ΚΡΥΠΤΟΓΡΑΦΙΑ, ΑΠΟ ΤΟΝ ΚΑΙΣΑΡΑ ΣΤΗΝ ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : ΤΡΙΑΝΤΑΦΥΛΛΙΔΗΣ ΑΝΑΣΤΑΣΙΟΣ

Βαγαίικα πιστόλια
Κων/νος Αγγέλου
Θανάσης κωτσέλης
Ηλίας Αντωνίου
Δημήτρης Μάρκου
Χαράλαμπος Κατρισιώσης

SPICY GIRLS
Νικολετα Κατρισιωση
Βαλια Μελισσαρη
Σοφια Μερκουρη
Σοφια Δουση
Εβελινα Μερκουρη

ΚΧΓΔ

Κατερίνα Βουδούρη
Χρυσούλα Ευθυμίου
Γιώργος Μπαρδώσας
Δημήτρης Ντούκας

milfs desire

δρενιος κων/νος
μερκουρης κων/νος
κολλιας γιωργος
κατρισιωσης γιαννης
μεξης παναγιωτης

Περιεχόμενα

1.ΟΡΙΣΜΟΣ

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

Η σημασία της κρυπτολογίας είναι τεράστια στους τομείς της ασφάλειας υπολογιστικών συστημάτων και των τηλεπικοινωνιών. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς ώστε 2 ή περισσότερα άκρα επικοινωνίας (π.χ. άνθρωποι, προγράμματα υπολογιστών κλπ.) να ανταλλάξουν μηνύματα, χωρίς κανένας τρίτος να είναι ικανός να διαβάζει την περιεχόμενη πληροφορία εκτός από τα δύο κύρια άκρα.

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

2. ΣΤΟΧΟΙ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

1. Εμπιστευτικότητα (Confidentiality).

Εμπιστευτικότητα είναι η ιδιότητα των δεδομένων ή πληροφοριών να είναι προσπελάσιμα μόνο από εξουσιοδοτημένα άτομα. Η εμπιστευτικότητα αναφέρεται στο περιεχόμενο ηλεκτρονικών εγγράφων ή γενικά αρχείων και μηνυμάτων, στην ύπαρξή τους και στην ταυτότητα αυτών που εκτελούν ενέργειες και ανταλλάσσουν μηνύματα. Επίσης, αναφέρεται στο χρόνο και την ποσότητα μηνυμάτων που ανταλλάσσονται. Η εμπιστευτικότητα, μερικές φορές, καλείται και «ιδιωτικότητα» ή «μυστικότητα» ή «προστασία του απορρήτου».

2. Ακεραιότητα (Integrity).
Η ακεραιότητα είναι η υπηρεσία κατά την οποία τα δεδομένα, οι πληροφορίες, οι υπολογιστικοί και επικοινωνιακοί πόροι τροποποιούνται μόνο από εξουσιοδοτημένες οντότητες κατά εξουσιοδοτημένο τρόπο. Η ακεραιότητα έχει να κάνει με την ακρίβεια και τη συνέπεια στη λειτουργία συστημάτων και διεργασιών. Τα δεδομένα σε κάθε σύστημα πρέπει να παραμένουν πλήρη και ορθά. Η ακεραιότητα διατηρείται όταν διατηρούνται και οι εξής ιδιότητες: η ακρίβεια, η μη τροποποίηση ή τροποποίηση από εξουσιοδοτημένους χρήστες ή διεργασίες, με συνέπεια, κατά αποδεκτό τρόπο. Έχουν αναγνωριστεί τρεις καθοριστικές συνιστώσες του όρου ακεραιότητα: οι «εξουσιοδοτημένες ενέργειες», ο «διαχωρισμός και η προστασία αγαθών» και, τέλος, «η ανίχνευση και διόρθωση σφαλμάτων».

3. Επαλήθευση (authentication).
Οι υπηρεσίες αυτές παρέχουν επιβεβαίωση της ταυτότητας και απευθύνονται τόσο στις οντότητες, όσο και στην ίδια την πληροφορία. Όταν δύο μέρη επικοινωνούν θα πρέπει το καθένα από αυτά να επιβεβαιώσει την ταυτότητά του. Οι πληροφορίες οι οποίες διακινούνται από ένα τηλεπικοινωνιακό κανάλι θα πρέπει να πιστοποιούν την προέλευσή τους, την ημερομηνία δημιουργίας τους, το περιεχόμενο τους, την ημερομηνία αποστολής τους κτλ. Για τους παραπάνω λόγους αυτή η υπηρεσία της κρυπτογραφίας χωρίζεται σε δύο τμήματα:

- Το πρώτο περιλαμβάνει την επαλήθευση μιας οντότητας (π.χ. μιας λέξης πρόσβασης password) που επιβεβαιώνει την ταυτότητα ενός απομακρυσμένου μέρους.
- Το δεύτερο πραγματοποιεί την επαλήθευση της προέλευσης των δεδομένων που επαληθεύει την ταυτότητα που ισχυρίζεται ότι έχει ένα τμήμα δεδομένων (π.χ. ένα μήνυμα).

4. Μη αποκήρυξη (non repudiation).
Η υπηρεσία αυτή αποτρέπει μία οντότητα από το να αρνηθεί ότι μία επικοινωνία ή μία συγκεκριμένη πράξη έχει ήδη πραγματοποιηθεί. Όταν μία πράξη αμφισβητείται από μία οντότητα τότε χρειάζεται ένα μέσο προκειμένου να επιλύεται μία διαφωνία, όπου αυτή προκύπτει. Έτσι υπάρχει προστασία έναντι μιας ανακριβούς άρνησης (μη παραδοχής) ενός μέρους ότι μια συναλλαγή πράγματι έχει επισημοποιηθεί.
Ένας από τους βασικός στόχος της κρυπτογραφίας είναι να εξασφαλίσει την καλύτερη δυνατή ικανοποίηση των τεσσάρων προηγούμενων υπηρεσιών ασφαλείας τόσο στην θεωρία όσο και στην πράξη. Αντικειμενικός της σκοπός είναι να ανακαλύψει και να αποτρέψει οποιαδήποτε προσπάθεια εξαπάτησης ή κακόβουλη ενέργεια.

3. ΚΡΥΠΤΟΓΑΦΗΣΗ

Κρυπτογράφηση (*encryption*) ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.

Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται **αποκρυπτογράφηση (*decryption*)**.

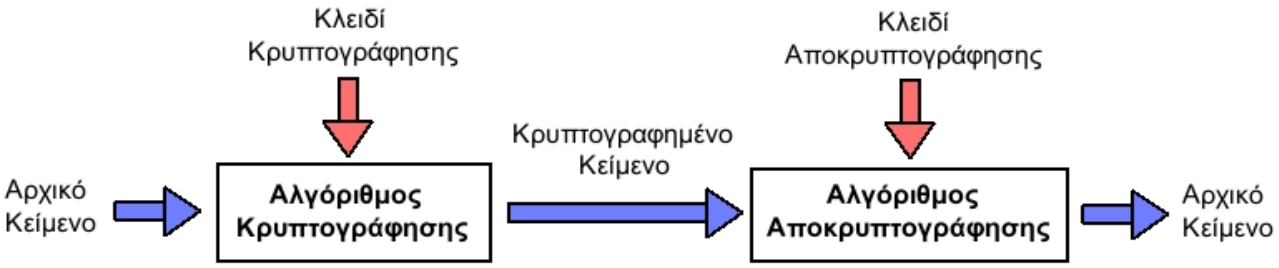
Κρυπτογραφικός αλγόριθμος (cipher) είναι η μέθοδος μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.

Αρχικό κείμενο (*plaintext*) είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.

Κλειδί (*key*) είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.

Κρυπτογραφημένο κείμενο (*ciphertext*) είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.

Κρυπτανάλυση (cryptanalysis) είναι μία επιστήμη που ασχολείται με το "σπάσιμο" κάποιας κρυπτογραφικής τεχνικής ούτως ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.



Εικόνα 1 Διαδικασία Κρυπτογράφησης

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης (cipher) και ενός κλειδιού κρυπτογράφησης (key). Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στη μυστικότητα του κλειδιού κρυπτογράφησης. Το μέγεθος του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bits. Γενικά ισχύει ο εξής κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς. Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

Ο αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει τη δυνατότητα σε δύο πρόσωπα, έστω τον Κώστα και τη Βασιλική, να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο, μη εξουσιοδοτημένο (ένας αντίπαλος), να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων.

Ένα κρυπτοσύστημα (σύνολο διαδικασιών κρυπτογράφησης - αποκρυπτογράφησης) αποτελείται από μία πεντάδα (P,C,k,E,D):

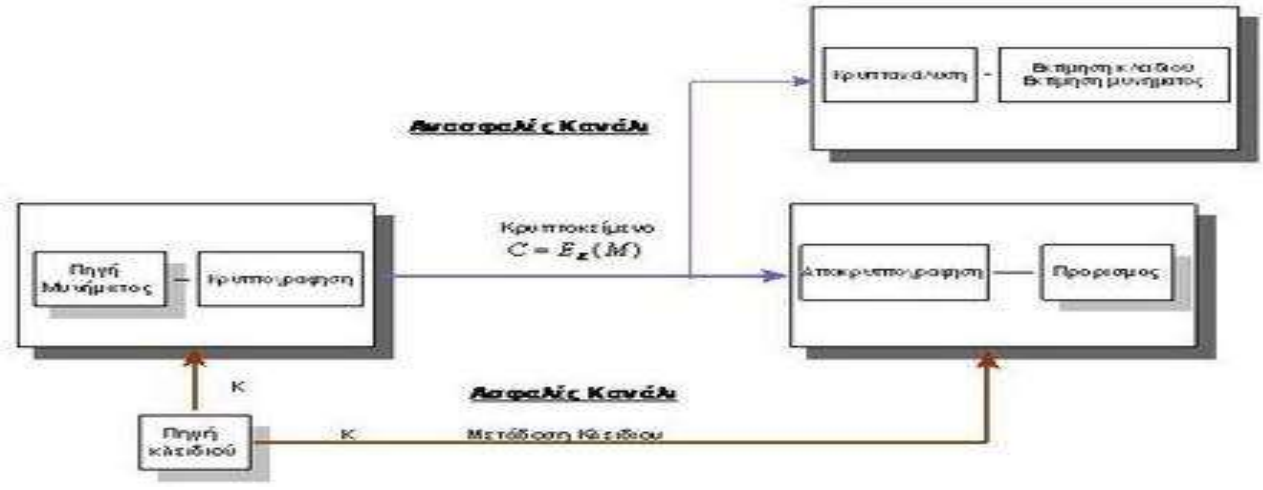
- Το P είναι ο χώρος όλων των δυνατών μηνυμάτων ή αλλιώς ανοικτών κειμένων
- Το C είναι ο χώρος όλων των δυνατών κρυπτογραφημένων μηνυμάτων ή αλλιώς κρυπτοκειμένων
- Το k είναι ο χώρος όλων των δυνατών κλειδιών ή αλλιώς κλειδοχώρος
- Η E είναι ο κρυπτογραφικός μετασχηματισμός ή κρυπτογραφική συνάρτηση
- Η D είναι η αντίστροφη συνάρτηση ή μετασχηματισμός αποκρυπτογράφησης

Η συνάρτηση κρυπτογράφησης E δέχεται δύο παραμέτρους, μέσα από τον χώρο P και τον χώρο k και παράγει μία ακολουθία που ανήκει στον χώρο C. Η συνάρτηση αποκρυπτογράφησης D δέχεται 2 παραμέτρους, τον χώρο C και τον χώρο k και παράγει μια ακολουθία που ανήκει στον χώρο P.

Το Σύστημα του Σχήματος λειτουργεί με τον ακόλουθο τρόπο :

1. Ο αποστολέας επιλέγει ένα κλειδί μήκους *n* από τον χώρο κλειδιών με τυχαίο τρόπο, όπου τα n στοιχεία του K είναι στοιχεία από ένα πεπερασμένο αλφάβητο.
2. Αποστέλλει το κλειδί στον παραλήπτη μέσα από ένα ασφαλές κανάλι.
3. Ο αποστολέας δημιουργεί ένα μήνυμα από τον χώρο μηνυμάτων.
4. Η συνάρτηση κρυπτογράφησης παίρνει τις δυο εισόδους (κλειδί και μήνυμα) και παράγει μια κρυπτοακολουθία συμβόλων (έναν γρίφο) και η ακολουθία αυτή αποστέλλεται διαμέσου ενός μη ασφαλούς καναλιού.
5. Η συνάρτηση αποκρυπτογράφησης παίρνει ως όρισμα τις δύο τιμές (κλειδί και γρίφο) και παράγει την ισοδύναμη ακολουθία μηνύματος.

