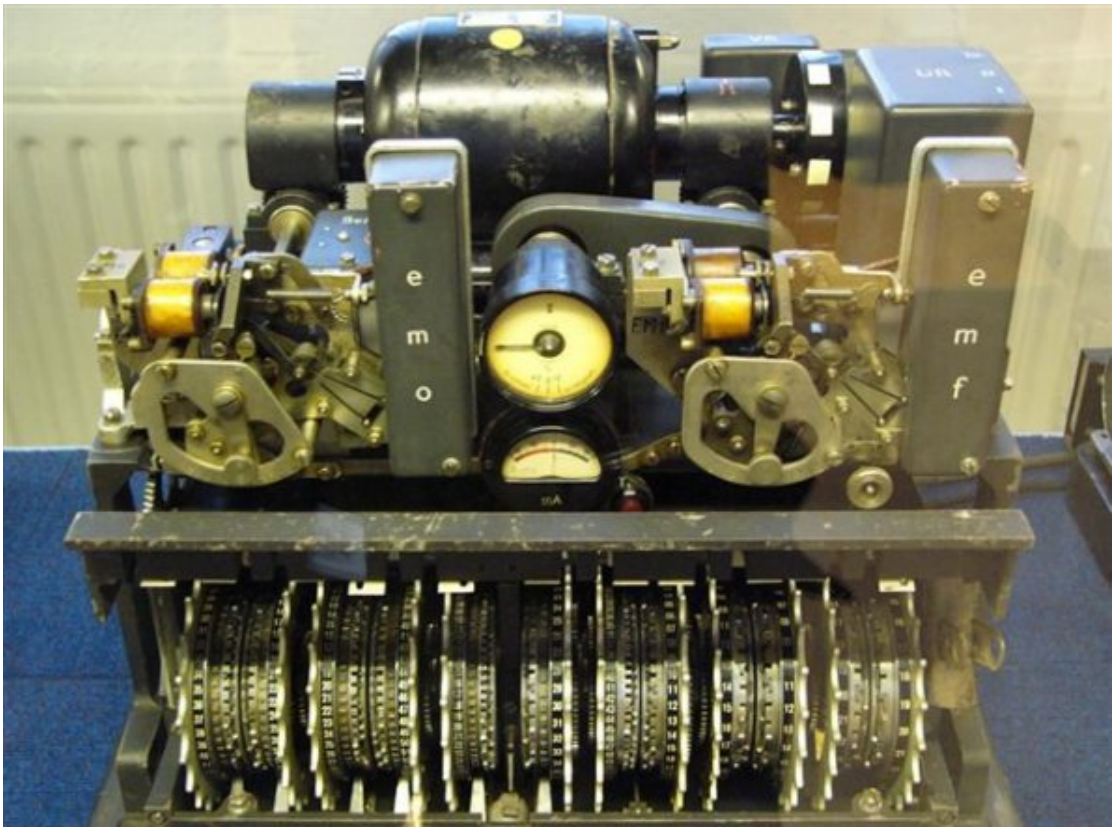
ΚΡΥΠΤΟΓΡΑΦΙΑ



ΜΑΘΗΤΕΣ:

ΔΕΣΠΟΙΝΑ ΛΕΒΕΝΤΕΛΗ

ΜΑΡΙΑ ΠΑΠΑΔΟΠΟΥΛΟΥ

ΕΛΕΝΗ ΜΑΝΟΥΣΟΥ

ΕΛΕΥΘΕΡΙΑ ΚΟΝΤΟΓΕΩΡΓΑΚΟΥ

ΓΕΩΡΓΙΟΣ ΔΙΟΝΥΣΑΤΟΣ

ΔΗΜΗΤΡΗΣ ΔΑΜΙΓΟΣ

ΑΓΓΕΛΟΣ ΑΝΑΣΤΑΣΗΣ

ΜΕΡΑΝ ΑΛΤΑΦ

ΦΩΤΗΣ ΝΤΙΜΕΡΗΣ

ΑΛΕΞΑΝΔΡΟΣ ΓΚΟΒΙΛΑΣ

ΚΩΣΤΑΣ ΓΕΩΡΓΙΟΥ

ΝΙΚΟΣ ΚΑΡΑΤΖΑΚΗΣ

ΧΡΗΣΤΟΣ ΔΙΑΚΟΓΙΑΝΝΗΣ

ΙΑΣΟΝΑΣ ΑΒΡΑΜΟΠΟΥΛΟΣ

ΑΓΓΕΛΟΣ ΧΑΤΣΗΣ

ΥΠΕΥΘΗΝΟΙ ΚΑΘΗΓΗΤΕΣ:

Τσατσουλή Αιμιλία Γροντάς Παναγιώτης

Περιεχόμενα

ΠΡΟΛΟΓΟΣ

Η κρυπτογραφία εμπλέκεται με τα αρχαία ευρήματα που έχουν ανακαλυφθεί από τον αρχαίο πολιτισμό και συνδέονται μέχρι το σύγχρονο κόσμο.

Επομένως στον αρχαίο πολιτισμό παρουσιάζονται μερικά επιτεύγματα όπως η Γραμμική Β η οποία είναι η πρώτη γραφή της ελληνικής γλώσσας και χρησιμοποιήθηκε στην Μυκηναϊκή περίοδο από το 17^{ο} έως τον 13^{ο} αιώνα Π.Χ για την τήρηση λογιστικών αρχείων στα ανάκτορα.

Στη συνέχεια εμφανίζεται ο Δίσκος της Φαιστού που αποτέλεσε ένα αρχαιολογικό εύρημα την Μινωική Πόλη και όσα αναφέρονται παραμένουν άγνωστα.

Η ανακάλυψη των ιερογλυφικών χρησιμοποιήθηκε στην γραφή της Αρχαίας Αιγύπτου. Η γραφή αυτή αποκρυπτογραφήθηκε το 1822 από τον Γάλλο αρχαιολόγο Σαμπολιόν.

Ένα ακόμα επίτευγμα είναι η στήλη της Ροζέτας είναι μια πέτρινη πλάκα που ήταν επιγραφημένη σε δυο γλώσσες [αιγυπτιακά+ ελληνικά].

Τέλος, η Συμβολή των Αράβων έπαιξε καθοριστικό ρόλο στην αποκρυπτογράφηση του Καίσαρα

Η ΓΡΑΜΜΙΚΗ Β

Από την ανακάλυψη των πινακίδων ο αρχιτέκτονας Μάικλ Βέντρις και ο φίλος Τζων Τσάντγουκ αποκρυπτογράφησαν 65 από τα 88 τότε βασικούς κανόνες ορθογραφίας και έφεραν στο φώς μια αρχαϊκή ελληνική διάλεκτο πέντε αιώνες παλαιότερα από του ελληνικού ομήρου.

Η Γραμμική Β΄ περιλαμβάνει 89 συλλαβογράμματα και 260 ιδεογράμματα που αναπαριστούν συλλαβές που αποδίδουν έννοιες όπως άνδρα-γυναίκα-λάδι-κρασί κλπ. Και σύμβολα για αριθμούς .

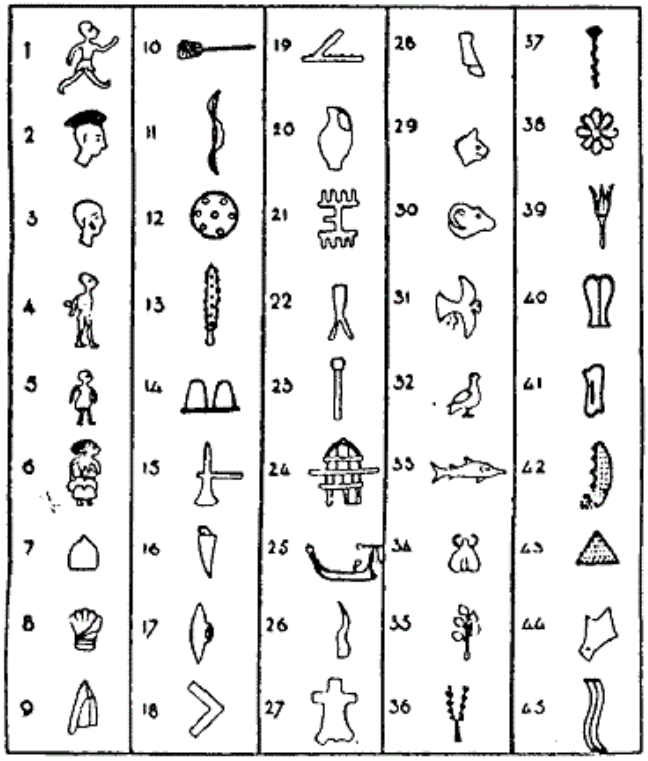
Η αξία τους για την θρησκεία το εμπόριο την οικονομία είναι τεράστια Σήμερα έχει αποκρυπτογραφηθεί το 87%των κειμένων.

ΔΙΣΚΟΣ ΤΗΣ ΦΑΙΣΤΟΥ

Ο δίσκος της Φαιστού είναι ένα αρχαιολογικό εύρημα από την Μινωική πόλη της Φαιστού στην νότια Κρήτη και χρονολογείται πιθανώς στον 17^{ο} αιώνα πχ. Αποτελεί ένα από τα γνωστότερα μυστήρια της αρχαιολογίας, αφού ο σκοπός της κατασκευής του και το νόημα των όσων αναγράφονται σε αυτό παραμένουν άγνωστα.

Ο δίσκος της Φαιστού ανακαλύφθηκε στης 3 Ιουνίου 1908 από τον Ιταλό αρχαιολόγο Λουϊτζι Περνιέ και φυλάσσεται σήμερα στο Αρχαιολογικό Μουσείο Ηρακλείου.

