο Turing προτίμησε την μποέμικη ατμόσφαιρα του Cambridge και απέρριψε την προσφορά. Το 1939 μπήκε στη βρετανική υπηρεσία κρυπτογραφικής ανάλυσης του Bletchley Park.

Παρότι παρασημοφορήθηκε από την τάξη της βρετανικής αυτοκρατορίας για τη συνεισφορά του την περίοδο του πολέμου, η ομοφυλοφιλία του είχε ως αποτέλεσμα την απόρριψή του από την ακαδημαϊκή κοινότητα. Θύμα βαθιάς κατάθλιψης, ο Alan Turing αυτοκτόνησε στις 08.06.1954, παίρνοντας κυανιούχο κάλιο. Ήταν τότε 42 ετών.

26. Οι κωδικοποιητές Ναβάχο

Ένα από τα πιο εκπληκτικά μέσα αποκωδικοποίησης της πληροφορίας από τον εχθρό, κατά τη διάρκεια πολέμου, υπήρξε αυτό που χρησιμοποιήθηκε από τους Αμερικάνους στις επιχειρήσεις τους στον Ειρηνικό ωκεανό. Οι αξιωματικοί των υπηρεσιών πληροφοριών των ΗΠΑ επέλεξαν σε αυτή την περίπτωση διάφορους κώδικες με την αυστηρή έννοια της λέξης, δηλαδή αλγόριθμους κρυπτογράφησης που επηρέαζαν έμμεσα τη φύση των λέξεων. Αυτοί οι κώδικες, ο Τσοκτάου, ο Κομάντσι, ο Μεσκουάκι και κυρίως ο Ναβάχο, ούτε εξηγούνταν σε πολύπλοκα εγχειρίδια ούτε ήταν αποτέλεσμα προσεκτικού σχεδιασμού μιας υπηρεσίας κρυπτογράφων, είχε να κάνει με αληθινές ινδοαμερικανικές γλώσσες.

Ο στρατός των ΗΠΑ τοποθέτησε ασυρματιστές από αυτές τις εθνικότητες σε διάφορες μονάδες κατανεμημένες στο μέτωπο και τους ανέθεσε τη μετάδοση των μηνυμάτων στις αντίστοιχες γλώσσες τους, άγνωστες όχι μόνο στους Ιάπωνες, αλλά και στους υπόλοιπους συμπατριώτες. Σε αυτά τα κωδικοποιημένα με αυτό τον τρόπο μηνύματα προστέθηκε ένα βιβλίο βασικής κωδικοποίησης, ώστε ένας αιχμάλωτος στρατιώτης να μην μπορούσε να τα μεταφράσει. Αυτοί οι code talkers (κωδικο-ομιλητές), οι ραδιοκωδικοποιητές, υπηρέτησαν σε διάφορες μονάδες, έως και στον πόλεμο της Κορέας.

Δύο κωδικο-ομιλητές Ναβάχο στη μάχη του Bougainville το 1943.

27. Οι δρόμοι της καινοτομίας, το κρυπτογράφημα Hill

Τα κρυπτογραφήματα που παρουσιάστηκαν έως τώρα, όπου ένας χαρακτήρας αντικαθίσταται από έναν άλλο με προκαθορισμένο τρόπο, είναι, όπως είδαμε, επιρρεπή στην κρυπτανάλυση. Το 1929 ο Βορειοαμερικάνος μαθηματικός Lester S. Hill επινόησε, πατεντάρισε και κυκλοφόρησε στην αγορά, με αποτυχία, ένα νέο σύστημα κρυπτογράφησης, που συνδύαζε την αριθμητική των υπολοίπων με τη γραμμική άλγεβρα. Ένας μαθηματικός πίνακας μπορεί να αποτελέσει ένα πολύ χρήσιμο εργαλείο για την κρυπτογράφηση ενός μηνύματος, αποσυνθέτοντας το κείμενο ανά ζεύγη γραμμάτων και συσχετίζοντας κάθε γράμμα με μια αριθμητική τιμή του αλφάβητου. Για την κρυπτογράφηση ενός μηνύματος, χρησιμοποιούμε έναν πίνακα $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Με την προϋπόθεση η ορίζουσά του να είναι ίση με 1, δηλαδή ad-bc=1. Για την αποκρυπτογράφηση, θα χρησιμοποιήσουμε τον αντίστροφο πίνακα $A^{-1}=\begin{pmatrix} a & -b \\ -c & d \end{pmatrix}$. Η προϋπόθεση που τίθεται στην ορίζουσα του πίνακα οφείλεται στο