Ο αντίπαλος παρακολουθεί την επικοινωνία, ενημερώνεται για την κρυπτοακολουθία αλλά δεν έχει γνώση για την κλείδα που χρησιμοποιήθηκε και δεν μπορεί να αναδημιουργήσει το μήνυμα. Αν ο αντίπαλος επιλέξει να παρακολουθεί όλα τα μηνύματα θα προσανατολιστεί στην εξεύρεση του κλειδιού. Αν ο αντίπαλος ενδιαφέρεται μόνο για το υπάρχον μήνυμα θα παράγει μια εκτίμηση για την πληροφορία του μηνύματος.



Εικόνα 2 Σύστημα Σχήματος Κρυπτογράφησης

4. ΑΝΑΓΚΑΙΟΤΗΤΑ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Κατά την διάρκεια των αιώνων έχουν δημιουργηθεί διάφορα πρωτοκόλλα και μηχανισμοί προκειμένου να δώσουν λύση στο πρόβλημα της ασφαλούς διακίνησης της πληροφορίας όταν αυτή μεταφέρεται σε φυσικά έγγραφα. Συχνά οι στόχοι της ασφάλειας δεν μπορούν να επιτευχθούν μόνο μέσω πολύπλοκων μαθηματικών αλγορίθμων και πρωτοκόλλων, αλλά απαιτούν διαδικαστικές τεχνικές και νόμους προκειμένου να προκύψει το επιθυμητό επίπεδο ασφάλειας.

Για παράδειγμα η μυστικότητα των γραμμάτων επιτυγχάνεται με την βοήθεια σφραγισμένων φακέλων και μίας κοινά αποδεκτής ταχυδρομικής υπηρεσίας. Η φυσική ασφάλεια των φακέλων είναι, για πρακτικούς λόγους, περιορισμένη και για αυτό έχουν θεσπιστεί νόμοι οι οποίοι καθορίζουν ως ποινικό αδίκημα το άνοιγμα ενός φακέλου από μη εξουσιοδοτημένα πρόσωπα.

Μερικές φορές η ασφάλεια της πληροφορίας δεν εξασφαλίζεται από τον τρόπο με τον οποίο είναι μετασχηματισμένη αλλά από το φυσικό έγγραφο στο οποίο καταγράφεται. Αυτό αφορά την περίπτωση της στεγανογραφίας όπου ουσιαστικά το ίδιο το μήνυμα αποκρύπτεται. Παλαιότερα για να επιτευχθεί αυτό χρησιμοποιείτο ειδικό μελάνι το οποίο υπό ορισμένες προϋποθέσεις γινόταν αόρατο.

Ο τρόπος με τον οποίο η πληροφορία καταγράφεται δεν έχει αλλάξει δραματικά κατά το πέρασμα του χρόνου. Παρόλο που παλαιότερα η πληροφορία αποθηκευόταν και μεταδιδόταν με την βοήθεια του χαρτιού, ενώ πλέον διανέμεται με οπτικά μέσα και μεταδίδεται μέσω τηλεπικοινωνιακών συστημάτων. Αυτό που έχει αλλάξει σημαντικά είναι η δυνατότητα για αντιγραφή και μεταβολή της πληροφορίας. Ο οποιοσδήποτε έχει την δυνατότητα να δημιουργήσει χιλιάδες πανομοιότυπα αντίτυπα ενός τμήματος πληροφορίας που είναι αποθηκευμένο ηλεκτρονικά, το καθένα από τα οποία να μην ξεχωρίζει από το πρωτότυπο. Με την πληροφορία αποθηκευμένη σε χαρτί αυτό απαιτούσε πολύ περισσότερη προσπάθεια.

Αυτό που χρειάζεται μία κοινωνία όπου η πληροφορία είναι κατά κύριο λόγω αποθηκευμένη και μεταδίδεται σε ηλεκτρονική μορφή είναι ένας τρόπος ο οποίος θα εξασφαλίσει την ασφάλεια της πληροφορίας ανεξάρτητα από το φυσικό μέσο στο οποίο είναι αποθηκευμένη και μεταφέρεται, έτσι ώστε οι στόχοι της ασφάλειας να στηρίζονται μόνο στην ψηφιακή πληροφορία.

Ένα από τα βασικότερα εργαλεία που χρησιμοποιείται για την ασφάλεια της πληροφορίας είναι η υπογραφή. Αποτελεί θεμέλιο στοιχείο για πολλές υπηρεσίες όπως η μη αποκήρυξη μίας ενέργειας, η επαλήθευση της προέλευσης της πληροφορίας και η εξακρίβωση της ακεραιότητα της. Κάθε άτομο μαθαίνει να δημιουργεί την δική του ξεχωριστή υπογραφή η οποία αποτελεί μέρος της ταυτότητάς του. Με την ηλεκτρονικά αποθηκευμένη πληροφορία όμως αυτός ο τρόπος δεν μπορεί να εφαρμοστεί, καθώς η ηλεκτρονική αντιγραφή μίας υπογραφής είναι πάρα πολύ απλή διαδικασία.
Για την επίτευξη της ασφάλειας της πληροφορίας την σημερινή εποχή απαιτούνται πολύ διαφορετικά τεχνικά μέσα και νομικά πλαίσια. Τα τεχνικά αυτά μέσα παρέχονται από την κρυπτογραφία.

5.Η ΕΞΕΛΙΞΗ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

5.1 ΓΕΝΙΚΑ

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. Σκοπός της κρυπτογραφίας είναι να αποκρύψει όχι την καθαυτή ύπαρξη ενός μηνύματος, αλλά τη σημασία του. Το τελευταίο επιτυγχάνεται μέσα από τη διαδικασία της κρυπτογράφησης, δηλαδή της τεχνικής συγκάλυψης ενός μηνύματος, ώστε να διαβαστεί μόνο από τον παραλήπτη του.

Εικόνα 3 Σπαρτιατική Σκυτάλη

Η ανάγκη για μυστικότητα -επομένως και ασφάλεια- οδήγησε τα έθνη στην οργάνωση υπηρεσιών κωδικοποίησης και τα αντίπαλα μέρη στην ανάπτυξη της αποκωδικοποίησης: οι κωδικοπλάστες επινοούν τους κώδικες, ενώ οι κωδικοθραύστες είναι οι «γλωσσικοί αλχημιστές» που επιχειρούν την αποκάλυψη των κωδίκων.

Η ανάπτυξη της αποκρυπτογράφησης γίνεται εμφανής και στην πολύχρονη προσπάθεια αποκάλυψης της Γραμμικής Β και των αιγυπτιακών ιερογλυφικών. Αν και η κρυπτογραφία αφορά τις επικοινωνίες που σχεδιάζονται σκόπιμα και όχι τα κείμενα των αρχαίων πολιτισμών, που δεν είχαν σκοπό να παραμείνουν ανεξιχνίαστα, οι γνώσεις και δεξιότητες που απαιτούνται για την αποκάλυψη του νοήματος των αρχαιολογικών κειμένων, σχετίζονται στενά με την «τέχνη» του σπασίματος των κωδίκων.

Εικόνα 4 Ιερογλυφικά

Για να καταστεί ένα μήνυμα μη κατανοητό, μετασχηματίζεται σύμφωνα με ένα ειδικό πρωτόκολλο, το οποίο έχει συμφωνηθεί μεταξύ του αποστολέα και του παραλήπτη. Ακόμα κι αν ο «εχθρός» κλέψει το κρυπτογραφημένο μήνυμα, δεν μπορεί να το διαβάσει εφόσον δεν γνωρίζει το πρωτόκολλο μετασχηματισμού.

Σχετικά με τα πρωτόκολλα μετασχηματισμού, η κρυπτογραφία χωρίζεται σε δύο κλάδους, τη μετάθεση και την υποκατάσταση:

α) στη μετάθεση τα γράμματα του μηνύματος αλλάζουν θέσεις και έτσι δημιουργείται ένας αναγραμματισμός. Όταν πρόκειται για μια μικρή λέξη, η μέθοδος αυτή δεν είναι τόσο ασφαλής επειδή η εύρεση των πιθανών συνδυασμών είναι σχετικά εύκολη. Όμως, όσο αυξάνει ο αριθμός των γραμμάτων,Κώδικες ο αριθμός των πιθανών συνδυασμών γίνεται αστρονομικός καθιστώντας αδύνατη την εύρεση του πραγματικού μηνύματος, εκτός κι αν είναι γνωστή η μέθοδος αναδιάταξης.

β) στην υποκατάσταση κάθε γράμμα στο αλφάβητο αντικαθίσταται από ένα άλλο. Μία από τις συνιστώμενες τεχνικές είναι να ζευγαρώνονται τυχαία τα γράμματα του αλφαβήτου και στη συνέχεια να αντικαθίσταται κάθε γράμμα του αρχικού μηνύματος με το ταίρι του. Π.χ. στο ελληνικό αλφάβητο: Α με Ω, Δ με Χ, Η με Β, κ.ο.κ. Έτσι αντί για «συνάντηση τα μεσάνυχτα», ο αποστολέας μπορεί να γράψει ΕΠΡΩΡΖΕΒ ΖΩ ΨΣΕΩΡΠΔΖΩ.

Συνοπτικά, στη μετάθεση κάθε γράμμα διατηρεί την ταυτότητά του αλλά αλλάζει θέση, ενώ στην υποκατάσταση κάθε γράμμα αλλάζει ταυτότητα, αλλά διατηρεί τη θέση του.

Κάποιες από τις αρχαιότερες καταγραφές μυστικής γραφής ανάγονται στον Ηρόδοτο. Σύμφωνα με τον Ηρόδοτο, ήταν η τέχνη της μυστικής γραφής που έσωσε την Ελλάδα από τον Ξέρξη.

Κατά το χτίσιμο της Περσέπολης, ο Ξέρξης λάμβανε δώρα από όλη την αυτοκρατορία του και τα γειτονικά κράτη εκτός από την Αθήνα και τη Σπάρτη. Αποφασισμένος να πάρει εκδίκηση γι' αυτό, ξεκινά τη συγκέντρωση στρατιωτικών δυνάμεων και έτσι, πέντε χρόνια μετά, καθίσταται έτοιμος για αιφνιδιαστική επίθεση κατά των ελληνικών πόλεων. Εν τω μεταξύ, η συγκρότηση αυτής της πολεμικής δύναμης γίνεται αντιληπτή από το Δημάρατο, Έλληνα εξόριστο και κάτοικο στα Σούσα της Περσίας. Αν και εξόριστος, ο Δημάρατος αποφασίζει να στείλει μήνυμα ώστε να προειδοποιήσει τους Σπαρτιάτες για το σχέδιο επίθεσης. Το ζήτημα ήταν πώς να σταλεί το μήνυμα, ώστε να μην υποκλαπεί από τους Πέρσες. Αναφέρει σχετικά ο Ηρόδοτος: …υπήρχε ένας μόνο τρόπος: να ξύσει το κερί από δύο πτυσσόμενες πινακίδες, να γράψει στο ξύλο που υπήρχε από κάτω και μετά να επικαλύψει το μήνυμα με κερί. Έτσι οι πινακίδες, φαινομενικά κενές, δεν θα προκαλούσαν την περιέργεια των φρουρών καθ' οδόν. Όταν το μήνυμα έφτασε στη Σπάρτη κανείς δεν κατάλαβε εκτός της Γοργούς, κόρης του Κλεομένη και συζύγου του Λεωνίδα, η οποία και είπε στους άλλους ότι αν έξυναν το κερί θα έβρισκαν κάτι γραμμένο στο ξύλο από κάτω. Οπότε, το μήνυμα αποκαλύφθηκε και στη συνέχεια μεταδόθηκε στους υπόλοιπους Έλληνες. Αυτή η μορφή μυστικής επικοινωνίας ανήκει στη μέθοδο της στεγανογραφίας.

Στην αρχαία Ελλάδα, πλέον της στεγανογραφίας, αναπτύχθηκε ιδιαίτερα η μέθοδος της κρυπτογραφίας και συγκεκριμένα της μετάθεσης (που εξηγήθηκε παραπάνω).