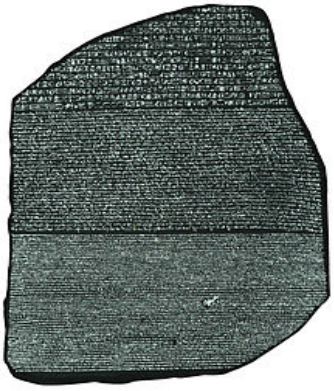
Πολλά από τα οποία αναπαριστούν εύκολα αναγνωρίσιμα αντικείμενα όπως ανθρώπινες μορφές, ψάρια, πουλιά, έντομα, φυτά κτλ. Συνολικά υπάρχουν 241 σύμβολα, 122 στην 1^{η} πλευρά και 119 στην 2^{η},τοποθετημένα σπειροειδές



ΙΕΡΟΓΛΥΦΙΚΑ-ΣΤΗΛΗ ΤΗΣ ΡΟΖΕΤΑΣ

Τα ιερογλυφικά είναι αρχαία εικονιστικά στοιχεία που χρησιμοποιούνται στην αρχαία Αιγυπτιακή γραφή. Η λέξη προέρχεται από τα αρχαία ελληνικά <<ιερές γλυφές >>δηλαδή ιερά ανάγλυφα επειδή χρησιμοποιήθηκαν σε ιερά θρησκευτικά κείμενα. Η γραφή αυτή αποκρυπτογραφήθηκε από τον Ζαν-Φρανσουά Σαμπολιόν το 1822, ο οποίος χρησιμοποίησε την Στήλη της ροζέτας

Η Στήλη της ροζέτας είναι μια πέτρινη πλάκα από γρανοδιορίτη που συχνά αναφέρεται λανθασμένα γρανίτης που προέρχεται από τον ναό του Πτολεμαίου Ε΄ του επιφανούς. Χρονολογείται στο 2^{ο} αιώνα πχ. και φέρει εγχάρακτη μια επιγραφή σε δύο γλώσσες [αιγυπτιακά+ ελληνικά] και 3 συστήματα γραφής [ιερογλυφικά, δημώδη αιγυπτιακή, ελληνική].

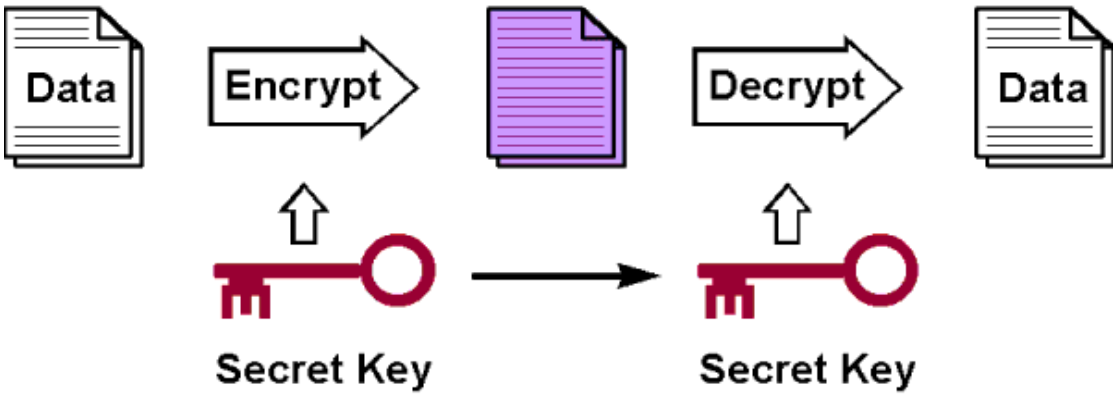


ΣΤΗΛΗ ΤΗΣ ΡΟΖΕΤΑΣ

ΙΕΡΟΓΛΥΦΙΚΑ

ΜΥΣΤΙΚΟ ΚΛΕΙΔΙ +ΚΑΙΣΑΡΑΣ

Το κλειδί καθορίζει το ακριβές κρυπτογραφικό αλφάβητο που πρέπει να χρησιμοποιηθεί για μια συγκεκριμένη κρυπτογράφηση. Ένας εχθρός που μελετά ένα υποκλαπέν κρυπτογραφημένο μήνυμα να έχει ισχυρή υποψία για τον αλγόριθμο, αλλά δεν γνωρίζει το ακριβές κλειδί. Αν το κρυπτογραφικό αλφάβητο, το κλειδί, έχει τηρηθεί απόλυτα μυστικό ανάμεσα στον αποστολέα και τον παραλήπτη, τότε ο εχθρός δεν μπορεί να αποκρυπτογραφήσει το υποκλαπέν μήνυμα.



Ο Καίσαρ χρησιμοποιούσε τη μυστική γραφή τόσο συχνά, ώστε ο Βαλέριος Πρόβος έγραψε μια ολόκληρη πραγματεία για τα κρυπτογράμματα του ,ενός από τους τύπους κρυπτογραφικής υποκατάστασης που χρησιμοποιούσε ο Ιούλιος Καίσαρ: απλώς αντικαθιστούσε κάθε γράμμα του μηνύματος με το κατά τρεις θέσεις επόμενο του στο αλφάβητο.

ΤΟ ΚΡΥΠΤΟΓΡΑΜΜΑ ΠΛΕΪΦΕΑΡ

Στις αρχές του 1854, ο Σκοτσέζος επιστήμονας και πολιτικός Λάιον Πλέιφεαρ περιέγραψε στους καλεσμένους ενός δείπνου του προέδρου της κυβέρνησης έναν νέο τύπο κρυπτογράμματος, που είχε σχεδιάσει ο φίλος του Τσαρλς Γουίτστοουν, ως το πλέον ασφαλές μέσον τηλεγραφικής επικοινωνίας. Το κρυπτόγραμμα ήταν το πρώτο που χρησιμοποιούσε την τεχνική δίγραφου, στην οποία τα γράμματα υποκαθίστανται δύο δύο και όχι ανεξάρτητα.

Για τη χρήση του κρυπτογράμματος, επιλέγεται μία λέξη κλειδί γνωστή τόσο στον αποστολέα όσο και στον παραλήπτη π.χ., η λέξη ΠΟΤΑΜΙ. Σε ένα παραλληλόγραμμο 4Χ6, γράφεται το κλειδί (παραλείποντας επαναλήψεις γραμμάτων), ακολουθούμενο από τα υπόλοιπα γράμματα του αλφάβητου στη σειρά

Π Ο Τ Α

Μ Ι Β Γ

Δ Ε Ζ Η

Θ Κ Λ Ν

Ξ Ρ Σ Υ

Φ Χ Ψ Ω

Για να κρυπτογραφηθεί το μήνυμα, το κείμενο χωρίζεται σε ζεύγη. Τα διπλά γράμματα χωρίζονται με ένα χ, και ένα χ προστίθεται για να κάνει το μονό τελευταίο γράμμα δίγραφο. Π.χ., η λέξη *κομμάτια* θα γίνει *κο μχ μα τι αχ*. Μόλις τα γράμματα χωριστούν σε ζεύγη, σε κάθε δίγραφο τα δύο γράμματα βρίσκονται στην ίδια σειρά, ή στην ίδια στήλη, ή σε τίποτε από τα δύο.

Κάθε σειρά θεωρείται κυκλική, έτσι, για παράδειγμα, το γράμμα << δεξιά >> από το Γ είναι το Μ. Γράμματα που εμφανίζονται στην ίδια στήλη αντικαθίστανται με το αμέσως από κάτω γράμμα με την ίδια μέθοδο.

Στην περίπτωση γραμμάτων του κανονικού κειμένου μου δεν εμφανίζονται ούτε στην ίδια στήλη, το καθένα αντικαθίσταται από το γράμμα που βρίσκεται στη δική του σειρά και τη στήλη του άλλου. Έτσι, το << ον >> θα γινόταν ΑΚ.

Για να αποκρυπτογραφηθούν κώδικες με δίγραφα, όπως του Πλεϊφεαρ, μια τακτική είναι η αναζήτηση των πιο κοινών δίγραφων στο κρυπτογράφημα και η παραδοχή ότι αυτά αντιπροσωπεύουν τα πιο συχνά δίγραφα στη γλώσσα που θεωρείται ότι είναι γραμμένο το κανονικό κείμενο. Στα ελληνικά μερικά πλέον συνηθισμένα είναι τα:

<< το >>, << τα >>, << τη >>, << μη >>, << με >>, << να >>, << αν >>, << θα >>.

Ένα άλλο τέχνασμα είναι η αναζήτηση ανεστραμμένων διγράφων στο κρυπτογράφημα, όπως ΑΝ και ΝΑ. Σε κείμενα κρυπτογραφημένα κατά Πλέιφεαρ, αυτά θα αποκρυπτογραφούνται πάντα με τον ίδιο τύπο γραμμάτων στο κανονικό κείμενο.

Ο αναλυτής μπορεί να αναζητήσει κοντινά ανεστραμμένα δίγραφα στο κρυπτογράφημα, και ταιριάζοντας τον τύπο σε γνωστές λέξεις αρχικού κειμένου που τον περιέχουν, να αρχίσει την ανασύνθεση του κλειδιού.

ΣΠΑΡΤΙΑΤΙΚΗ ΣΚΥΤΑΛΗ

Για χιλιάδες χρόνια, βασιλείς, ηγεμόνες και στρατηγοί στηρίζονταν στην αποτελεσματική μετάδοση μηνυμάτων, προκειμένου να κυβερνούν χώρες και στρατούς και ταυτόχρονα να προφυλάσσουν μυστικά υψίστης σημασίας για την προστασία των συνόρων τους .Η τέχνη της κρυπτογράφησης χρησιμοποιήθηκε ιδιαίτερα για πολεμικούς σκοπούς .Ο όρος σκυτάλη , μέθοδος των Σπαρτιατών, είναι ευφυής και διάσημος αλλά και παρεξηγημένος .Γύρω από ξύλινο κύλινδρο (σκυτάλη) τυλίγεται ταινία περγαμηνής ή υφάσματος ή δέρματος . Κατά μήκος της περιέλιξης καταγράφονταν σειρές μηνύματος .Όταν ξετυλίγονταν η ταινία , τα γράμματα βρίσκονταν σε αταξία ,η οποία δεν επέτρεπε να αποκωδικοποιηθεί το μήνυμα .Ο παραλήπτης έπρεπε να τυλίξει την ταινία σε κύλινδρο (σκυτάλη) ίδιου μήκους και διαμέτρου ,με τον τρόπο που είχε προ-συμφωνηθεί με τον αποστολέα , προκειμένου να αποκαλύψει το μήνυμα . Τα μηνύματα που μεταφέρονταν με την μέθοδο αυτή , θα πρέπει να ήταν σύντομα, δηλαδή <<λακωνικά>> .