γεγονός ότι, για να εξασφαλιστεί η αποκρυπτογράφηση, πρέπει να διαθέτει κανείς τον αντίστροφο πίνακα. Κατά γενικό κανόνα, για ένα αλφάβητο από η χαρακτήρες πρέπει ο μέγιστος κοινός διαιρέτης ΜΚΔ (ορίζουσα του Α, n) να ισούται με 1. Διαφορετικά, δεν μπορούμε να είμαστε σίγουροι για την ύπαρξη αντίστροφου στην αριθμητική των υπολοίπων.

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	@
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Ας πάρουμε ένα παράδειγμα: Έστω ένα αλφάβητο 26 γραμμάτων που περιέχει έναν χαρακτήρα «κενό», τον οποίο θα ονομάσουμε σε αυτό το παράδειγμα @. Αποδίδουμε σε κάθε γράμμα μια αριθμητική τιμή, όπως φαίνεται στον πίνακα. Για να πάρουμε τιμές ανάμεσα στο 0 και στο 26, θα δουλέψουμε modulo 27. Η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης θα είναι η εξής: πρώτα απ'όλα ας ορίσουμε ένα μαθηματικό πίνακα κρυπτογράφησης Α με ορίζουσα 1. Για παράδειγμα: $A=\begin{pmatrix}1 & 3\\ 2 & 7\end{pmatrix}$. Ο πίνακας αποκρυπτογράφησης θα είναι ο πίνακας $A^{-1}=\begin{pmatrix}7 & -3\\ -2 & 1\end{pmatrix}$. Άρα, το Α θα είναι το κλειδί κρυπτογράφησης και το A^{-1} εκείνο της αποκρυπτογράφησης;. στη συνέχεια, ας πάρουμε για παράδειγμα το μήνυμα «OUI» («NAI»). Ομαδοποιούμε τους χαρακτήρες του μηνύματος ανά ζεύγη: OUI@. Οι αριθμητικές αντιστοιχίες τους είναι, σύμφωνα με τον πίνακα, τα ζεύγη των κρυπτογραμμάτων (14,20) και (8,26). Έπειτα πολλαπλασιάζουμε τον πίνακα Αμε κάθε ζεύγος κρυπτογραμμάτων. Και αυτό μας δίνει το κρυπτογραφημένο:«OU» $=\begin{pmatrix}1 & 3\\ 2 & 7\end{pmatrix}\begin{pmatrix}14\\ 20\end{pmatrix}$ $=\begin{pmatrix}74\\ 168\end{pmatrix}=\begin{pmatrix}20\\ 6\end{pmatrix}$ (mod. 27), που αντιστοιχεί σύμφωνα με τον πίνακα αντιστοιχιών στους χαρακτήρες (U, G). Το δεύτερο ζεύγος δίνει κρυπτογραφημένο:
«I @» $=\begin{pmatrix}1 & 3\\ 2 & 7\end{pmatrix}\begin{pmatrix}8\\ 26\end{pmatrix}=\begin{pmatrix}80\\ 198\end{pmatrix}=\begin{pmatrix}5\\ 9\end{pmatrix}$ (mod, 27) που αντιστοιχεί στους χαρακτήρες (F, J)

Το μήνυμα «OUI» κρυπτογραφείται λοιπόν ως «UGFJ». Για να αποκρυπτογραφήσουμε, κάνουμε ην αντίστροφη πράξη χρησιμοποιώντας τον πίνακα $A^{-1}=\begin{pmatrix}7 & -3\\ -2 & 1\end{pmatrix}$

Παίρνουμε το ζεύγος χαρακτήρων (U, G) και ψάχνουμε το αριθμητικό του ισοδύναμο, (20,6). Έπειτα πολλαπλασιάζουμε με το A^{-1} και παίρνουμε $\begin{pmatrix}7 & -3\\ -2 & 1\end{pmatrix}\begin{pmatrix}20\\ 6\end{pmatrix}=\begin{pmatrix}122\\ -34\end{pmatrix}\equiv \begin{pmatrix}14\\ 20\end{pmatrix}$ (mod, 27), ισοδύναμο του (I, @). Το αποκρυπτογραφημένο μήνυμα είναι σωστό.