Μια μορφή μετάθεσης εφαρμόστηκε στην πρώτη στην Ιστορία κρυπτογραφική συσκευή, τη σπαρτιατική σκυτάλη, που ανάγεται στον 5ο αιώνα π.Χ. Η σκυτάλη είναι ένα ξύλινο ραβδί γύρω από το οποίο τυλίγεται μια λωρίδα από δέρμα ή περγαμηνή. Ο αποστολέας γράφει το μήνυμα κατά μήκος της σκυτάλης και μετά ξετυλίγει τη λωρίδα. Τώρα η λωρίδα φαίνεται να

περιέχει μια σειρά γράμματα χωρίς νόημα. Το μήνυμα έχει αναδιαταχτεί. Ο αγγελιαφόρος παίρνει τη δερμάτινη λωρίδα και ενίοτε, σαν επιπρόσθετο στεγανογραφικό μέτρο, τη φοράει σαν ζώνη, με τα γράμματα κρυμμένα στη μέσα μεριά. Για να ανασύρει το μήνυμα ο παραλήπτης, απλώς τυλίγει τη δερμάτινη λωρίδα γύρω από μια σκυτάλη ίδιας διαμέτρου με αυτήν που χρησιμοποίησε ο αποστολέας. Το 404 π.Χ., ένας αγγελιαφόρος καταματωμένος -ο ένας από τους πέντε επιζήσαντες ενός εξοντωτικού ταξιδιού στην Περσία- παρουσιάζεται στο Σπαρτιάτη Λύσανδρο. Ο αγγελιαφόρος παραδίδει τη ζώνη του στο Λύσανδρο, που την τυλίγει γύρω από τη σκυτάλη του και έτσι μαθαίνει πως ο σατράπης Φαρνάβαζος σχεδιάζει να του επιτεθεί. Χάρη στη σκυτάλη, ο Λύσανδρος πρόλαβε να προετοιμαστεί για την επίθεση την οποία και εντέλει απέκρουσε.

Ο Βαλέριος Πρόβος έγραψε μια ολόκληρη πραγματεία για τα κρυπτογράμματα του Καίσαρα (δυστυχώς, η πραγματεία αυτή δεν διασώθηκε). Κρυπτόγραμμα λέγεται οποιαδήποτε μορφή κρυπτογραφικής υποκατάστασης, στην οποία κάθε γράμμα αντικαθίσταται με ένα άλλο γράμμα ή σύμβολο.

Η πρώτη τεκμηριωμένη χρήση μεθόδου υποκατάστασης, για στρατιωτικούς σκοπούς, εμφανίζεται στους γαλατικούς πολέμους του Ιουλίου Καίσαρα. Ο ΚώδικεςΚαίσαρ περιγράφει πώς έστειλε ένα μήνυμα στον Κικέρωνα, που ήταν πολιορκημένος και στα πρόθυρα παράδοσης. Με βάση τη μέθοδο της υποκατάστασης, αντικατέστησε τα λατινικά γράμματα με ελληνικά, καθιστώντας το μήνυμα ακατανόητο στον εχθρό. Πολύ χαρακτηριστικά περιγράφεται: Ο αγγελιαφόρος είχε λάβει εντολή, αν δεν μπορούσε να πλησιάσει, να ρίξει μέσα στο στρατόπεδο μια λόγχη με το γράμμα δεμένο στον ιμάντα…έτυχε όμως η λόγχη να καρφωθεί και να σφηνώσει στον πύργο και επί δύο ημέρες οι στρατιώτες μας δεν την έβλεπαν. Την τρίτη ημέρα την είδε ένας στρατιώτης, την κατέβασε και την παρέδωσε στον Κικέρωνα. Εκείνος διάβασε το μήνυμα και μετά το ανέγνωσε δυνατά σε μια παρέλαση των στρατευμάτων, προς μεγάλη χαρά όλων.

Στους Βίους των δώδεκα καισάρων του Σουητώνιου, (2ος αιώνας μ.Χ.), περιγράφεται λεπτομερώς ένας από τους τύπους κρυπτογραφικής υποκατάστασης που χρησιμοποιούσε ο Ιούλιος Καίσαρας. Σύμφωνα με τον τύπο αυτό, αντικαθιστούσε κάθε γράμμα του μηνύματος με το κατά τρεις θέσεις επόμενό του στο αλφάβητο. Αυτός ο τύπος υποκατάστασης αποκαλείται μεταθετικό κρυπτόγραμμα του Καίσαρα ή απλώς κρυπτόγραμμα του Καίσαρα. Αν και ο Σουητώνιος αναφέρει μόνο έναν τύπο μετάθεσης κατά τρεις θέσεις, αν χρησιμοποιηθεί οποιαδήποτε μετάθεση μεταξύ 1 και 23 θέσεων, μπορούν να δημιουργηθούν 23 ξεχωριστά κρυπτογράμματα.

Οι κρυπτογράφοι χρησιμοποιούν τον όρο κανονικό αλφάβητο για αυτό στο οποίο γράφεται το αρχικό μήνυμα και κρυπτογραφικό αλφάβητο για αυτό το οποίο αποτελείται από τα γράμματα τα οποία αντικαθιστούν τα κανονικά.

Η κρυπτογραφία δεν είναι διανοητικό άθλημα, αλλά μια αναγκαιότητα που διασφαλίζει - και επιδιώκεται να συνεχίζει να διασφαλίζει- την ιδιωτική ζωή του ατόμου, των κυβερνήσεων και των δραστηριοτήτων κάθε είδους. Η κρυπτογραφία έχει πλέον, χάρη στις αλματώδεις μαθηματικές και τεχνολογικές εξελίξεις, μια καθημερινή, παγκόσμια «παρουσία».

Καθώς η πληροφορία αποτελεί πλέον πολυτιμότατο αγαθό, υπηρεσία και τομέα τεχνολογίας, με αδιαμφισβήτητα υψηλότατη συμβολή στην εξέλιξη του κόσμου μας, είναι προφανές ότι η «μάχη» ανάμεσα σε κωδικοπλάστες και κωδικοθραύστες θα συνεχίζεται αέναα…

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

Η 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 μετάθεσης. Όπως αναφέρει ο Πλούταρχος, η «Σπαρτιατική Σκυτάλη», 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 αναδιάταξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης.

Στην αρχαιότητα χρησιμοποιήθηκαν κυρίως συστήματα, τα οποία βασίζονταν στη στεγανογραφία 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 oValerius 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. OΙταλός 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 ΓάλλοςVigenere, 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 του Ναπολέοντα 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, που ανακαλύφθηκε το 1908 στη νότια Κρήτη και σε άλλα αντικείμενα όπως σφραγίδες και πέλεκεις. Ο δίσκος της Φαιστού είναι 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.

Εικόνα 5 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 το 1900. 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 στο Μουσείο 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 την Τίρυνθα. Σήμερα αποτε-

λούν 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 είδοςελληνικής 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».

5.2 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 6).

Εικόνα 6 Η μηχανή ENIGMA

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 στο Μπλέτσλεϊ Παρκ (Bletchley Park), κέντρο της Βρετανικής Υπηρεσίας α-πό/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 το 1940) 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 ΣτόλουΙζορόκου 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 Μ-209 και τη λιγότερη ασφαλή οικογένεια κρυπτομηχανών Μ-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.

5.2.1 ΚΩΔΙΚΑΣ ΝΑΒΑΧΟ

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.

Εικόνα 7 Οι codetalkers

5.2.2 ΜΗΧΑΝΗ ΑΙΝΙΓΜΑ – ΑΛΑΝ ΤΟΥΡΙΝΓΚ

Ο Άλαν Μάθισον Τούρινγκ (Alan Matheson Turing, 23 Ιουνίου, 1912 - 7 Ιουνίου, 1954) ήταν Βρετανός μαθηματικός, καθηγητής της λογικής και κρυπτογράφος. Θεωρείται «πατέρας της επιστήμης υπολογιστών», χάρη στην πολύ μεγάλη συνεισφορά του στο γνωστικό πεδίο της θεωρίας υπολογισμού κατά τη δεκαετία του 1930, αλλά και της τεχνητής νοημοσύνης, χάρη στη λεγόμενη δοκιμή Τούρινγκ την οποία πρότεινε το 1950: έναν τρόπο να διαπιστωθεί πειραματικά αν μία μηχανή έχει αυθεντικές γνωστικές ικανότητες και μπορεί να σκεφτεί.

Το έργο του από τη δεκαετία του '30 προσέδωσε στην ως τότε άτυπη έννοια του αλγορίθμου μία επίσημη, αυστηρή μαθηματική διατύπωση μέσω της λεγόμενης Μηχανής Τούρινγκ. Ακόμα, ο Τούρινγκ διατύπωσε από κοινού με τον Αλόνζο Τσερτς την περίφημη εικασία του, ευρέως αποδεκτή, σύμφωνα με την οποία οποιοδήποτε μαθηματικό μοντέλο υπολογισμού είναι είτε ισοδύναμο είτε υποδεέστερο της Καθολικής Μηχανής Τούρινγκ, επομένως αυτή περιγράφει τον ευρύτερο δυνατό υπολογιστή γενικού σκοπού: είναι θεωρητικά ικανή να υπολογίσει ό,τι είναι δυνατό να υπολογιστεί αλγοριθμικά.

Οι επιστημονικές συνεισφορές του Τούρινγκ κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου δεν αναγνωρίστηκαν ποτέ δημόσια κατά τη διάρκεια της ζωής του επειδή η εργασία του ήταν απόρρητη. Στο Μπλέτσλεϊ Παρκ (Bletchley Park), κέντρο της Βρετανικής Υπηρεσίας Αντικατασκοπείας, ήταν το κεντρικό πρόσωπο στην αποκρυπτογράφηση των γερμανικών στρατιωτικών κωδικών, όντας ο προϊστάμενος της Ομάδας 8. Η ομάδα αυτή ήταν που επιφορτίστηκε με την αποκωδικοποίηση τηςγερμανικής κρυπτογραφικής συσκευής Enigma.

Μετά τον Πόλεμο, σχεδίασε έναν από τους πρώτους ηλεκτρονικούς προγραμματίσιμους ψηφιακούς υπολογιστές στο Εθνικό Φυσικό Εργαστήριο, όπως λεγόταν, και κατασκεύασε μια δεύτερη υπολογιστική μηχανή στο Πανεπιστήμιο του Μάντσεστερ. Ο Τούρινγκ αυτοκτόνησε το 1954. Το Βραβείο Τούρινγκ, η ύψιστη επιστημονική διάκριση στον χώρο της πληροφορικής από το 1966 κι έπειτα, ονομάστηκε έτσι προς τιμήν του.

Κατά τη διάρκεια του 2ου παγκόσμιου πολέμου ήταν σημαντικός συμμετέχων στις προσπάθειες στο Μπλέτσλεϊ Παρκ να αποκρυπτογραφήσουν τα γερμανικά μηνύματα. Η εργασία του Τούρινγκ κρατήθηκε μυστική μέχρι τη δεκαετία του '70, ακόμη και οι στενοί φίλοι του δεν την ήξεραν. Συνέβαλε με διάφορες μαθηματικές ιδέες για την αποκρυπτογράφηση μηνυμάτων των συσκευών Enigma και Lorenz SZ 40/42. Στο Μπλέτσλεϊ Παρκ ο Τούρινγκ εργάστηκε από το 1939 ως το 1940 όταν και μετακινήθηκε προς την Ομάδα 8. Ο Τούρινγκ συνειδητοποίησε ότι δεν ήταν απαραίτητο να εξεταστούν όλοι οι πιθανοί συνδυασμοί για να σπάσουν τους κωδικούς της μηχανής Enigma. Απέδειξε ότι ήταν δυνατό να εξετάσει τις σωστές τοποθετήσεις των διακοπτών (περίπου ένα εκατομμύριο συνδυασμοί) χωρίς να πρέπει να εξεταστούν οι τοποθετήσεις του πίνακα συνδέσεων (περίπου 157 εκατομμύριο συνδυασμοί). Ενώ ακόμα ένας τρομερός στόχος, ένα εκατομμύριο συνδυασμοί ήταν επιτεύξιμοι χρησιμοποιώντας μια ηλεκτρομηχανική μηχανή - τη βόμβα, ονομασμένη από τη σχεδιασμένη από τους Πολωνούς bomba. Για ένα χρόνο, ο Τούρινγκ ήταν επικεφαλής του "καταλύμα-

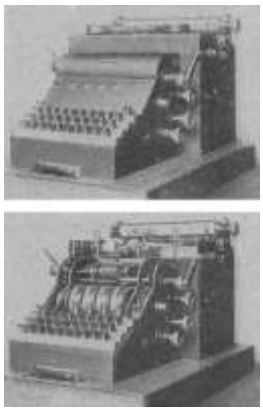
τος 8", τμήματος αρμόδιου για τα γερμανικά ναυτικά σήματα. Ο Τούρινγκ εφηύρε επίσης την τεχνική Banburismusγια να βοηθήσει στο σπάσιμο της Γερμανική κρυπτογραφικής συσκευής Enigma. Για να βοηθήσει, ο πρώτος ψηφιακός προγραμματίσιμος ηλεκτρονικός υπολογιστής αναπτύχθηκε, ο Colossus Mark I. Ο Τούρινγκ, εντούτοις, δεν συμμετείχε άμεσα - ο Colossus σχεδιάστηκε και κατασκευάστηκε στον ερευνητικό σταθμό ταχυδρομείων στο Hill Dollis από μια ομάδα με επικεφαλής τον Τόμας Φλάουερς (Thomas Flowers) το 1943.