ΤΟ ΤΕΤΡΑΓΩΝΟ ΤΟΥ ΠΟΛΥΒΙΟΥ

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

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

Το αυθεντικό Τετράγωνο του Πολυβίου βασίστηκε στην ελληνική αλφάβητο (για αυτό το λόγο δεν είναι συμπληρωμένο και το κελί 55), ωστόσο η ίδια μεθοδολογία μπορεί να εφαρμοσθεί με την ίδια επιτυχία για κάθε αλφάβητο (σχεδόν). Έτσι οι Ιάπωνες από το 1500 έως το 1910 έκαναν χρήση του Τετραγώνου του Πολυβίου, τροποποιημένο ώστε να καλύπτει τα 48 γράμματα της Ιαπωνικής (πίνακας 7Χ7). Αντίστοιχα το μέγεθος του πίνακα μπορεί να τροποποιηθεί σε 6 επί 6 δίνοντας τη δυνατότητα να κωδικοποιηθεί η Κυριλλική αλφάβητος (που περιλαμβάνει από 33 ως 37 γράμματα).

Η εφαρμογή του Τετραγώνου του Πολυβίου στην Αγγλική αλφάβητο, τυπικά έχει ως έξης:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

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

Κρυπτογράφηση Δημόσιου Κλειδιού

Η κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman και παρέχει έναν εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται ιδιωτικό κλειδί (private key) και το άλλο δημόσιο κλειδί (public key). Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να το ανακοινώνει σε όλη την διαδικτυακή κοινότητα ή σε συγκεκριμένους παραλήπτες. Υπάρχουν δε και ειδικοί εξυπηρετητές δημοσίων κλειδιών (public key servers) στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό.

Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού

κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.

Δημιουργία κλειδιών

Η δημιουργία του δημόσιου και του ιδιωτικού κλειδιού γίνεται από ειδικές συναρτήσεις οι οποίες δέχονται ως είσοδο έναν μεγάλο τυχαίο αριθμό και στην έξοδο παράγουν το ζεύγος των κλειδιών. Είναι προφανές ότι όσο πιο τυχαίος είναι ο αριθμός που παρέχεται ως είσοδος στην γεννήτρια κλειδιών τόσο πιο ασφαλή είναι τα κλειδιά που παράγονται. Σε σύγχρονα προγράμματα κρυπτογράφησης ο τυχαίος αριθμός παράγεται ως εξής: Κατά την διαδικασία κατασκευής των κλειδιών, το πρόγραμμα σταματάει για 5 λεπτά και καλεί τον χρήστη να συνεχίσει να εργάζεται με τον υπολογιστή. Στην συνέχεια για να παράξει τον τυχαίο αριθμό συλλέγει στα 5 αυτά λεπτά τυχαία δεδομένα που εξαρτώνται από την συμπεριφορά του χρήστη (κινήσεις ποντικιού, πλήκτρα του πληκτρολογίου που πατήθηκαν, κύκλοι μηχανής που καταναλώθηκαν κοκ). Με βάση αυτά τα πραγματικά τυχαία δεδομένα υπολογίζεται ο τυχαίος αριθμός και εισάγεται στην γεννήτρια κλειδιών για να κατασκευαστεί το δημόσιο και το ιδιωτικό κλειδί του χρήστη

Πιστοποίηση

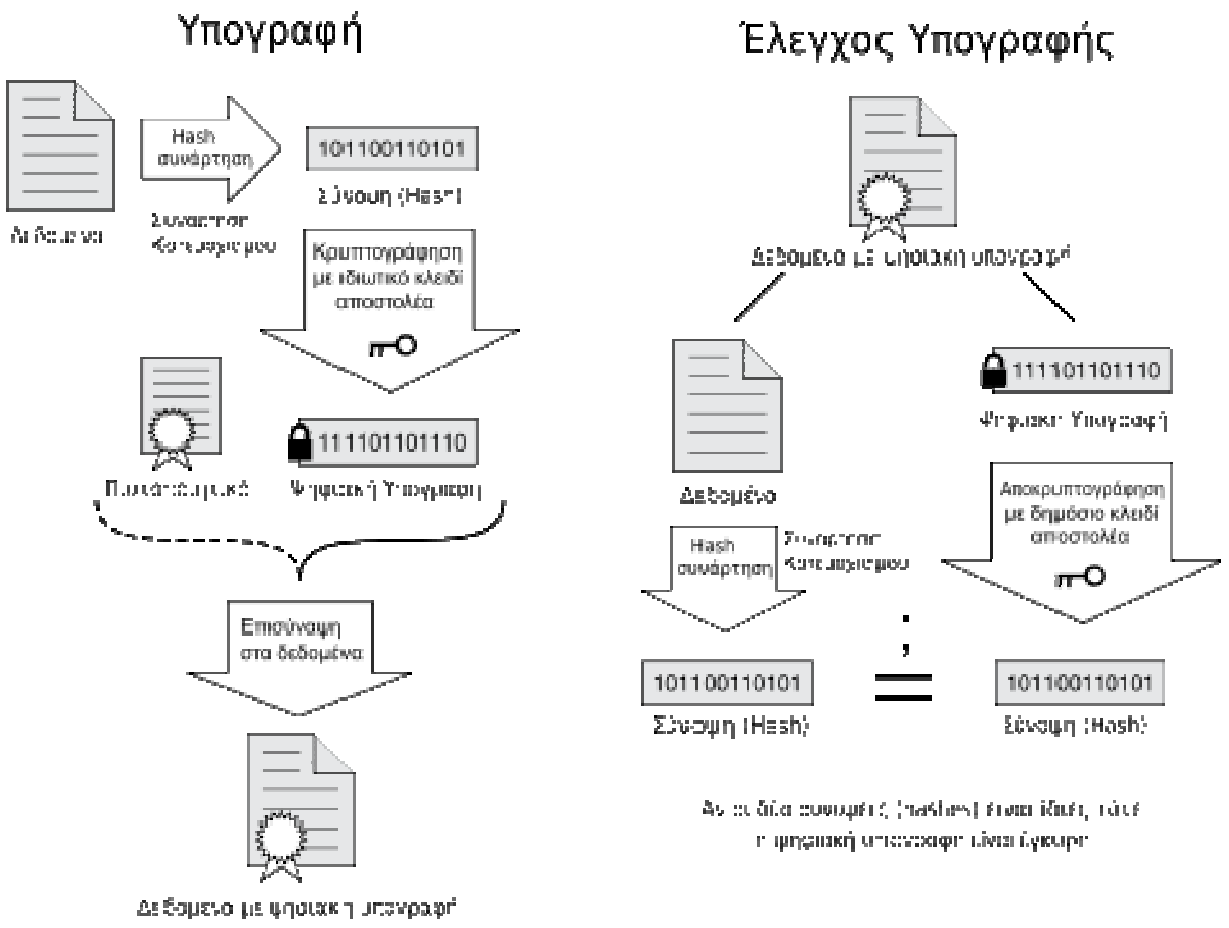
Χρησιμοποιώντας κατάλληλα τους κρυπτογραφικούς αλγορίθμους δημοσίου κλειδιού μπορεί να επιτευχθεί πιστοποίηση (authentication), δηλαδή ο παραλήπτης να γνωρίζει με ασφάλεια την ταυτότητα του αποστολέα. Για να επιτευχθεί αυτό θα πρέπει ο αποστολέας να χρησιμοποιήσει το ιδιωτικό του κλειδί για την κρυπτογράφηση του μηνύματος. Στην συνέχεια στέλνει το μήνυμα στον παραλήπτη και ο τελευταίος χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για την αποκρυπτογράφησή του. Δεδομένου ότι το ιδιωτικό κλειδί του αποστολέα είναι γνωστό μονάχα στον ίδιο, ο παραλήπτης μπορεί να είναι σίγουρος για την ταυτότητα του αποστολέα. Παρόλο που η παραπάνω μέθοδος εγγυάται την ταυτοποίηση του αποστολέα, δεν δύναται να εγγυηθεί την εμπιστευτικότητα του μηνύματος. Πράγματι, το μήνυμα μπορεί να το αποκρυπτογραφήσει οποιοσδήποτε διαθέτει το δημόσιο κλειδί του αποστολέα. Όπως έχει ήδη ειπωθεί, το δημόσιο κλειδί είναι γνωστό σε όλη την διαδικτυακή κοινότητα, άρα πρακτικά ο οποιοσδήποτε μπορεί να διαβάσει το περιεχόμενο του μηνύματος.