Για αυτό το παράδειγμα χρησιμοποιήσαμε ζεύγη χαρακτήρων. Η ασφάλεια θα ήταν καλύτερη, αν ομαδοποιούσαμε τους χαρακτήρες ανα τρεις ή και ανά τέσσερις. Σε αυτή την περίπτωση, οι υπολογισμοί θα γίνονταν με τους πίνακες 3x 3 και 4x4 αντίστοιχα, κάτι που θα ήταν δύσκολο να γίνει στο χέρι. Με τους σημερινούς υπολογιστές, όμως, είναι δυνατόν να εργαστούμε με πολύ μεγάλους πίνακες και με τα αντίστροφά τους. Το κρυπτογράφημα Hill πάσχει από μια σημαντική αδυναμία: Αν ο παραλήπτης διαθέτει έστω ένα μικρό τμήμα του κανονικού κειμένου, μπορεί να αποκρυπτογραφήσει το μήνυμα στο σύνολο του. Η έρευνα του τέλειου κρυπτογραφήματος απείχε ακόμη πολύ από την ολοκλήρωσή της.

27.1 Μία ιδέα από γραμμική άλγεβρα

Ένας πίνακας μπορεί να θεωρηθεί ως ένας πίνακας διατεταγμένος σε γραμμές και στήλες. Για παράδειγμα, ένας πίνακας 2x2 έχει την εξής μορφή $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ Και ένας πίνακας 1x2 (που λέγεται και διάνυσμα) έχει την εξής μορφή $\begin{pmatrix}x\\ y\end{pmatrix}$. Από τον πολλαπλασιασμό των δύο πινάκων παίρνουμε ένα νέο πίνακα 1x2, που ονομάζεται διάνυσμα στήλης:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + & by \\ cx + & dy \end{pmatrix}$$

Στην περίπτωση του πίνακα 2x2, η τιμή του ad-bc ονομάζεται ορίζουσα του πίνακα.

28. Διάλογος με τα μηδέν και τα ένα

Η αποκρυπτογράφηση του κρυπτοσυστήματος Enigma και η εφεύρεση του Colossus ήταν η απαρχή της πιο μεγάλης επανάστασης που γνώρισε η ανθρωπότητα: της σύγχρονης πληροφορικής. Αυτό το γιγαντιαίο βήμα πραγματοποιήθηκε κατά μεγάλο μέρος με αφορμή την ανάπτυξη ενός συστήματος κωδικοποίησης που επέτρεψε τη μετάδοση εύκολων και γρήγορων επικοινωνιών σε ένα ευρύ δίκτυο κατασκευασμένο γύρω από δύο βασικούς φορείς, τους υπολογιστές και τους χρήστες, δηλαδή όλους εμάς. Στη βάση αυτής της τεχνολογικής επανάστασης βρίσκεται το δυαδικό σύστημα. Αυτός ο εκπληκτικά απλός κώδικας που αποτελείται από δύο χαρακτήρες, το 0 και το 1, είναι ο πλέον χρησιμοποιούμενος στην πληροφορική, λόγω της ικανότητάς του να εκφράζει λογικές πράξεις που αλληλοεπιδρούν μέσα στα ηλεκτρονικά κυκλώματα των υπολογιστών και άλλων συσκευών. Κάθε 0 και 1 ονομάζεται bit (όρος προερχόμενος από το αγγλικό binary digit ή «δυαδικό ψηφίο»). Ένας καλός παραλληλισμός θα ήταν να πούμε ότι το δυαδικό σύστημα είναι η ιδιωματική γλώσσα των υπολογιστών.

29. Ο κώδικας ASCII

Μία από τις πολυάριθμες εφαρμογές του δυαδικού συστήματος είναι μια ξεχωριστή οικογένεια χαρακτήρων που επινοήθηκε με τέτοιο τρόπο ώστε κάθε χαρακτήρας να αποτελείται από 8 bits (1byte). Αυτοί οι χαρακτήρες, οι οποίοι αποκαλούνται αλφαριθμητικοί, είναι το σύνολο βασικών σημάτων που χρησιμοποιούνται στη συμβατική επικοινωνία, και ονομάζεται ASCII.

Μνήμη σε BYTES
Η μνήμη ή η χωρητικότητα αποθήκευσης ενός υπολογιστή και γενικότερα κάθε μηχανής υπολογίζεται σε bytes. Kilobyte (KB): 1.024 bytes, Mégabyte (MB): 1.048.576 bytes