Στο τελευταίο μέρος του πολέμου, ο Τούρινγκ ανέλαβε (με τον μηχανικό Ντόναλντ Μπέιλι (Donald Bayley)) το σχέδιο μιας φορητής μηχανής με κωδικό Delilah για να επιτρέψει τις ασφαλείς μεταδόσεις φωνής. Προορισμένος για τις διαφορετικές εφαρμογές, Το Delilah στερήθηκε τη δυνατότητα που χρησιμοποιείται πέρα από τις μεγάλης απόστασης ραδιομεταδόσεις. Το Delilah ολοκληρώθηκε πάρα πολύ αργά για να χρησιμοποιηθεί στον πόλεμο. Ενώ ο Τούρινγκ το κατέδειξε στους ανώτερους υπαλλήλους με την κωδικοποίηση/αποκωδικοποίηση μιας καταγραφής μιας ομιλίας του Ουίνστων Τσώρτσιλ, δεν υιοθετήθηκε για τη χρήση.

Η πρώτη μηχανή Enigma δημιουργήθηκε από τον γερμανό Ηλεκτρολόγο Μηχανικό Arthur Scherbius (20 Οκτωβρίου 1878 – 13 Μαϊου 1929), με σκοπό την προστασία των εταιρικών μυστικών μεγάλων επιχειρήσεων της εποχής, κυρίως τραπεζών. Η μηχανή ονομάστηκε Enigma από την ελληνική λέξη «αίνιγμα». (Ευρεσιτεχνία US1657411 A)

Αργότερα, το 1926 μία τροποποιημένη έκδοση της απλής Enigma χρησιμοποιήθηκε από τον γερμανικό στρατό, και λίγα χρόνια αργότερα, μία άλλη τροποποιημένη έκδοση της Enigma (με ακόμα περισσότερους πιθανούς συνδυασμούς.

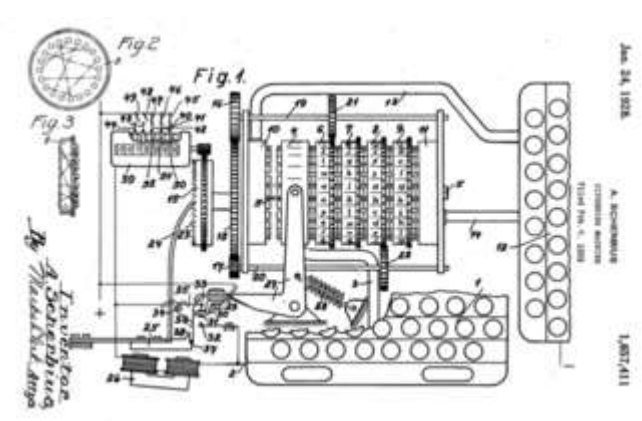
Ο τρόπος λειτουργίας της Enigma



Εικόνα 8 Enigma A, Η πρώτη μηχανή Enigma

Η βασική αρχή λειτουργίας της Enigma ήταν απλή: Πιέζοντας ένα πλήκτρο από το πληκτρολόγιο της μηχανής (το οποίο περιελάμβανε 26 γράμματα του λατινικού αλφαβήτου), το ηλεκτρικό σήμα που ξεκινούσε από αυτό το πλήκτρο, περνούσε μέσα από τους 3 ρότορες

(και στην τροποποιημένη στρατιωτική έκδοση που χρησιμοποιήθηκε από την Ναζιστική Γερμανία πρώτα από το Plugboard = Πίνακας ηλεκτρικών υποδοχών), κατέληγε σε ένα λαμπτήρα, ο οποίος υποδείκνυε ένα «τυχαίο» γράμμα στον πίνακα λυχνιών, ακριβώς από πάνω από το πληκτρολόγιο, το οποίο θα αναμεταδίδοταν μέσω ασυρμάτου σε κώδικα Mors, ένα κρυπτογραφημένο μήνυμα (δηλαδή ο χειριστής της Enigma θα πληκτρολογούσε το μήνυμα που ήθελε να μεταδώσει στην Enigma, και θα σημείωνε κατά σειρά ποιο γράμμα άναβε στον πίνακα με τους λαμπτήρες, και αντίστροφα για να το αποδικοποιήσει). Αυτό βέβαια προϋποθέτει και οι δύο χειριστές να έχουν τις μηχανές τους ρυθμισμένες κατά τον ίδιο τρόπο (ίδια θέση ρότορα, και στην στρατιωτική έκδοση, ίδια συνδεσμολογία στον πίνακα ηλεκτρικών υποδοχών (Plugboard)).



Εικόνα 9 Σχέδιο της εμπορικής Enigma

Για παράδειγμα, έστω ότι πατάμε το γράμμα «Ε«. Το ηλεκτρικό σήμα θα περάσει από τον διακόπτη του γράμματος «Ε», θα περάσει από τους 3, θα ξαναπεράσει από τους ρότορες, και τελικά, ανάλογα με τις ρυθμίσεις τις μηχανής θα καταλήξει στο γράμμα π.χ. «Η«.

Το δυνατό χαρακτηριστικό, και παράλληλα αδυναμία της Enigma ήταν ότι αν πατούσαμε π.χ. το «Α», όσες φορές και να το πατούσαμε στον πίνακα με τους λαμπτήρες δεν θα έβγαινε ποτέ το Α, ανεξαρτήτως ρύθμισης.

Η αρχική έκδοση της Enigma (αυτή που ήταν διαθέσιμη στο εμπόριο) χρησιμοποιούσε 3 ρότορες, οι οποίοι μπορούσαν να ρυθμιστούν με 26 διαφορετικούς τρόπους ο καθένας, δηλαδή, αν υπολογίσουμε τις πιθανότητες (26x26x26), έχουμε 17576 πιθανούς συνδυασμούς.

Για να ρυθμίζουν σωστά τις μηχανές τους οι στρατιώτες, μοιράζονταν ανά μήνα οι ρυθμίσεις που θα χρησιμοποιούσαν για κάθε μέρα εκείνου του μήνα (και αυτό ήταν ουσιαστικά το «κλειδί» για να αποκρυπτογραφήσει τα μηνύματα).

Η τροποποίηση της Enigma από την Ναζιστική Γερμανία

Θεωρώντας ότι οι 17576 συνδυασμοί ήταν λίγοι, ο γερμανικός στρατός πρόσθεσε έναν πίνακα ηλεκτρικών υποδοχών (αγγλ: Plugboard), και αργότερα ένα σετ με 5 ρότορες από τους οποίους θα έπρεπε να μπουν οι 3 στην μηχανή, ή ακόμα σε κάποιες μηχανές μέχρι και 4 ρότορες την φορά.

Δηλαδή, εάν υπολογίσουμε τους πιθανούς συνδυασμούς για μία μηχανή που χρησιμοποιούσε 3 ρότορες από ένα σετ των 5 ρότορων, η οποία χρησιμοποιούσε και τον πίνακα τον ηλεκτρικών υποδοχών (plugboard), έχουμε:

Εικόνα 10 Η συνδεσμολογία του εσωτερικού του ρότορα

Για την επιλογή 3 από τους 5 ρότορες:

5 x 4 x 3 = 60 πιθανοί συνδυασμοί

Για την ρύθμιση των ρότορων:

(Σημείωση: Οι ρότορες έπρεπε να ρυθμιστούν με αριθμούς από το 1 εώς το 26, και όταν ο 1ος ρότορας έκανε μία πλήρης περιστροφή, παρέσυρε τον 2ο να γυρίσει, και μόλις και ο 2ος ολοκληρώσει μία πλήρης περιστροφή παρασύρει και τον τρίτο κ.ο.κ.)

Με 3 ρότορες έχουμε:

26 x 26 x 26, δηλαδή 26 στον κύβο, δηλαδή = 17576 συνδυασμούς

Για την ρύθμιση του πίνακα ηλεκτρικών υποδοχών (Plugboard):

(Σημείωση: Αυτός ο πίνακας ήταν ουσιαστικά 26 υποδοχές, και η κάθε μία από αυτές ήταν «ονομασμένη» με ένα από τα 26 γράμματα του λατινικού αλφαβήτου (26 γράμματα για 26 υποδοχές). Επίσης, με κάθε Enigma που έφερε την τροποποίηση αυτή, είχε και 10 καλώδια τα οποία σύνδεε το καθένα 2 υποδοχές μεταξύ τους, π.χ. το «A» με το «J», δηλαδή περίσσευαν 6 γράμματα (20 γράμματα/26)).

Άρα:

26! (26 παραγοντικό δλδ 26x25x24…x1) / 6! x 10! x 210 = 150.738.274.937.250 πιθανοί τρόποι σύνδεσης, δηλαδή στο σύνολο έχουμε:

158.962.555.217.826.360.000 ή

158 εξακισεκατομύρια 962 πεντακισεκατομύρια 555 τετρακισεκατομύρια 217 τρισεκατομύρια 826 εκατομύρια 360 χιλιάδες!

Τρόπος λειτουργίας της τροποποιημένης Enigma

Ο τρόπος κρυπτογράφησης/αποκρυπτογράφησης της τροποποιημένης Enigma σε σχέση με την εμπορική, διέφερε στο ότι αντί το ηλεκτρικό σήμα από τον διακόπτη πηγαίνει και περνάει από τους ρότορες, και ξαναπερνάει από τους ρότορες και καταλήγει τελικά στον λαμπτήρα που υποδικνύει ποιο γράμμα να γραφτεί στο κωδικοποιημένο μήνυμα (στην παραπάνω φωτογραφία), περνάει πρώτα από τον πίνακα υποδοχών, και μετά από τους ρότορες όπως η πιο απλή Enigma. Δηλαδή:

Η αποκρυπτογράφηση της Enigma

Η αποκρυπτογράφηση της Enigma δεν βασίστηκε τόσο στις αδυναμίες τις μηχανής όσο στην ανθρώπινη αδυναμία. Ο Γερμανός απόστρατος Χανς-Θίλο Σμιντ μετά από μια ανεπιτυχή καριέρα στις τάξεις του γερμανικού στρατού έκανε διάφορες εργασίες στο Βερολίνο όπου και διέμενε.

Αυτή που τελικά του εξασφάλισε τα προς το ζην ήταν η πώληση μυστικών πληροφοριών σχετικών με την Enigma σε ξένες δυνάμεις, μέσω της απασχόλησής του στο γραφείο Chiffrierstelle, το οποίο είχε την ευθύνη της διαχείρισης των κρυπτογραφημένων επικοινωνιών της Γερμανίας και του είχε προσφέρει εργασία σε μια περίοδο της ζωής του στιγματισμένη από άκαρπες επιχειρηματικές προσπάθειες σχετικές με τις σπουδές του στη χημεία.

Ο αδελφός του, Rudolf, ο οποίος είχε καλύτερη τύχη παραμένοντας στην υπηρεσία του στρατού μετά τον πόλεμο, ήταν αυτός που τον πρότεινε στο Γραφείο Κρυπτογραφίας του

Υπουργείου Αμύνης, εξασφαλίζοντάς του έμμεσα και την ελευθερία κινήσεων ενός έμπιστου υπαλλήλου.