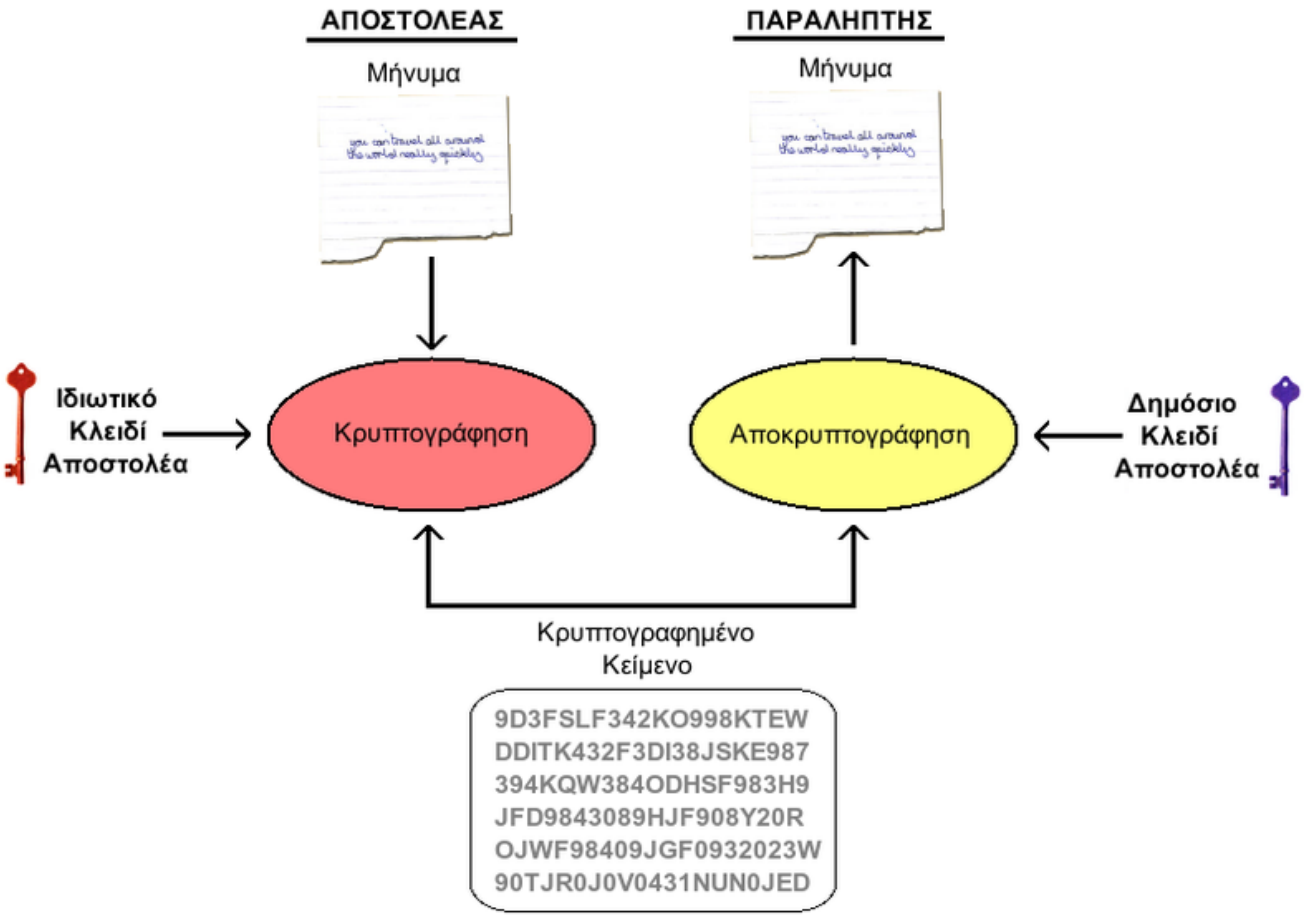
Ψηφιακές Υπογραφές

Η κρυπτογράφηση δημόσιου κλειδιού μαζί με την συνάρτηση κατατεμαχισμού (hash function) βρίσκει εφαρμογή στις ψηφιακές υπογραφές. Υπολογίζεται με την συνάρτηση κατεμαχισμού, η σύνοψη (digest) του μηνύματος/εγγράφου.Στην συνέχεια η σύνοψη κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα (ο οποίος με αυτήν την ενέργεια υπογράφει ψηφιακά το μήνυμα έγγραφο). Η κρυπτογραφημένη σύνοψη είναι η ψηφιακή υπογραφή η οποία επισυνάπτεται στο μήνυμα/έγγραφο. Μαζί με την ψηφιακή υπογραφή μπορεί να επισυναφθεί και ένα πιστοποιητικό του δημόσιου κλειδιού (το οποίο έχει εκδοθεί από κάποιο αξιόπιστο πάροχο/οργανισμό υπηρεσιών πιστοποίησης: το πιστοποιητικό ταυτοποιεί ένα δημόσιο κλειδί με τον δικαιούχο του). Στην διαδικασία ελέγχου της ψηφιακής υπογραφής, ξεχωρίζεται η ψηφιακή υπογραφή από το μήνυμα/έγγραφο. Η ψηφιακή υπογραφή αποκρυπτογραφείται με το δημόσιο κλειδί του αποστολέα και εξάγεται η σύνοψη. Παράλληλα υπολογίζεται η σύνοψη του ληφθέντος μηνύματος/εγγράφου. Αν οι δύο συνόψεις είναι ίδιες σημαίνει ότι το μήνυμα/έγγραφο έχει την υπογραφή του αποστολέα (που ανήκει το δημόσιο κλειδί) και ότι το μήνυμα/έγγραφο δεν έχει παραποιηθεί κατά την μεταφορά.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP Key Server 0.9.6

mQGiBDmXx8cRBADd0Dko7J7Gb5G/FINwO48AgrlYE87wCT5dlqSXl2uoDmR0/dKp
pJmvDeLQw+Z02yGx7TKf7PC5dfh61tIHyeI0SfCZVA5DtRDk3keNXy2WLnLMg2yS
J44JG3I/o1QKXL8PKD2bkv/vUl7gtXe3qa57oC+2ZmxzptnLeBh08QrWXwCg/8A2
L7WHGKbhYKCApM+0FJStYrcD/1iTYhNsiZnW2tc86e/uHiX8rg7tD7VGm/Wg2E4V
Hadsb4wMLhlfi/vCSEZmlH3hFxvGk6YCWXkdFxzqhq2ZJRWQStqZqjSPWTI3HvOK
Nzjq5DbRMQY2O025g1FyWB62ZDrUWXqzybi4okoEdXT/lQA7Xe95T8uy1zfTUmBg
ieTtA/0RU3MYboVOyDgGvJ7fVyFNdk8+v6Hzcn6EZMWYJifE5hw/tSLnRAXb7ejh
wsLDDCGsjloUj4TnMHH0LUTZSWbgDZwCF6tig3mbhk7YH21zWrVQwPidSpS5O3Oh
85V3nJx5r0406nM4N1cp46yKUMekE6nhubCpVme6o+f9sUMXkLQhR2VydCBLYXNw
ZXJzZW4gPGdla2FzQHdtkGF0YS5jb20+iQBLBBARAgALBQI5l8fHBAsDAgEACgkQ
Ls3rBj/p+6oQGwCgv5ML3xAatvJtY1mKnwz1SH2YbJ8AoPeBkUY73P+QDc5aFdHC
rCkobzlYuQQNBDmXx8cQEAD5GKB+WgZhekOQldwFbIeG7GHszUUfDtjgo3nGydx6
C6zkP+NGlLYwSlPXfAIWSIC1FeUpmamfB3TT/+OhxZYgTphluNgN7hBdq7YXHFHY
UMoiV0MpvpXoVis4eFwL2/hMTdXjqkbM+84X6CqlFGHjhKlP0YOEqHm274+nQ0YI
xswdd1ckOErixPDojhNnl06SE2H22+slDhf99pj3yHx5sHIdOHX79sFzxIMRJitD
YMPj6NYK/aEoJguuqa6zZQ+iAFMBoHzWq6MSHvoPKs4fdIRPyvMX86RA6dfSd7ZC
LQI2wSbLaF6dfJgkCo1+Le3kXXn11JJPmxiO/CqnS3wy9kJXtwh/CBdyorrWqULz
Bej5UxE5T7bxbrlLOCDaAadWoxTpj0BV89AHxstDqZSt90xkhkn4DIO9ZekX1KHT
UPj1WV/cdlJPPT2N286Z4VeSWc39uK50T8X8dryDxUcwYc58yWb/Ffm7/ZFexwGq
01uejaClcjrUGvC/RgBYK+X0iP1YTknbzSC0neSRBzZrM2w4DUUdD3yIsxx8Wy2O
9vPJI8BD8KVbGI2Ou1WMuF040zT9fBdXQ6MdGGzeMyEstSr/POGxKUAYEY18hKcK
ctaGxAMZyAcpesqVDNmWn6vQClCbAkbTCD1mpF1Bn5x8vYlLIhkmuquiXsNV6z3W
FwACAhAAumPF6HT301BhkfuMTVI2jFXUJ7prdWy4pwZArvdDVYQ35M8sG/ISJjwg
B2GdpK9i02B25Cen309snDSj/aJkz7PQgD8CyB1V0KiDFX+KxR8S0le2k1tdbiP3
wNYxw7MDiz757IY9/hmv6YDwSeS2sWnyjgfQXR5z2RBs4r+UZ8YWk8h4YQsLSL2B
Z/PImaiopMScDJy1m4AzasXNdyr1SywU4tlwOXZhZh6ccZB/z6nlZJgMnwfVw1fZ
8wyiTKGoyOp5eh9edDFwtcAVNHVoI0hj9kDfa5sfA9zcKfeLH7TouYLuMcdws9Uc
fNeJI6AgzUvGwzvG9HVuVGf7n5b1j9Kp+jcSjvWqpQX1/iDEN8KG6/yk5mtok4lv
JBieGM2SahP1cTk1P4kcrlwJ419EhKtC6xZS96J0+TmyLBTSrJHazWR+n/lQsXvz
g7wNUycZx+/v1QDGO3HyekqZR76BSMVrpNEYEWcBclTeJ6nBJCPTGxqvP4IQhzhJ
3znANVOsViJZ7rG3DrygE+8vQ32GjbBZzouN/gHxmSKOuvw6yjFdkiSMNNdlIeKm
05Z5aVSXPuE7+TfkbFGHy+GCxjsH6FNhU/8QKtr712NO9laDARGCVaOiVvBVevVO
PXajFSW19F7Rswmh7kD5jUEy9E7ANAa0YD5i07ee0wvmaGSwfKKIRgQYEQIABgUC
OZfHxwAKCRAuzesGP+n7qj2kAJ48xQqu8b8kzQHmmUvMFr8z+bfivQCgxXhBHUT1
LsvbbxbTJ/Da6n5YSYE=
=9v+B
-----END PGP PUBLIC KEY BLOCK-----
```


Υπογραφή
Hash συνάρτηση
101100110101
Κρυπτογράφηση με ιδιωτικό κλειδί αποστολέα
111101101110
Επισύναψη στα δεδομένα
Έλεγχος Υπογραφής
Δεδομένο
Hash συνάρτηση
101100110101
Αποκρυπτογράφηση με δημόσιο κλειδί αποστολέα
111101101110
101100110101


ΑΠΟΣΤΟΛΕΑΣ
Μήνυμα
ΠΑΡΑΛΗΠΤΗΣ
Μήνυμα
Ιδιωτικό Κλειδί Αποστολέα
Κρυπτογράφηση
Αποκρυπτογράφηση
Δημόσιο Κλειδί Αποστολέα
Κρυπτογραφημένο Κείμενο
9D3FSLF342KO998KTEW
DDITK432F3DI38JSKE987
394KQW384ODHSF983H9
JFD9843089HJF908Y20R
OJWF98409JGF0932023W
90TJR0J0V0431NUN0JED

ΣΤΕΓΑΝΟΓΡΑΦΙΑ-ΤΕΧΝΗ ΤΗΣ ΑΠΟΠΛΑΝΗΣΗΣ

Ο άνθρωπος σε όλη τη διαδρομή της ιστορίας ανακάλυπτε συνεχώς νέες μεθόδους για να κρύψει μηνύματα αλλα και να αποδικωποιησει μηνύματα. Μια παρα πολύ σημαντική τεχνική ήταν η μέθοδος της στενογραφίας. Σε αντίθεση με την κρυπτογράφηση στην όποια το μήνυμα φαίνεται, ενώ στη στενογραφία έχεις την δυνατότητα να κρύψεις ένα μήνυμα μέσα σ' ένα άλλο αθώο μήνυμα. Επίσης στις μέρες μας η τεχνική της στενογραφίας έχει αναπτυχτεί θετικά και στην τεχνική της επικοινωνίας όπου εκεί μπορείς να κρύψεις τη ιδία την ύπαρξη της πληροφορίας. Ο καλυτερος τροπος για να κρύψεις ένα μήνυμα είναι με την μεθοδο της στενογραφίας διοτι έχεις την ευχερια να κρύψεις το μήνυμα μέσα σ΄ ένα άλλο που διχνει «αθώο» ετσι ώστε να μην γινεται αντιληπτο στον εχθρο.Παρ' όλα αυτά όμως το αρνητικο που προβαλλει η στενογραφία είναι ότι αν καποιος ξερει που έχεις κρυψει το μήνυμα, θα είναι ευκολο να το βρει!Αλλος δυνατος συνδιασμος θα ηταν αν καποιος μπορουσε να στεγανογραφησει καποιο κρυπτογραφημενο μηνυμα.Μερικες φορες όμως δεν πρεπει να βασιζομαστε μονο στα στοιχεια που μας δινουν αλλα ουτε ότι είναι ένα μυστικο διοτι καποιος άλλος μπορει να παραδωσει το μυστικο αυτό,αφηνοντας αυτόν που το έχει κρυψει να νομιζει ότι είναι ασφαλες.Ενα παραδειγμα στενογραφίας οσο αναφορα τους αρχαιοτερους χρονους λεγεται, ότι σε μια αφηγηση ιστορικου γεγονοτος αναφερεται ότι ο Δημοκριτος ηθελε να ειδοποιησει τη Σπαρτη ότι ο Ξερξης προτιθετο να εισβαλλει στην Ελλαδα.Για να αποφυγει την κλοπη του μηνυματος εγραψε το μήνυμα του σε ξυλινη πινακιδα αφου εξυσε το κερι που αυτή ειχε και την οποια καλυψε παλι με κερι. Ακομα η στεγανογραφια,δηλαδη η κρυμμενη γραφη, είναι η ελληνικη λεξη και τεχνική γνωστη ηδη από την εποχη του Ηροδοτου που

χρησιμοποιηθηκε κατά κορον στη Γερμανια(και όχι μονον του

δευτερου παγκοσμιου πολεμου)και εδώ και χρονια απεκτησε ηλεκτρονικη υποσταση. Αρα λοιπον τι είναι το καινουριο,δεδομενου ιδιως ότι η κρυπτογραφηση-κωδικοποιηση είναι ευρεως διαδεδομενη στον κοσμο της πληροφορικης. « Το καινουριο που κομιζει η στεγανογρφια είναι ότι το κτυπτογραφημενο μήνυμα δεν φαινεται κρυπτογραφημενο. Δηλαδη, κρυβουμε το κρυμμενο μήνυμα

ΚΡΥΠΤΟΓΡΑΦΗΜΑ V□GENERE

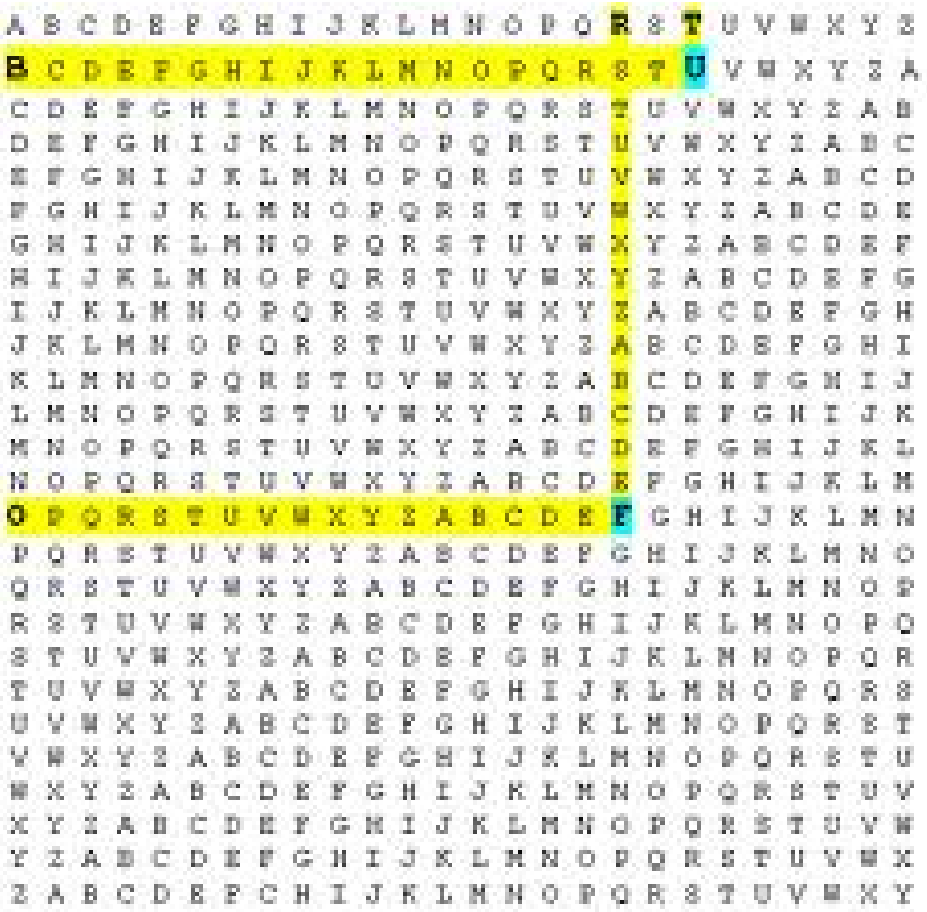
Vigere κρυπτογράφημα είναι μια μορφή περιοδικής αντικατάστασης και βασίζεται σ ένα άλλο μετατοπισμένο αλφάβητο. η κρυπτογράφηση της λέξης SUBSTITUTION υπό το κλειδί BAND.

M= SUBS TITU TION

K= BAND BAND BAND

Ek= TUOV UIGC UIBQ

Το πρώτο γράμμα μετατοπίζεται στα δεξιά κατά μια θέση, το δεύτερο κατά 0 , το τρίτο κατά 13 και το τέταρτο κατά 3.



ΜΑΡΙΑ ΤΗΣ ΣΚΩΤΙΑΣ

Η ελισαβετιανή Αγγλία είχε πολλούς λογούς να περηφανεύεται:

Ήταν το κέντρο του ευρωπαϊκού εμπορίου, ήταν η πατρίδα του Σαίξπηρ και είχε αρχίσει να ιδρύει αποικίες στο Νέο Κόσμο. Όμως είχε περιορισμένη στρατιωτική δύναμη και ζούσε κάτω από την συνεχή απειλή της εισβολής της Ισπανίας και της Γαλλίας. Ανίκανη να ανταγωνιστεί τους εχθρούς της, η βασίλισσα Ελισάβετ αναγκάστηκε να τους παρασύρει σε μια διπλωματική αναμέτρηση. Το μυστικό της όπλο ήταν ο Σερ Φράνσις Ουολσινχαμ, που έφερε το μετριοπαθή τίτλο του αρχιγραμματέα της , ενώ στην πραγματικότητα ήταν κατάσκοπος. Ο ουολσινχαμ χειραγωγούσε τις καθολικές χώρες με μια δύναμη που υπερείχε κατά πολύ της ισπανικής ομάδας: τη κατασκοπεία! Σπέρνοντας η στρατολογώντας κατασκόπους σε όλες τις ξένες αυλές της Ευρώπης αλλά και στη κάρδια των εγχώριων συνωμοτών. Ο ουολσινχαμ αντιμετώπισε επαναλαμβανόμενες απόπειρες κατά της βασίλισσας στο αγγλικό έδαφος.Χχρησιμοποίησε τα μαθηματικά και την αποδικωποιηση προκειμένου να αποκρυπτογραφήσει μηνύματα που αντάλλασσαν οι πρέσβεις με τους βασιλείς. Οργάνωσε δίκτυο ευφυούς προπαγάνδας παραπληροφόρηση, ώστε να εξουδετερώσει τους αντίπαλους της Αγγλίας και να παραπλανήσει τους συμμάχους της. Τέλος με μοναδική πανουργία παρέσυρε τη Μαρία της Σκωτίας σε συνομωσία εναντία στη ζωή της Ελισάβετ και έστειλε την καθολική βασίλισσα στην αγχόνη. Οι μυστικές επιχειρήσεις ήταν το δυνατό σημείου του Ουολσινχαμ και οι πρωτοποριακές του τεχνικές παραμένουν μέχρι σήμερα βασικά εργαλεία της διεθνούς κατασκοπείας.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Όσο αναφορά για την στενογραφία έχει προσφέρει πολύτιμη βοήθεια ειδικά στους αρχαίους χρόνους βοηθώντας να στέλνονται αλλά και να λαμβάνονται μηνύματα με την χρήση άλλων μηνυμάτων τα οποία φαίνονται αθώα στα μάτια της αντίπαλης παράταξης. Επίσης πολύτιμη είναι η συνεισφορά της στην σημερινή κοινωνία έχοντας την δυνατότητα να κρύψεις μηνύματα σε κάποιο άλλο αρχείο υπολογιστή πχ. Ipeg