Ο δρόμος για την επίλυση του αινίγματος είχε ανοίξει με τον Σμιντ να βλέπει ότι ο μόνος τρόπος για να κερδίσει χρήματα, ήταν να πουλήσει ότι μπορούσε να έχει στα χέρια του, μιας και βασικά πνευματικά αγαθά, έλαμπαν δια της απουσίας τους από την ιδιοσυγκρασία του και ασφαλώς δεν μπορούσαν να του αποφέρουν χρήματα, τουλάχιστον άμεσα.

Τελικά, την 1η Απριλίου 1943 η Γκεστάπο εισέβαλε στο διαμέρισμα του, τον συνέλαβε και τον φυλάκισε. Έμεινε για λίγο καιρό απομονωμένος στην φυλακή μέχρι να επιτραπεί στην κόρη του Γκιζέλα, να τον επισκεφθεί.

Μετά τις πολλαπλές τροποποιήσεις μετά την τελευταία προδοσία του Σμιντ, πίστευαν ότι το μυστικό της Enigma θα ήταν ασφαλές. Όμως ήταν ήδη πολύ αργά. Η απληστία του Χανς-Θίλο, ο άσωτος τρόπος ζωής του, το πάθος του για τις γυναίκες και οι πολιτικές διαφορές του με την διακυβέρνηση της χώρας, τον είχαν οδηγήσει να παραδώσει στους Πολωνούς και στους Γάλλους ικανό όγκο πληροφοριών, προκειμένου να ανατρέψουν το ναζιστικό καθεστώς πολύ νωρίτερα από ότι περίμεναν.

Η συμβολή της Πολωνίας στην Αποκρυπτογράφηση της Enigma

Η Πολωνία, φοβούμενη μία γερμανική εισβολή ήδη από τις αρχές του 1930, είχε θέσει ως ζωτικής σημασίας στόχο την αποκρυπτογράφηση των κωδικοποιημένων μηνυμάτων των Γερμανών. Έτσι, το 1931 δημιουργείται ένα ειδικό τμήμα κρυπτανάλυσης στις Πολωνικές μυστικές υπηρεσίες το Biuro Szyfrów (Cipher Bureau = Γραφείο Αποκρυπτογράφησης/Κρυπτανάλυσης).

Περίπου στα τέλη το 1927 ή στις αρχές του 1928, φτάνει στο τελωνείο της Βαρσοβίας ένα κουτί, το οποίο έγραφε απ'έξω «Εξοπλισμός Ραδιοτηλεπικοινωνιών». Το παραπάνω δέμα είχε σταλεί κατα λάθος στην Βαρσοβία, και οι Γερμανοί απέτησαν την άμεση επιστροφή του.
Τότε, το πακέτο προωθήθηκε στο νεοσύστατο Γραφείο Αποκρυπτογράφησης/Κρυπτανάλυσης, όπου και άνοιξαν προσεκτικά το πακέτο. Ήταν μία μηχανή Enigma η οποία ήταν διαθέσιμη στο εμπόριο (δεν είχαν γίνει ακόμα οι μετατροπές από τον γερμανικό στρατο).

Στις 15 Ιουλίου 1928 (πριν την δημιουργία του Biuro Szyfrow), άρχισαν οι εκπομπές κωδικοποιημένων γερμανικών μηνυμάτων, που αν και έγιναν αρχικά προσπάθειες αποκρυπτογράφησης, μάταια βέβαια, τελικά σταμάτησαν προσωρινά.

Τελικά, ο Rejewski άρχισε να δουλεύει πάνω στην αποκρυπτογράφηση της Enigma. Με τις πολύτιμες πληροφορίες που μεταβίβασε ο προδότης Σμιντ, ο Rejewski κατάφερε να αποκρυπτογραφήσει την Enigma χρησιμοποιώντας θεωρητικά μαθηματικά. Σε συνεργασία με τον Antoni Palluth, συνιδρυτή της πολωνικής εταιρίας τηλεπικοινωνιών AVA, κατασκεύασε ένα αντίγραφο της μηχανής Enigma. Ο Marian Rejewski, σε συνεργασία με τους μαθηματικούς που επίσης δούλευαν στο Biuro Szyfrow, Jerzy Rozycki και Henryk Zygalski, δημιούργησαν την μηχανή Bombe (πολ: Bomby), η οποία δοκίμαζε όλες τις θέσεις των ρότορων της Enigma, μέχρι να βρει την σωστή ρύθμιση. Σε συνδυασμό με τα Zygalski Sheets (ελλ: Φύλλα του Zygalski), η Πολωνοί, για ένα χρονικό διάστημα, ήταν ικανοί να αποκρυπτογραφούν και να συλλέγουν πολύτιμες πληροφορίες που μετέδιδαν οι Γερμανοί μέσω ασυρμάτου.

Η τροποποίηση της Enigma, και η συνάντηση με τους Συμμάχους

Αν και οι τροποποιήσεις στην Enigma την περίοδο 1932-1937 δεν ήταν λίγες, οι 3 μαθηματικοί κατάφεραν να ξεπεράσουν τις δυσκολίες και συνέχισαν έτσι να προμηθεύουν τις Πολωνικές μυστικές υπηρεσίες με πολύτιμες πληροφορίες. Ωστόσο, στις 15 Δεκεμβρίου 1938, ο γερμανικός στρατός εισάγει ένα σετ με 5 ρότορες, από τους οποίους θα χρησιμοποιούνταν 3 απο αυτούς. Αυτό αύξανε την πολυπλοκότητα της μηχανής και τον αριθμό των πιθανών συνδυασμών, σε συνδυασμό με την έλλειψη κεφαλαίων, να σταματήσει η αποκρυπτογράφηση των γερμανικών μηνυμάτων. Τελικά, στις 25 με 26 Ιουλίου 1939, συναντήθηκαν στο Πέρε (πολ: Pyry), λίγα χιλιόμετρα έξω από την Βαρσοβία οι 3 μαθηματικοί και αξιωματούχοι των Πολωνικών Μυστικών Υπηρεσιών με Άγγλους και Γάλλους αντιπροσώπους των αντίστοιχων μυστικών υπηρεσιών. Οι Πολωνοί παρέδωσαν ένα αντίγραφο της Enigma στον κάθενα τους, και όλες τις γνώσεις τους για την Enigma και τους εξήγησαν τον τρόπο που την έσπασαν.
Οι αξιωματούχοι είχαν μείνει έκπληκτοι από το έργο των Πολωνών, αφού οι προσπάθειες για το σπάσιμο της Enigma από την πλευρά τους είχε είτε παρατηθεί, είτε δεν είχε αποδώσει καρπούς.
Οι άνθρωποι αυτοί, ακόμα και κατά την περίοδο της φυλακισής τους από τους Ναζί, δεν αποκάλυψαν το μυστικό, ότι η Enigma είχε πλέον σπάσει, πράγμα που αν το μάθαιναν, θα ήταν καταστροφικό για τις Συμμαχικές Δυνάμεις, και θα άλλαζε την πορεία της ιστορίας.

5.3 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 1949 δημοσίευσε 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.

6. ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΔΙΑΔΙΚΤΥΟ

Η κρυπτογράφηση στο διαδίκτυο χρησιμοποιείτε για την ασφαλή μετακίνηση δεδομένων και εγγράφων μεταξύ υπολογιστών από όλες τις άκρες του κόσμου. Διαδεδομένη χρήση του Διαδικτύου σε εφαρμογές που περιλαμβάνουν επικοινωνία ευαίσθητων δεδομένων:

- τραπεζικές συναλλαγές
- ηλεκτρονικό εμπόριο
- ιατρική πληροφορία

6.1 Είδη Επιθέσεων στο Διαδίκτυο

- Υποκλοπή (Eavesdropping)
- Η μεταφερόμενη πληροφορία παραμένει ακέραιη, όχι όμως η εμπιστευτικότητα της Παραποίηση (Tampering)
- Η πληροφορία που μεταφέρεται μπορεί να αλλαχθεί ή να αντικατασταθεί από κάποιον τρίτο Πλαστοπροσωπία (impersonation)
- Η πληροφορία μεταφέρεται σε μη εξουσιοδοτημένο υπολογιστή που παριστάνει το νόμιμο παραλήπτη
- Προσποίηση (spoofing)

6.2 Κρυπτογράφηση Δημόσιου Κλειδιού

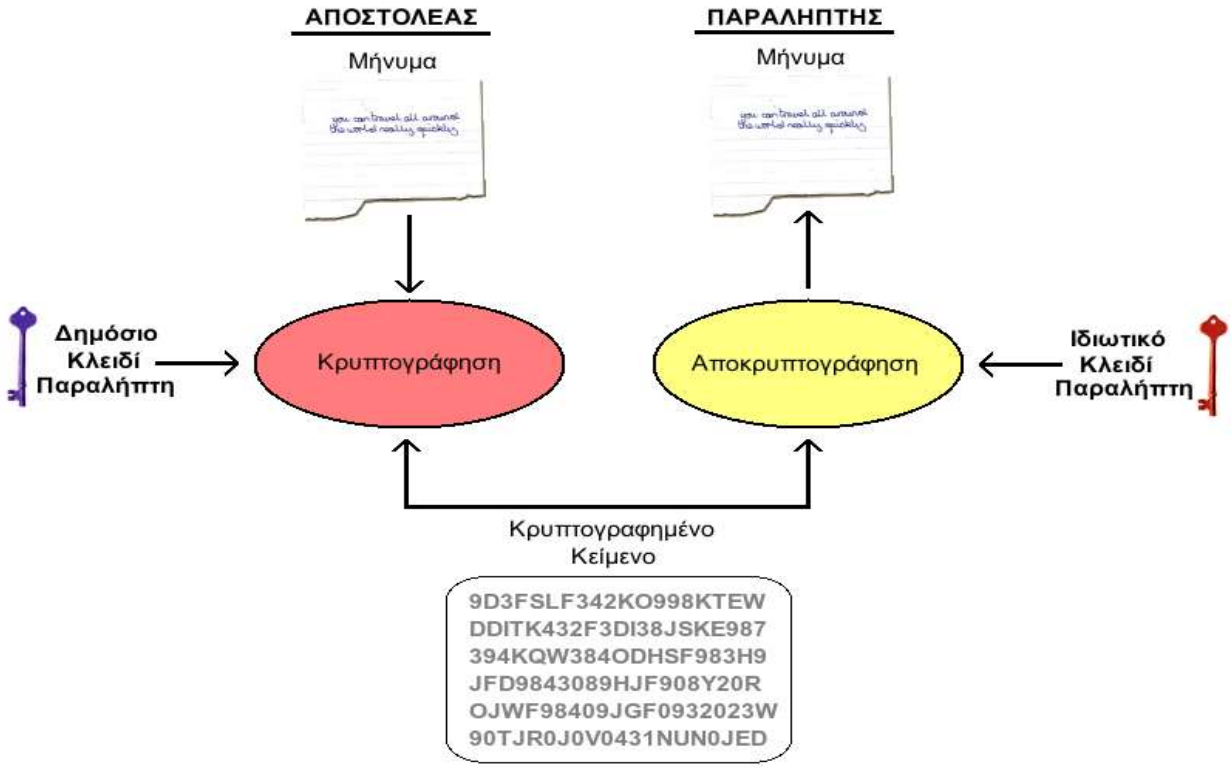
Η κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman και παρέχει ένα εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης από την προγενέστερη κρυπτογράφηση συμμετρικού κλειδιού. 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 τη διαδικτυακ 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.

Η κρυπτογράφηση δημοσίου κλειδιού λύνει ένα σημαντικότατο πρόβλημα που υπήρχε στους κρυπτογραφικούς αλγόριθμους συμμετρικού κλειδιού. Συγκεκριμένα, οι κρυπτογραφικοί αλγόριθμοι συμμετρικού κλειδιού χρησιμοποιούν ένα κοινό μυστικό κλειδί, το οποίο το γνωρίζουν τόσο ο αποστολέας του κρυπτογραφημένου μηνύματος όσο και ο παραλήπτης. Αυτό το κοινό μυστικό κλειδί χρησιμοποιείται κατά τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης του μηνύματος. Προκύπτει όμως το εξής πρόβλημα: Εάν υποθέσουμε ότι το κανάλι επικοινωνίας δεν είναι ασφαλές, τότε πως γίνεται ο αποστολέας να στείλει το κλειδί κρυπτογράφησης στον παραλήπτη για να μπορέσει αυτός με τη σειρά του να αποκρυπτογραφήσει το μήνυμα; Αυτό το πρόβλημα είναι ιδιαίτερα έντονο στις σύγχρονες ψηφιακές επικοινωνίες όπου σε πολλές περιπτώσεις ο αποστολέας δεν γνωρίζει καν τον παραλήπτη και απέχει από αυτόν αρκετές χιλιάδες χιλιόμετρα. Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού λύνουν αυτό το πρόβλημα και ανοίγουν νέους δρόμους για εφαρμογές της κρυπτογράφησης (ηλεκτρονικά μηνύματα, διαδικτυακές αγορές κοκ).

6.3 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 στη γεννήτρια κλειδιών τόσο πιο ασφαλή είναι τα κλειδιά που παράγονται. Σε σύγχρονα προγράμματα κρυπτογράφησης ο τυχαίος αριθμός παράγεται ως εξής: Κατά τη διαδικασία κατασκευής των κλειδιών, το πρόγραμμα σταματάει για 5 λεπτά και καλεί τον χρήστη να συνεχίσει να εργάζεται με τον υπολογιστή. Στη συνέχεια για να παράξει τον τυχαίο αριθμό συλλέγει στα 5 αυτά λεπτά τυχαία δεδομένα που εξαρτώνται από τη συμπεριφορά του χρήστη (κινήσεις ποντικιού, πλήκτρα τουπληκτρολογίου που πατήθηκαν, κύκλοι μηχανής που καταναλώθηκαν κοκ). Με βάση αυτά τα πραγματικά τυχαία δεδομένα υπολογίζεται ο τυχαίος αριθμός και εισάγεται στη γεννήτρια κλειδιών για να κατασκευαστεί το δημόσιο και το ιδιωτικό κλειδί του χρήστη.

6.4 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. Στη 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.

7. ΜΗΝΥΜΑΤΑ ΠΟΥ ΔΕΝ ΕΧΟΥΝ ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΘΕΙ

1) **Ο αλγόριθμος κρυπτογράφησης Beale**

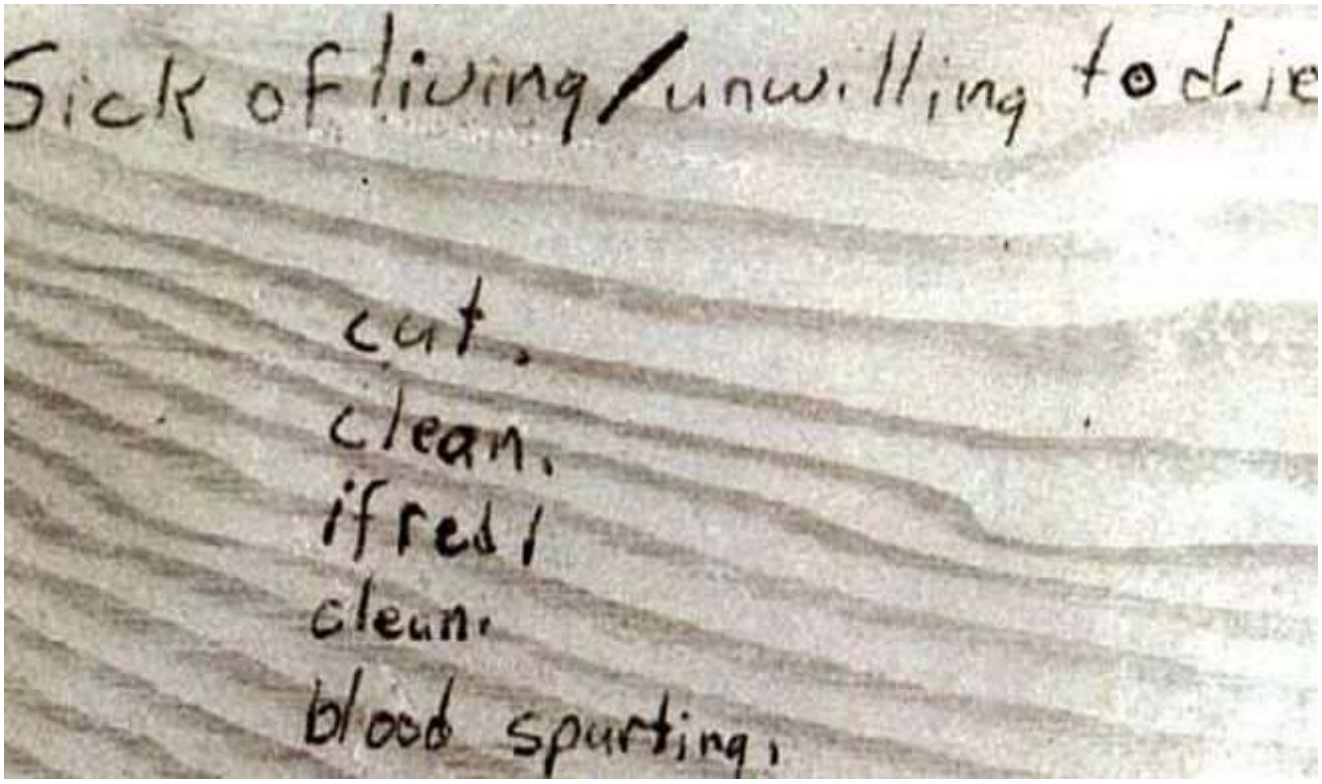
1, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416, 918, 263,
38, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 20
18, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61, 304,
4, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780, 18, 64, 463, 474
50, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 82
16, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150, 59,
14, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136, 872, 15, 28, 17
0, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 5
4, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38, 416, 89, 7
28, 965, 818, 2, 38, 121, 195, 14, 326, 148, 234, 18, 55, 131, 234, 361, 82
1, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206
6, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284, 919, 861, 326, 9
33, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612, 81, 360, 36,
94, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 46
0, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78, 14, 23, 111, 10
1, 501, 823, 216, 280, 34, 24, 150, 1000, 162, 286, 19, 21, 17, 340, 19, 24
6, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95, 12
48, 96, 11, 201, 77, 364, 218, 65, 667, 890, 236, 154, 211, 10, 98, 34, 119
16, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 1

Ο αλγόριθμος κρυπτογράφησης Beale περιλαμβάνει τρία κρυπτοκείμενα που υποτίθεται ότι αποκαλύπτουν την τοποθεσία ενός από τους μεγαλύτερους κρυμμένους θησαυρούς στην ιστορία των ΗΠΑ: χιλιάδες λίρες από χρυσό, ασήμι και κοσμήματα. Η ύπαρξη του θησαυρού αρχικά “εντοπίστηκε” από έναν μυστηριώδη άνδρα με το (γνωστό) όνομα Thomas Jefferson Beale, το 1818 στο Κολοράντο.

2)**Το Χειρόγραφο Voynich**

Το χειρόγραφο πήρε το όνομά του από τον πολωνικής καταγωγής Αμερικανό βιβλιοπώλη και παλαιοπώλη, Wilfrid M. Voynich, ο οποίος το απέκτησε το 1912. Το εν λόγω χειρόγραφο είναι ένα λεπτομερές βιβλίο 240 σελίδων, γραμμένο σε μια γλώσσα που παραμένει και σήμερα εντελώς άγνωστη. Οι σελίδες του είναι γεμάτες με πολύχρωμα σχέδια, παράξενα διαγράμματα, περίεργα γεγονότα και φυτά που δεν θυμίζουν κανένα γνωστό είδος, συμβάλλοντας έτσι στην ίντριγκα του εγγράφου και στη δυσκολία αποκρυπτογράφησης.

3)Τα κρυπτογραφημένα μηνύματα του Zodiac



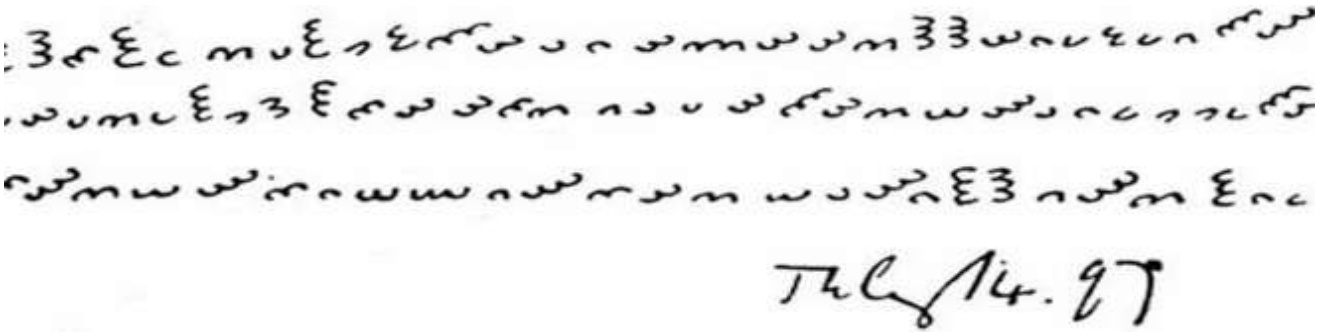
Ο λόγος για μια σειρά τεσσάρων κρυπτογραφημένων μηνυμάτων που πιστεύεται ότι έχουν γραφτεί από τον διάσημο Zodiac Killer, έναν κατά συρροή δολοφόνο, ο οποίος τρομοκρατούσε τους κατοίκους του San Francisco Bay Area στα τέλη του 1960 και στις αρχές της δεκαετίας του 1970. Οι επιστολές πιθανόν γράφτηκαν ως ένας τρόπος να κοροϊδέψει τους δημοσιογράφους και την αστυνομία. Μόνο ένα από τα μηνύματα έχει αποκρυπτογραφηθεί, ενώ τα υπόλοιπα τρία παραμένουν άλυτα.

4)Το κρυπτογραφημένο γλυπτό Kryptos

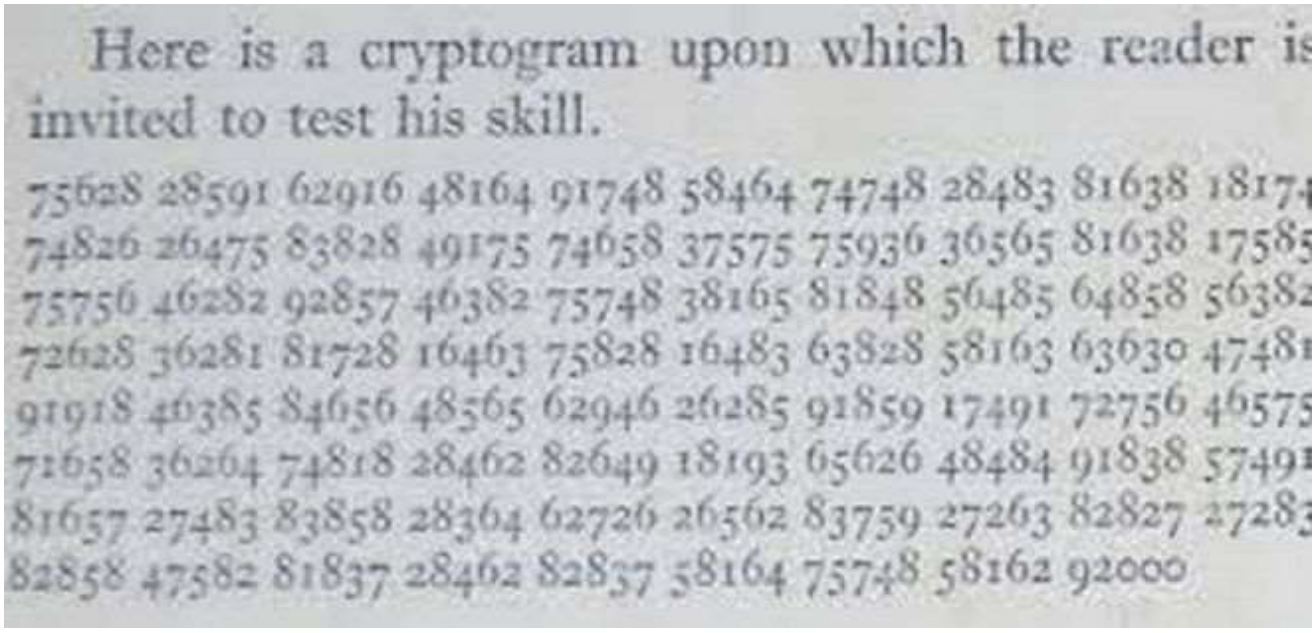
Το Kryptos είναι ένα μυστηριώδες κρυπτογραφημένο γλυπτό που σχεδιάστηκε από τον καλλιτέχνη Jim Sanborn και βρίσκεται ακριβώς έξω από την έδρα της CIA στο Λάνγκλεϊ της Βιρτζίνια. Πρόκειται για 865 συνολικά χαρακτήρες που δεν βγάζουν κανένα νόημα, που είναι γραμμένοι σε χαλκό πάχους 1,25 εκ. Ο γλύπτης εμπνεύστηκε το έργο του

από την ελληνική λέξη "κρυφός" και θεωρεί ότι είναι ένας στοχασμός στη φύση της μυστικότητας αφού το μήνυμά του είναι εξ ολοκλήρου κρυπτογραφημένο.