Το κρυπτογράφημα vigenere είναι μια μορφή περιοδικής αντικατάστασης που βασιζόταν σ ένα μετατοπισμένο αλφάβητο.

Τέλος το συμπέρασμα που βγάζουμε από την Μαρία της Σκωτίας είναι πως μέσω δολοπλοκιών-συνομοσιων και η συμβολή κυριότερα της κατασκοπίας άνοιξαν το δρόμο για τις μετέπειτα υπηρεσίες κατασκοπείας όπου είχε αρχίσει ο Ουολσινχαμ

Πρωτη περιοδος κρυπτογραφιας (1900 π.Χ.-1900 μ.Χ.)

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

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

Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Γύρω στον 5ο π.Χ. αιώνα εφηύραν την «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποίησαν για την κρυπτογράφηση τη μέθοδο της αντικατάστασης. Όπως αναφέρει ο Πλούταρχος, η «Σπαρτιατική Σκυτάλη» Σχήμα (2.1), ήταν μια ξύλινη ράβδος, ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα, όταν δε ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο

εξαιτίας της ανάμειξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης.

Σχήμα 2.1 Η Σπαρτιατική Σκυτάλη, μια πρώιμη συσκευή για την κρυπτογράφηση

Στην αρχαιότητα χρησιμοποιήθηκαν κυρίως συστήματα, τα οποία βασίζονταν στηστεγανογραφία και όχι τόσο στην κρυπτογραφία. Οι Έλληνες συγγραφείς δεν αναφέρουν αν και πότε χρησιμοποιήθηκαν συστήματα γραπτής αντικατάστασης γραμμάτων, αλλά τα βρίσκουμε στους Ρωμαίους, κυρίως την εποχή του Ιουλίου Καίσαρα. Ο Ιούλιος Καίσαρας έγραφε στον Κικέρωνα και σε άλλους φίλους του, αντικαθιστώντας τα γράμματα του κειμένου, με γράμματα, που βρίσκονται 3 θέσεις μετά, στο Λατινικό Αλφάβητο. Έτσι, σήμερα, το σύστημα κρυπτογράφησης που στηρίζεται στην αντικατάσταση των γραμμάτων του αλφαβήτου με άλλα που βρίσκονται σε καθορισμένο αριθμό θέσης πριν ή μετά, λέγεται κρυπτοσύστημα αντικατάστασης του Καίσαρα. Ο Καίσαρας χρησιμοποίησε και άλλα, πιο πολύπλοκα συστήματα κρυπτογράφησης, για τα οποία έγραψε ένα βιβλίο ο Valerius Probus, το οποίο δυστυχώς δεν διασώθηκε, αλλά αν και χαμένο, θεωρείται το πρώτο βιβλίο κρυπτολογίας. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες.

Στη διάρκεια του Μεσαίωνα, η κρυπτολογία ήταν κάτι το απαγορευμένο και αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας, κάτι που συντέλεσε στην καθυστέρηση της ανάπτυξης της. Η εξέλιξη, τόσο της κρυπτολογίας, όπως και των μαθηματικών, συνεχίζεται στον Αραβικό κόσμο. Στο γνωστό μυθιστόρημα «Χίλιες και μία νύχτες» κυριαρχούν οι λέξεις-αινίγματα, οι γρίφοι, τα λογοπαίγνια και οι αναγραμματισμοί. Έτσι, εμφανίστηκαν βιβλία που περιείχαν κρυπταλφάβητα, όπως το αλφάβητο «Dawoudi» που πήρε το όνομα του από τον βασιλιά Δαυίδ. Οι Άραβες είναι οι πρώτοι που επινόησαν αλλά και χρησιμοποίησαν μεθόδους κρυπτανάλυσης. Το κυριότερο εργαλείο στην κρυπτανάλυση, η χρησιμοποίηση των συχνοτήτων των γραμμάτων κειμένου, σε συνδυασμό με τις συχνότητες εμφάνισης στα κείμενα των γραμμάτων της γλώσσας, επινοήθηκε από αυτούς γύρω στον 14ο αιώνα. Η κρυπτογραφία, λόγω των στρατιωτικών εξελίξεων, σημείωσε σημαντική ανάπτυξη στους επόμενους αιώνες. Ο Ιταλός *Giovanni Batista Porta*, το 1563, δημοσίευσε το περίφημο για την κρυπτολογία βιβλίο «*De furtivis literarum notis*», με το οποίο έγιναν γνωστά τα πολυαλφαβητικά συστήματα κρυπτογράφησης και τα διγραφικά κρυπτογραφήματα, στα οποία, δύο γράμματα αντικαθίστανται από ένα. Σημαντικός εκπρόσωπος εκείνης της εποχής είναι και ο Γάλλος *Vigenere*, του οποίου ο πίνακας πολυαλφαβητικής αντικατάστασης, χρησιμοποιείται ακόμη και σήμερα.

Ο *C.Wheatstone*, γνωστός από τις μελέτες του στον ηλεκτρισμό, παρουσίασε την πρώτη μηχανική κρυπτοσυσκευή, η οποία απετέλεσε τη βάση για την ανάπτυξη των κρυπτομηχανών της δεύτερης ιστορικής περιόδου της κρυπτογραφίας. Η μεγαλύτερη αποκρυπτογράφηση ήταν αυτή των αιγυπτιακών ιερογλυφικών τα οποία, επί αιώνες, παρέμεναν μυστήριο και οι αρχαιολόγοι μόνο εικασίες μπορούσαν να διατυπώσουν για τη σημασία τους. Ωστόσο, χάρη σε μία κρυπταναλυτική εργασία, τα ιερογλυφικά εν τέλει αναλύθηκαν και έκτοτε οι αρχαιολόγοι είναι σε θέση να

διαβάζουν ιστορικές επιγραφές. Τα αρχαιότερα ιερογλυφικά χρονολογούνται περίπου από το 3000 π.Χ. Τα σύμβολα των ιερογλυφικών ήταν υπερβολικά πολύπλοκα για την καταγραφή των συναλλαγών εκείνης της εποχής. Έτσι, παράλληλα με αυτά, αναπτύχθηκε για καθημερινή χρήση η ιερατική γραφή, που ήταν μία συλλογή συμβόλων, τα οποία ήταν εύκολα τόσο στο γράψιμο όσο και στην ανάγνωση. Τον 17ο αιώνα αναθερμάνθηκε το ενδιαφέρον για την αποκρυπτογράφηση των ιερογλυφικών, έτσι το 1652 ο Γερμανός Ιησουΐτης Αθανάσιος Κίρχερ εξέδωσε ένα λεξικό ερμηνείας τους, με τίτλο «*Oedipus Aegyptiacus*». Με βάση αυτό προσπάθησε να ερμηνεύσει τις αιγυπτιακές γραφές, αλλά η προσπάθεια του αυτή ήταν κατά γενική ομολογία αποτυχημένη. Για παράδειγμα, το όνομα του Φαραώ Απρίη, το ερμήνευσε σαν «τα ευεργετήματα του θεϊκού Όσιρι εξασφαλίζονται μέσω των ιερών τελετών της αλυσίδας των πνευμάτων, ώστε να επιδαψιλεύσουν τα δώρα του Νείλου». Παρόλα αυτά, η προσπάθεια του άνοιξε τον δρόμο προς τη σωστή ερμηνεία των ιερογλυφικών, που προχώρησε χάρη στην ανακάλυψη της «Στήλης της Ροζέτας». Ήταν μια πέτρινη στήλη που βρήκαν τα στρατεύματα τουΝαπολέοντα στην Αίγυπτο και είχε χαραγμένο πάνω της το ίδιο κείμενο τρεις φορές. Μια με ιερογλυφικά, μια στα ελληνικά και μια σς ιερατική γραφή. Δύο μεγάλοι αποκρυπτογράφοι της εποχής, ο Γιάνγκ και ο Σαμπολιόν, μοιράστηκαν τη δόξα της ερμηνείας τους. Οι προϊστορικοί πληθυσμοί χρησιμοποίησαν τρεις γραφές μέχρι να επινοήσουν αλφάβητο, γύρω στο 850 π.Χ.

Χρονολογικά, οι γραφές αυτές κατατάσσονται ως εξής

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

Η Κρητική εικονογραφική (ή ιερογλυφική) γραφή δεν μας έχει αποκαλύψει τον κώδικα της, γνωρίζουμε ωστόσο ότι δεν πρόκειται για γραφή που χρησιμοποιεί εικόνες ως σημεία, αλλά για φωνητική γραφή, η οποία εξαντλείται σε

περίπου διακόσιους σφραγιδόλιθους και συνυπήρχε με τη γραμμική γραφή Α, τόσο χρονικά όσο και τοπικά, όπως προκύπτει από τις ανασκαφές στο ανάκτορο των Μαλίων της Κρήτης. Εμφανίζεται στον Δίσκο της Φαιστού (Σχήμα 2.2), που ανακαλύφθηκε το 1908 στη νότια Κρήτη. Πρόκειται για μια κυκλική πινακίδα, που χρονολογείται γύρω στο 1700 π.Χ. και φέρει γραφή με τη μορφή δύο σπειρών. Τα σύμβολα δεν είναι χειροποίητα, αλλά έχουν χαραχθεί με τη βοήθεια μίας ποικιλίας σφραγίδων, καθιστώντας τον Δίσκο ως το αρχαιότερο δείγμα στοιχειοθεσίας. Δεν υπάρχει άλλο ανάλογο εύρημα και έτσι η αποκρυπτογράφηση στηρίζεται σε πολύ περιορισμένες πληροφορίες. Μέχρι σήμερα δεν έχει αποκρυπτογραφηθεί και παραμένει η πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή.

Σχήμα 2.2 Ο Δίσκος της Φαιστού

Οι πρώτες επιγραφές με Γραμμική γραφή ανακαλύφθηκαν από τον Άρθουρ Έβανς (Sir Arthur Evans), τον μεγάλο Άγγλο αρχαιολόγο, που άνεσκαψε συστηματικά την Κνωσό το1900. Ο ίδιος ονόμασε αυτή τη γραφή γραμμική, επειδή τα γράμματα της είναι γραμμές (ένα γραμμικό σχήμα) και όχι σφήνες, όπως στη σφηνοειδή