5)Το κρυπτογραφημένο μήνυμα του Edward Elgar



Το 1897, ο συνθέτης Edward Elgar έστειλε αυτό το κρυπτογραφημένο μήνυμα σε μια 23χρονη φίλη του, την Dora Penny.



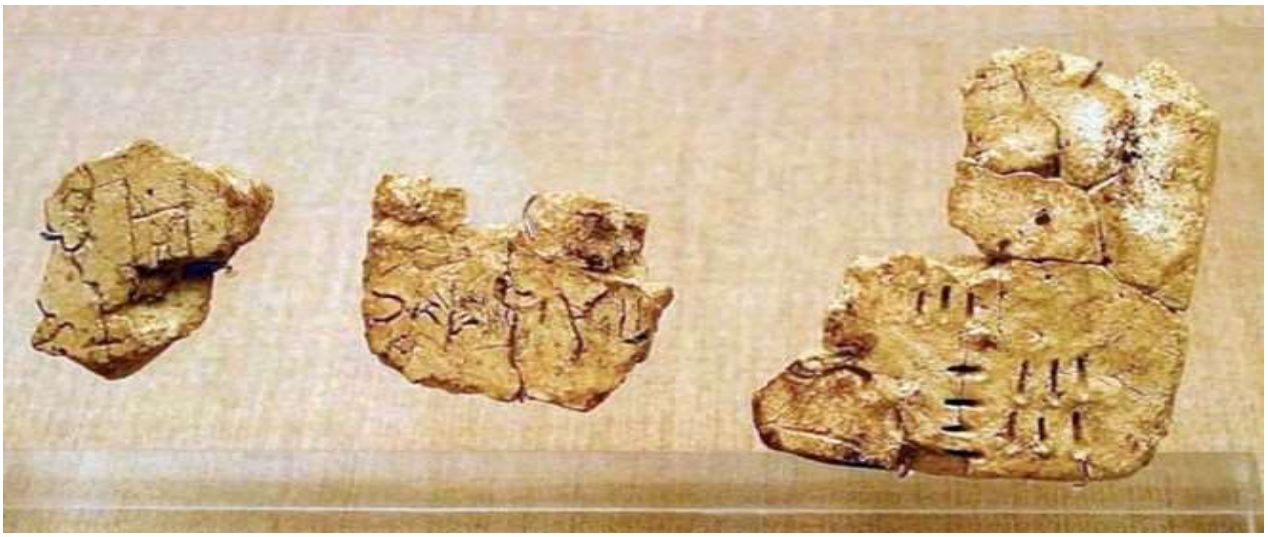
Here is a cryptogram upon which the reader is invited to test his skill.

75628 28591 62916 48164 91748 58464 74748 28483 81638 18174
74826 26475 83828 49175 74658 37575 75936 36565 81638 17585
75756 46282 92857 46382 75748 38165 81848 56485 64858 56382
72628 36281 81728 16463 75828 16483 63828 58163 63630 47481
91918 46385 84656 48565 62946 26285 91859 17491 72756 46575
71658 36264 74818 28462 82649 18193 65626 48484 91838 57491
81657 27483 83858 28364 62726 26562 83759 27263 82827 27283
82858 47582 81837 28462 82837 58164 75748 58162 92000

6)Βιβλίο για την κρυπτογραφία από τον Agapeyeff

Ο Alexander d'Agapeyeff έγραψε ένα βιβλίο για την κρυπτογραφία το 1939 συμπεριλαμβανομένης μιας που δημιούργησε ο ίδιος.

7)Γραμμική Α



Γραμμική Α: Το 1990, ένας αριθμός πήλινων σπασμένων δοχείων βρέθηκαν στη Κρήτη και χρονολογούνται από το 1800 π.Χ. Περιέχει δυο γραφές, την Γραμμική Α και Β. Μόνο η Β έχει αποκρυπτογραφηθεί.

8)Ο δίσκος της Φαιστού

Το μυστήριο του δίσκου της Φαιστού είναι μια ιστορία από τα μέρη μας. Ανακαλύφθηκε από τον ιταλό αρχαιολόγο Luigi Pernier το 1908 στο μινωικό ανάκτορο της Φαιστού. Ο δίσκος είναι κατασκευασμένος από ψημένο πηλό και περιέχει μυστηριώδη σύμβολα που ενδέχεται να αντιπροσωπεύουν μια άγνωστη μορφή ιερογλυφικών. Πιστεύεται ότι έχει σχεδιαστεί κάποια στιγμή κατά τη δεύτερη χιλιετία π.Χ.

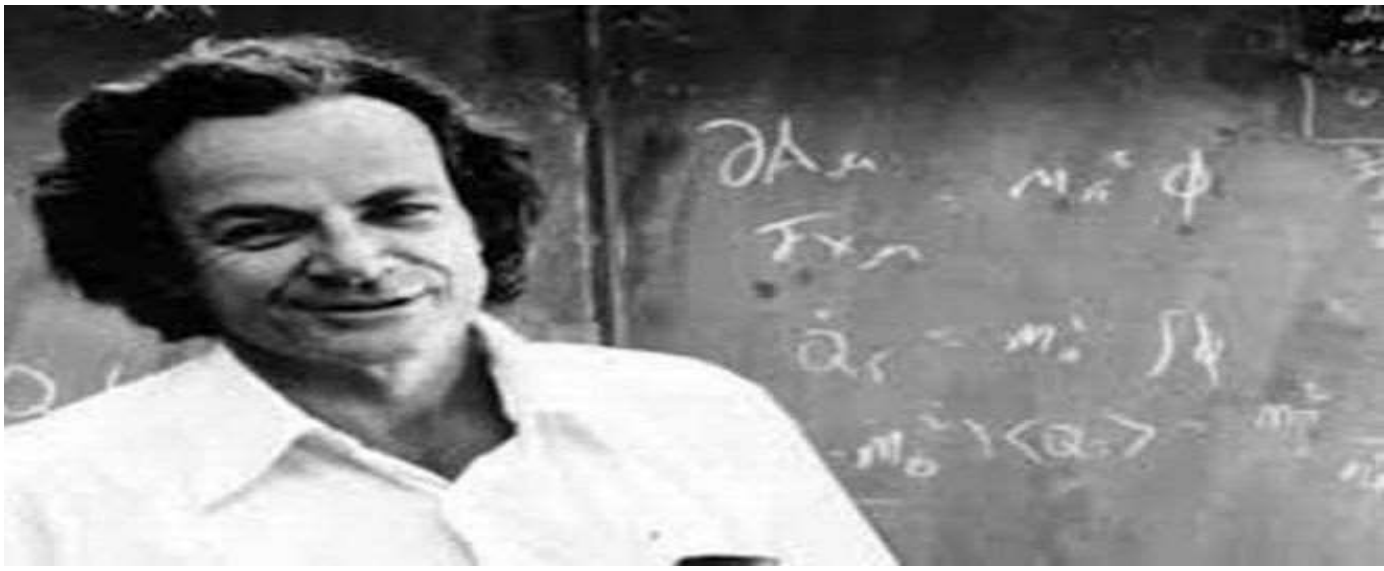
9)Κρυπτογραφία σε ράβδους χρυσού

Επτά ράβδοι χρυσού που βρέθηκαν στη Σαγκάη. Περιέχουν εικόνες, γράμματα και λατινικά γράμματα.

10)Κρυπτογραφήματα από τον πολιτισμό της κοιλάδας του Ινδού

Ο πολιτισμός της κοιλάδας του Ινδού υπήρχε μεταξύ 2600-1800 π.Χ.. Άφησαν πίσω τους χιλιάδες αντικείμενα χαραγμένα.

11)Οι κώδικες Feynman



Το 1987, ο RIchard Feynman έδωσε τρεις κώδικες σε έναν συνάδελφο. Από τότε μόνο ένας έχει λυθεί.Ήταν ένας από τους σημαντικότερους θεωρητικούς φυσικούς, ο οποίος τιμήθηκε και με το Βραβείο Νόμπελ Φυσικής για την δουλειά του στην Κβαντική Μηχανική, ειδικά για τη συμβολή του στην ανάπτυξη της Κβαντικής ηλεκτροδυναμικής.

12)Γερμανικός μηχανισμός κρυπτογράφησης του Β' Παγκόσμιου

Πόλεμου

Μηχανισμός κρυπτογράφησης που χρησιμοποιήθηκε από τη Γερμανία στο Β 'Παγκόσμιο Πόλεμο. Είχε ως αποτέλεσμα ορισμένα από τα μηνύματα να μην αποκρυπτογραφηθούν.

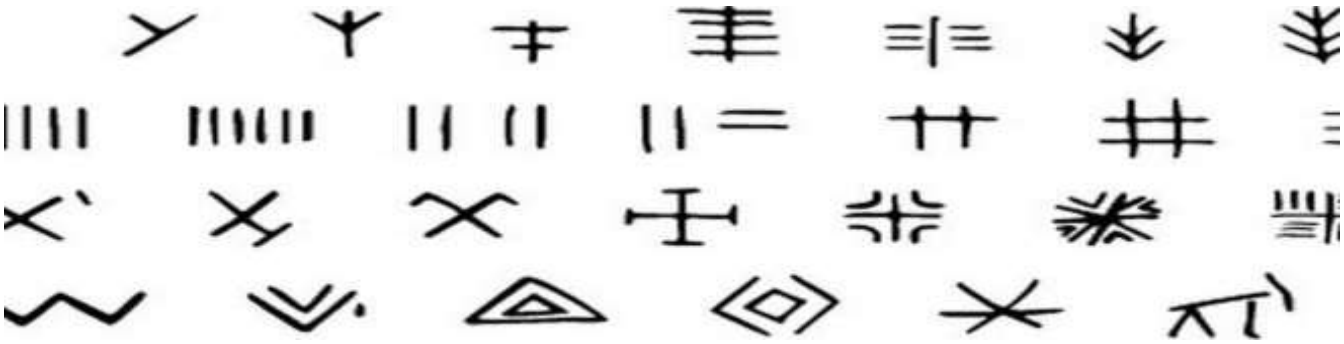
13)**Μήνυμα σε περιστέρι**

Μήνυμα που βρέθηκε στο δεμένο στο πόδι ενός περιστεριού που ποτέ δεν κατάφεραν να το αποκρυπτογραφήσουν.

14)**Το Rongorongo**

Το 1868, οι Ευρωπαίοι βρήκαν ξύλινα γλυπτά θρησκευτικών χειροποίητων αντικειμένων και επιπλέον αρκετών επιγραφών γνωστών ως Rongo - Rongo, οι οποίες αποτελούσαν ένα αρχείο της χαμένης γλώσσας του Rapa Nui. Το Rongorongo είναι ένα σύστημα μυστηριωδών ιερογλυφικών που ανακαλύφθηκε γραμμένο σε διάφορα αντικείμενα στα Νησία του Πάσχα. Πολλοί πιστεύουν ότι αντιπροσωπεύουν ένα χαμένο σύστημα γραφής ή μία πρώτη γραφή και θα μπορούσε να είναι ένας από τις μόλις 3 ή 4 ανεξάρτητες εφευρέσεις της γραφής στην ιστορία της ανθρωπότητας.

15)**Vinca**



Μια συλλογή από σύμβολα που βρέθηκαν σε χειροποίητα αντικείμενα που χρονολογούνται από το 6.000 έως το 4.500 π.Χ. Δεν είναι γνωστό αν αυτά τα σύμβολα είναι ένα σύστημα γραφής.

16)Επιγραφή Proto-Elamite

Επιγραφή που βρέθηκε στο νοτιοδυτικό Ιράν και χρονολογείται από το 2900 π.Χ.