γραφή ή εικόνες όντων, όπως στην αιγυπτιακή ιερατική. Η γραμμική γραφή Α είναι μάλλον η γραφή των Μινωιτών (από το μυθικό Μίνωα, βασιλιά της Κνωσού), των κατοίκων της αρχαίας Κρήτης και από αυτή ίσως να προήλθε το σημερινό ελληνικό αλφάβητο. Τα γράμματα της γραμμικής γραφής χαράζονταν με αιχμηρό αντικείμενο πάνω σε πήλινες πλάκες, οι οποίες κατόπιν ξεραίνονταν σε φούρνους. Οι περισσότερες από τις επιγραφές με Γραμμική γραφή Α (περίπου 1500) είναι λογιστικές και περιέχουν εικόνες ή συντομογραφίες των εμπορεύσιμων προϊόντων και αριθμούς για υπόδειξη της ποσότητας ή οφειλής.

Ο Έβανς κατέγραψε 135 σύμβολα της. Χρησιμοποιήθηκε κυρίως στην Κρήτη, αν και ορισμένα πρόσφατα ευρήματα καταδεικνύουν ότι μπορεί να αποτέλεσε μέσο γραφής και αλλού, αφού επιγραφές με Γραμμική Α έχουν βρεθεί στην Κνωσό και Φαιστό της Κρήτης, αλλά και στη Μήλο και τη Θήρα. Πλάκες με επιγραφές σε γραμμική Α, εκτίθενται στοΜουσείο Ηρακλείου. Παρά την πρόοδο που έχει σημειωθεί, η γραμμική γραφή Α δεν έχει αποκρυπτογραφηθεί ακόμη. Ο Evans έδωσε και την ονομασία στη Γραμμική Γραφή Β, επειδή αναγνώρισε ότι πρόκειται για συγγενική γραφή με τη γραμμική Α, πιο πρόσφατη ωστόσο και εξελιγμένη. Με βάση όσα γνωρίζουμε σήμερα, η γραφή αυτή υιοθετήθηκε αποκλειστικά για λογιστικούς σκοπούς. Πινακίδες χαραγμένες με τη γραμμική γραφή Β βρέθηκαν στην Κνωσό, στα Χανιά αλλά και στην Πύλο, τις Μυκήνες, τη Θήβα και τηνΤίρυνθα. Σήμερα αποτελούν ένα σύνολο 10.000 τεμαχίων. Τα σχήματα των πινακίδων της γραφής αυτής ποικίλουν, επικρατούν όμως οι φυλλοειδείς και «σελιδόσχημες», οι οποίες διαφέρουν ως προς τις διαστάσεις, ανάλογα με τις προτιμήσεις του κάθε γραφέα. Έπλαθαν πηλό σε σχήμα κυλίνδρου, τον τοποθετούσαν σε λεία επιφάνεια και την πίεζαν μέχρι να γίνει επίπεδη, επιμήκης και συμπαγής πινακίδα, σαφώς διαφοροποιημένη σε δύο επιφάνειες: μία επίπεδη λειασμένη, που επρόκειτο να αποτελέσει την κύρια γραφική επιφάνεια και μία κυρτή, που συνήθως έμενε άγραφη. Πολλές φορές, όταν τα κείμενα απαιτούσαν περισσότερες από μία πινακίδες, έχουμε τις

αποκαλούμενες «ομάδες» ή «πολύπτυχα» πινακίδων, οι οποίες εμφανίζουν κοινά χαρακτηριστικά και ως προς την αποξήρανση και το μίγμα του πηλού και κυρίως, ως προς το γραφικό χαρακτήρα του ίδιου του γραφέα. Τα πολύπτυχα αυτά φυλάσσονταν σε αρχειοφυλάκια και ταξινομούνταν κατά θέματα σε ξύλινα κιβώτια. Για να γνωρίζει ο ενδιαφερόμενος το περιεχόμενο των καλαθιών, κυρίως, χρησιμοποιούσαν ετικέτες: ένα σφαιρίδιο πηλού, εντυπωμένο στην πρόσθια πλευρά, στο οποίο καταγράφονταν συνοπτικές πληροφορίες. Συστηματικά, με τη γραφή αυτή, με την οποία είχε πραγματικό πάθος, ασχολήθηκε ο Άγγλος αρχιτέκτονας και ερασιτέχνης αρχαιολόγος Μ. Βέντρις. Ήταν ο πρώτος που κατάλαβε ότι επρόκειτο για κάποιο είδος ελληνικής γραφής, αλλά η άποψη του αυτή δεν έγινε δεκτή αρχικά από τους ειδικούς. Στη συνέχεια, όμως, αρκετοί προσχώρησαν στην άποψή του. Ένας από αυτούς ήταν ο κρυπταναλυτής Τζον Τσάντγουικ, ο οποίος, στη διάρκεια του πολέμου, είχε εργασθεί στην ανάλυση της γερμανικής κρυπτομηχανής Enigma. Προσπάθησε να μεταφέρει την πείρα του στην κρυπτανάλυση της Γραμμικής Β, αλλά χωρίς επιτυχία μέχρι τότε. Όμως, ο συνδυασμός των δύο επιστημόνων έφερε το πολυπόθητο αποτέλεσμα.
Το 1953 κατέγραψαν τα συμπεράσματά τους στο μνημειώδες έργο «Μαρτυρίες για την ελληνική διάλεκτο στα μυκηναϊκά αρχεία», που έγινε το πιο διάσημο άρθρο κρυπτανάλυσης. Η αποκρυπτογράφηση της Γραμμικής Β απέδειξε ότι επρόκειτο για ελληνική γλώσσα, ότι οι Μινωίτες της Κρήτης μιλούσαν ελληνικά και ότι η δεσπόζουσα δύναμη εκείνη την εποχή ήταν οι Μυκήνες. Η αποκρυπτογράφηση της Γραμμικής Β θεωρήθηκε επίτευγμα ανάλογο της κατάκτησης του Έβερεστ, που συνέβη την ίδια ακριβώς εποχή. Για αυτό και έγινε γνωστή σαν το «Έβερεστ της Ελληνικής αρχαιολογίας».

Δευτερη περιοδος κρυπτογραφιας (1900 μ.Χ.-1950 μ.Χ.)

Η δεύτερη περίοδος της κρυπτογραφίας όπως προαναφέρθηκε τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950. Καλύπτει, επομένως, τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων (λόγω της εξαιρετικά μεγάλης ανάγκης που υπήρξε για ασφάλεια κατά τη μετάδοση ζωτικών πληροφοριών μεταξύ των στρατευμάτων των χωρών) αναπτύχθηκε η κρυπτογραφία τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές». Η κρυπτανάλυση τους, απαιτεί μεγάλο αριθμό προσωπικού, το οποίο εργαζόταν επί μεγάλο χρονικό διάστημα ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ. Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά τη διάρκεια αυτής της περιόδου η κρυπτανάλυση τους είναι συνήθως επιτυχημένη.Οι Γερμανοί έκαναν εκτενή χρήση (σε διάφορες παραλλαγές) ενός συστήματος γνωστού ως Enigma (Εικόνα 2.3).

[[Αρχείο:Enigma.jpg|thumb|400px|Εικόνα 2.3 : Η μηχανή Αίνιγμα χρησιμοποιήθηκε ευρέως στη Γερμανία Ο Marian Rejewski, στην Πολωνία, προσπάθησε και, τελικά, παραβίασε την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma (που χρησιμοποιούσε μια ηλεκτρομηχανική κρυπτογραφική συσκευή) χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ήταν η μεγαλύτερη σημαντική ανακάλυψη στην κρυπτολογική ανάλυση της εποχής. Οι Πολωνοί συνέχισαν να αποκρυπτογραφούν τα μηνύματα που βασιζονταν στην κρυπτογράφηση με το Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε ορισμένες σημαντικές αλλαγές

και οι Πολωνοί δεν μπόρεσαν να τις παρακολουθήσουν, επειδή η αποκρυπτογράφηση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν. Έτσι, εκείνο το καλοκαίρι μεταβίβασαν τη γνώση τους, μαζί με μερικές μηχανές που είχαν κατασκευάσει, στους Βρετανούς και τους Γάλλους. Ακόμη και ο Rejewski και οι μαθηματικοί και κρυπτογράφοι του, όπως ο Biuro Szyfrow, κατέληξαν σε συνεργασία με τους Βρετανούς και τους Γάλλους μετά από αυτή την εξέλιξη. Η συνεργασία αυτή συνεχίστηκε από τον Άλαν Τούρινγκ (Alan Turing), τον Γκόρντον Ουέλτσμαν (Gordon Welchman) και από πολλούς άλλους στοΜπλέτσλεϊ Παρκ (Bletchley Park), κέντρο της Βρετανικής Υπηρεσίας απο/κρυπτογράφησης και οδήγησε σε συνεχείς αποκρυπτογραφήσεις των διαφόρων παραλλαγών του Enigma, με τη βοήθεια και ενός υπολογιστή, που κατασκεύασαν οι Βρετανοί επιστήμονες, ο οποίος ονομάσθηκε Colossus και, δυστυχώς, καταστράφηκε με το τέλος του Πολέμου. Οι κρυπτογράφοι του αμερικανικού ναυτικού (σε συνεργασία με Βρετανούς και Ολλανδούς κρυπτογράφους μετά από το1940) έσπασαν αρκετά κρυπτοσυστήματα του Ιαπωνικού ναυτικού. Το σπάσιμο ενός από αυτά, του JN-25, οδήγησε στην αμερικανική νίκη στη Ναυμαχία της Μιντγουέι καθώς και στην εξόντωση του Αρχηγού του Ιαπωνικού Στόλου Ιζορόκου Γιαμαμότο.

Το Ιαπωνικό Υπουργείο Εξωτερικών χρησιμοποίησε ένα τοπικά αναπτυγμένο κρυπτογραφικό σύστημα, (που καλείται Purple), και χρησιμοποίησε, επίσης, διάφορες παρόμοιες μηχανές για τις συνδέσεις μερικών ιαπωνικών πρεσβειών. Μία από αυτές αποκλήθηκε "Μηχανή-Μ" από τις ΗΠΑ, ενώ μια άλλη αναφέρθηκε ως «Red» (Κόκκινη). Μια ομάδα του αμερικανικού στρατού, η αποκαλούμενη SIS, κατάφερε να σπάσει το ασφαλέστερο ιαπωνικό διπλωματικό σύστημα κρυπτογράφησης (μια ηλεκτρομηχανική συσκευή, η οποία αποκλήθηκε "Purple" από τους Αμερικανούς) πριν καν ακόμη αρχίσει ο Β΄ Παγκόσμιος Πόλεμος. Οι Αμερικανοί αναφέρονται στο αποτέλεσμα της κρυπτανάλυσης, ειδικότερα της μηχανής Purple, αποκαλώντας το ως Magic (Μαγεία).

Οι συμμαχικές κρυπτομηχανές που χρησιμοποιήθηκαν στον δεύτερο παγκόσμιο πόλεμο περιλάμβαναν το βρετανικό TypeX και το αμερικανικό SIGABA (Σχήμα 2.4). Και τα δύο ήταν ηλεκτρομηχανικά σχέδια παρόμοια στο πνεύμα με το Enigma, με σημαντικές εν τούτοις βελτιώσεις. Κανένα δεν έγινε γνωστό ότι παραβιάστηκε κατά τη διάρκεια του πολέμου. Τα στρατεύματα στο πεδίο μάχης χρησιμοποίησαν το M-209 και τη λιγότερη ασφαλή οικογένεια κρυπτομηχανών M-94. Οι Βρετανοί πράκτορες της Υπηρεσίας "SOE" χρησιμοποίησαν αρχικά ένα τύπο κρυπτογραφίας που βασιζόταν σε ποιήματα (τα απομνημονευμένα ποιήματα ήταν τα κλειδιά). Οι Γερμανοί, ώρες πριν την Απόβαση της Νορμανδίας συνέλαβαν ένα μήνυμα - ποίημα του Πολ Βερλέν, για το οποίο, χωρίς να το έχουν αποκρυπτογραφήσει, ήταν βέβαιοι πως προανάγγελε την απόβαση. Η Γερμανική ηγεσία δεν έλαβε υπόψη της αυτή την προειδοποίηση.[1]

Οι Πολωνοί είχαν προετοιμαστεί για την εμπόλεμη περίοδο κατασκευάζοντας την κρυπτομηχανή LCD Lacida, η οποία κρατήθηκε μυστική ακόμη και από τον Rejewski. Όταν. τον Ιούλιο του 1941 ελέγχθηκε από τον Rejewski η ασφάλειά της, του χρειάστηκαν μερικές μόνον ώρες για να την "σπάσει" και έτσι αναγκάστηκαν να την αλλάξουν βιαστικά. Τα μηνύματα που εστάλησαν με Lacida δεν ήταν, εντούτοις, συγκρίσιμα με αυτά του Enigma, αλλά η παρεμπόδιση θα μπορούσε να έχει σημάνει το τέλος της κρίσιμης κρυπταναλυτικής Πολωνικής προσπάθειας.

Τριτη περιοδος κρυπτογραφιας (1950 μ.Χ.-Σήμερα)

Αυτή η περίοδος χαρακτηρίζεται από την έξαρση της ανάπτυξης στους επιστημονικούς κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει ουσιαστικά με τον Claude Shannon, αναμφισβήτητα ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας. Το 1949δημοσίευσε το έγγραφο «Θεωρία επικοινωνίας των συστημάτων μυστικότητας» (*Communication Theory of Secrecy Systems*) στο τεχνικό περιοδικό Bell System και λίγο αργότερα στο βιβλίο του, «Μαθηματική Θεωρία της Επικοινωνίας» (*Mathematical Theory of Communication*), μαζί με τον Warren Weaver. Αυτά, εκτός από τις άλλες εργασίες του επάνω στη θεωρία δεδομένων και επικοινωνίας καθιέρωσε μια στερεά θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση. Εκείνη την εποχή η κρυπτογραφία εξαφανίζεται και φυλάσσεται από τις μυστικές υπηρεσίες κυβερνητικών επικοινωνιών όπως η NSA. Πολύ λίγες εξελίξεις δημοσιοποιήθηκαν ξανά μέχρι τα μέσα της δεκαετίας του '70, όταν όλα άλλαξαν.

Στα μέσα της δεκαετίας του '70 έγιναν δύο σημαντικές δημόσιες (δηλ. μη-μυστικές) πρόοδοι. Πρώτα ήταν η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES (Data Encryption Standard) στον ομοσπονδιακό κατάλογο της Αμερικής στις 17 Μαρτίου 1975. Το προτεινόμενο DES υποβλήθηκε από την IBM, στην πρόσκληση του Εθνικού Γραφείου των Προτύπων (τώρα γνωστό ως NIST), σε μια προσπάθεια να αναπτυχθούν ασφαλείς ηλεκτρονικές εγκαταστάσεις επικοινωνίας για επιχειρήσεις όπως τράπεζες και άλλες μεγάλες οικονομικές οργανώσεις. Μετά από τις συμβουλές και την τροποποίηση από την NSA, αυτό το πρότυπο υιοθετήθηκε και δημοσιεύθηκε ως ένα ομοσπονδιακή τυποποιημένο πρότυπο επεξεργασίας

πληροφοριών το 1977 (αυτήν την περίοδο αναφέρεται σαν FIPS 46-3). Ο DES ήταν ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης που εγκρίνεται από μια εθνική αντιπροσωπεία όπως η NSA. Η απελευθέρωση της προδιαγραφής της από την NBS υποκίνησε μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας.

Ο DES αντικαταστάθηκε επίσημα από τον AES το 2001 όταν ανήγγειλε ο NIST το FIPS 197. Μετά από έναν ανοικτό διαγωνισμό, ο NIST επέλεξε τον αλγόριθμο Rijndael, που υποβλήθηκε από δύο Φλαμανδούς κρυπτογράφους, για να είναι το AES. Ο DES και οι ασφαλέστερες παραλλαγές του όπως ο 3DES ή TDES χρησιμοποιούνται ακόμα σήμερα, ενσωματωμένος σε πολλά εθνικά και οργανωτικά πρότυπα. Εντούτοις, το βασικό μέγεθος των 56-bit έχει αποδειχθεί ότι είναι ανεπαρκές να αντισταθεί στις επιθέσεις ωμής βίας (μια τέτοια επίθεση πέτυχε να σπάσει τον DES σε 56 ώρες ενώ το άρθρο που αναφέρεται ως το σπάσιμο του DES δημοσιεύτηκε από τον O'Reilly and Associates). Κατά συνέπεια, η χρήση απλής κρυπτογράφησης με τον DES είναι τώρα χωρίς την αμφιβολία επισφαλής για χρήση στα νέα σχέδια των κρυπτογραφικών συστημάτων και μηνύματα που προστατεύονται από τα παλαιότερα κρυπτογραφικά συστήματα που χρησιμοποιούν DES, και όλα τα μηνύματα που έχουν αποσταλεί από το 1976 με τη χρήση DES, διατρέχουν επίσης σοβαρό κίνδυνο αποκρυπτογράφησης. Ανεξάρτητα από την έμφυτη ποιότητά του, το βασικό μέγεθος του DES (56-bit) ήταν πιθανά πάρα πολύ μικρό ακόμη και το 1976, πράγμα που είχε επισημάνει ο Whitfield Diffie. Υπήρξε επίσης η υποψία ότι κυβερνητικές οργανώσεις είχαν ακόμα και τότε ικανοποιητική υπολογιστική δύναμη ώστε να σπάσουν μηνύματα που είχαν κρυπτογραφηθεί με τον DES.

ΚΩΔΙΚΑΣ ΝΑΒΑΧΩΝ

Μόνον 50 από τους 400 Code Talkers βρίσκονται εν ζωή σήμερα. Οι περισσότεροι διαβιώνουν σε μια έκταση που τους έχει παραχωρηθεί από την αμερικανική κυβέρνηση, κάπου ανάμεσα στην Αριζόνα, το Νέο Μεξικό και τη Γιούτα. Αρκετοί είναι άρρωστοι ή σε βαθιά γεράματα και νιώθουν ότι δεν τους απομένει πολύς χρόνος για να εξιστορήσουν τη συνεισφορά τους στον Β' Παγκόσμιο Πόλεμο.

Προ ημερών, οι Code Talkers έφτασαν στην Νέα Υόρκη για να συμμετάσχουν για πρώτη φορά στη μεγαλύτερη παρέλαση βετεράνων.

Οι πεζοναύτες Ναβάχο χρησιμοποίησαν μυστικούς στρατιωτικούς όρους στη γλώσσα της συγκεκριμένης φυλής και βοήθησαν έτσι τις ΗΠΑ να επικρατήσουν στη μάχη της Ιβοζίμα αλλά και σε άλλες μάχες στον Ειρηνικό. Οι αξιωματικοί του αμερικανικού στρατού υποστήριξαν από τότε ότι ο κώδικας, ο οποίος μεταδιδόταν προφορικά μέσω ασυρμάτου, ήταν ο λόγος που βοήθησε να σωθούν αμέτρητες ζωές.

ΟΙ ΙΔΙΟΙ ΟΡΚΙΣΤΗΚΑΝ να κρατήσουν τον κώδικα μυστικό. Είναι ένας κώδικας τόσο περίπλοκος που ακόμα και οι Ναβάχο που υπηρετούσαν ως πεζοναύτες δεν μπορούσαν να σπάσουν. Ο κώδικας παρέμεινε μυστικός για δεκαετίες λόγω της πιθανής χρησιμότητάς του μετά το τέλος του πολέμου. «Κανείς δεν ισχυρίστηκε ποτέ ότι έχει "σπάσει" τον κώδικά μας. Επίσης δεν κοινοποιήθηκαν ποτέ στους υπόλοιπους οι ταυτότητες των 29 Ναβάχο που τον δημιούργησαν», είπε σε συνέντευξή του ένας από αυτούς, ο 85χρονος, Κιθ Λιτλ.

Ο ΜΕΓΑΛΥΤΕΡΟΣ από τους 13 εναπομείναντες Code Talkers που επιβιώνουν είναι 92 ετών, ενώ η ομάδα αυτή συμπεριλαμβάνει και έναν από τους αρχικούς 29 δημιουργούς του κώδικα. Πολλοί από τους Code Talkers που υπηρέτησαν στον πόλεμο ήταν νεαροί αγρότες και βοσκοί που δεν είχαν φύγει ποτέ από το σπίτι τους. Πριν

από τον κώδικα, οι Ιάπωνες υπέκλεπταν και σαμποτάριζαν τις στρατιωτικές επικοινωνίες των ΗΠΑ καθώς είχαν πολύ ικανούς μεταφραστές. Οι αμερικανικές δυνάμεις τότε αναγκάστηκαν να προσφύγουν στον κώδικα, ο οποίος ήταν βασισμένος στην αρχαία γλώσσα των Ναβάχο και άλλαξε τα δεδομένα στα πεδία των μαχών. Τις πρώτες 48 ώρες της μάχης της Ιβοζίμα, έξι Code Talkers δούλευαν ασταμάτητα, μεταδίδοντας και λαμβάνοντας περισσότερα από 800 μηνύματα για τις κινήσεις μονάδων, από τα οποία κανένα δεν αποκωδικοποιήθηκε από τους Ιάπωνες. Αυτό που προκαλούσε σύγχυση στον εχθρό ήταν ότι οι Code Talkers μπορούσαν να χρησιμοποιήσουν πολύ διαφορετικές λέξεις για το ίδιο ακριβώς μήνυμα.

Η ΑΝΑΓΝΩΡΙΣΗ από την αμερικανική κυβέρνηση -ακόμα και από την ίδια την κοινότητα των Ναβάχο- άργησε να έρθει, αφού μόλις το 2000 τους απονεμήθηκε το Χρυσό Μετάλλιο του Κογκρέσου. Αλλοι πέντε από τους Code Talkers απεβίωσαν φέτος, γεγονός που οδήγησε το Ιδρυμα των Code Talkers να δημιουργήσει μέχρι το 2012 ένα μουσείο προς τιμήν τους στο Νέο Μεξικό, κοντά στην πρωτεύουσα των Ναβάχο στο Window Rock της Αριζόνα.

ΠΗΓΕΣ

1) WWW.WIKIPEDIA.ORG
2) WWW.GRAFI.GR
3) SIMON SINGH , ΚΩΔΙΚΕΣ ΚΑΙ ΜΥΣΤΙΚΑ,ΕΚΔΟΣΗ
4) www.google.com