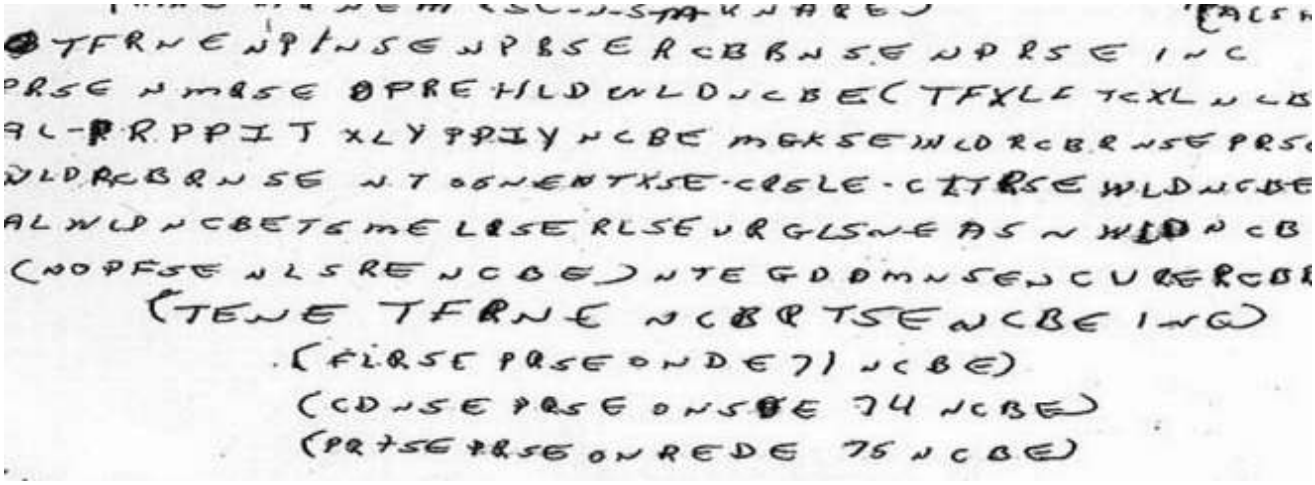
17)Κώδικας Rohonc

Επιγραφή που βρέθηκε στην Ουγγαρία γραμμένη σε άγνωστη γλώσσα.

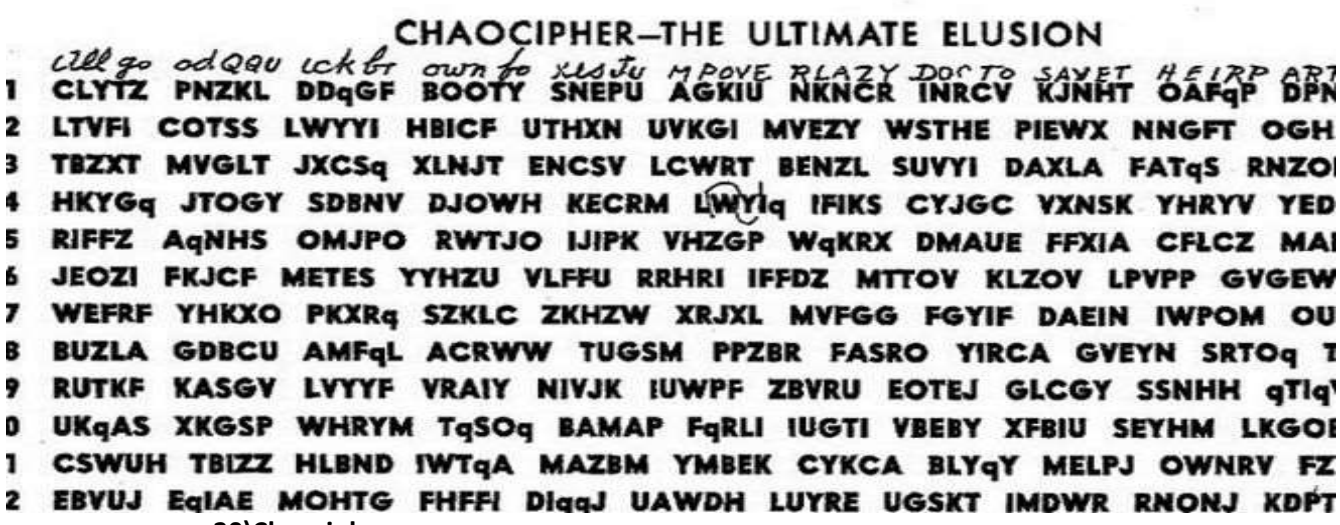
18)Το μυστήριο του Taman Shud

Ένα πτώμα ξεβράστηκε στις ακτές του Somerton στην περιοχή Αδελαϊδα, το 1948 μαζί με κάτι χαρτάκια. Το θύμα δεν αντιμετώπιζε προβλήματα υγείας, δεν έφερε κανένα τραύμα και δεν βρέθηκε δηλητήριο στον οργανισμό του. Κανείς δεν γνωρίζει πώς πέθανε. Το μόνο στοιχείο που βρέθηκε πάνω του ήταν ένα σημείωμα με τις λέξεις "Tamam Shud", (τετέλεσται). Η φράση ήταν απόσπασμα από ένα βιβλίο με ποιήματα του Ομάρ Καγιάμ, το οποίο βρέθηκε κοντά στο πτώμα. Μέσα στο βιβλίο οι αρχές βρήκαν ένα κωδικοποιημένο μήνυμα που ακόμα δεν έχει αποκρυπτογραφηθεί και η υπόθεση παραμένει άλυτη.

19)Το μυστήριο McCormick

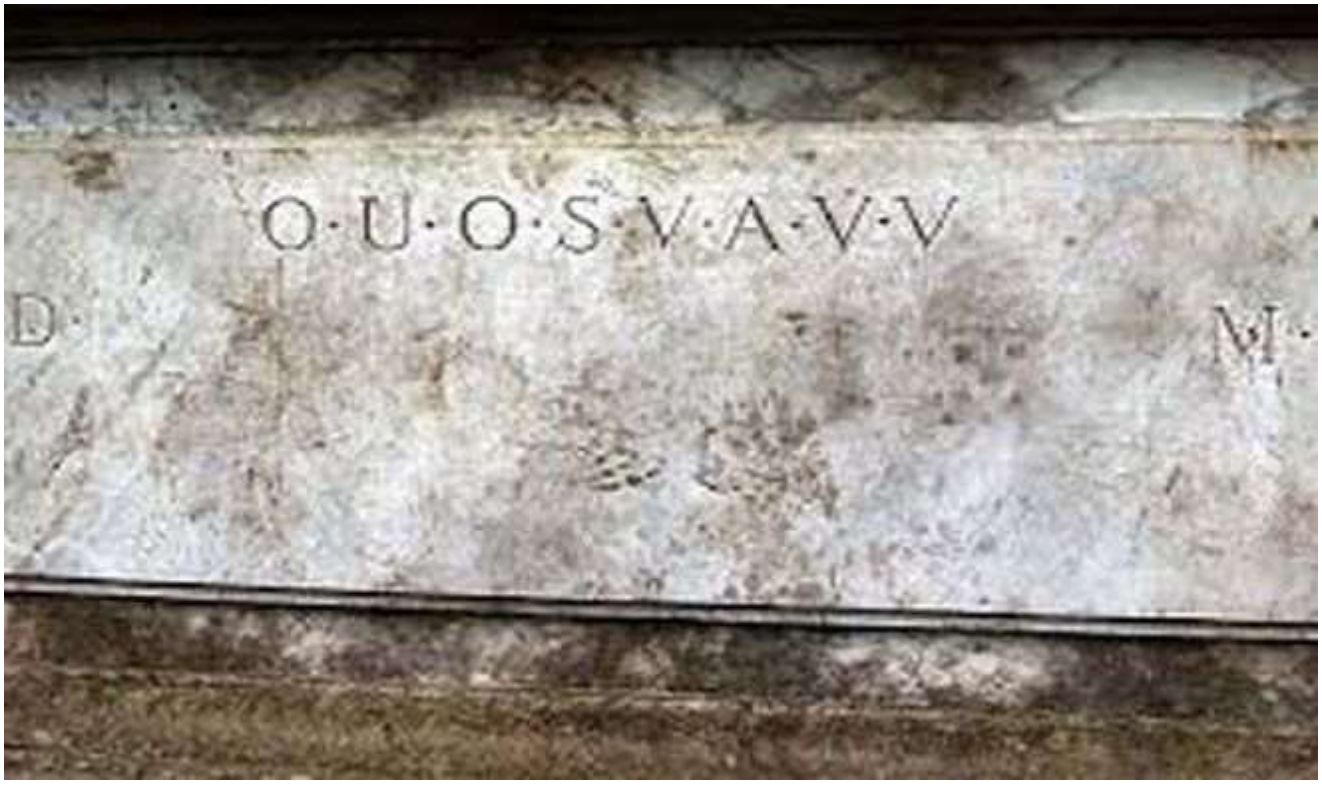


Το 1999, το πτώμα του Ricky McCormick βρέθηκε στο ανατολικό Μιζούρι. Στις τσέπες του είχε δυο αλγόριθμους κρυπτογραφημένους. Το FBI έχει ζητήσει τη βοήθεια του κοινού.



20)Chaocipher

Το παρακάτω κείμενο ήταν στην αυτοβιογραφία του συγγραφέα JF κ. Byrne.



21)Επιγραφή στο Staffordshire

Εκ πρώτης όψεως, αυτό το μνημείο από τον 18ο αιώνα στο Staffordshire της Αγγλίας, δεν έχει κάτι το παράξενο. Όμως, με μια πιο προσεκτική ματιά, ο παρατηρητής θα δει μία μυστηριώδη επιγραφή: DOUOSVAVVM. Εδώ και 250 χρόνια, κανείς δεν έχει καταφέρει να εξηγήσει τι σημαίνουν αυτά τα γράμματα.

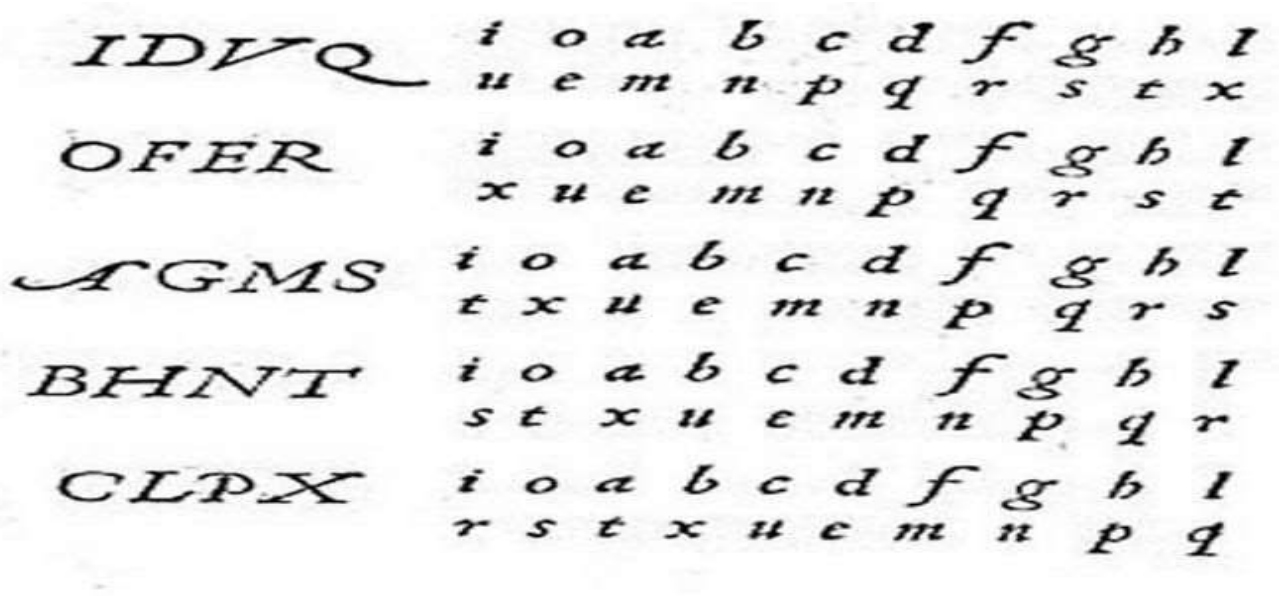
22)Κώδικας Navajo

Κατά τη διάρκεια του Β 'Παγκοσμίου Πολέμου οι σύμμαχοι χρησιμοποιούσαν τη γραφή των Ινδών Navajo.

23)Blitz

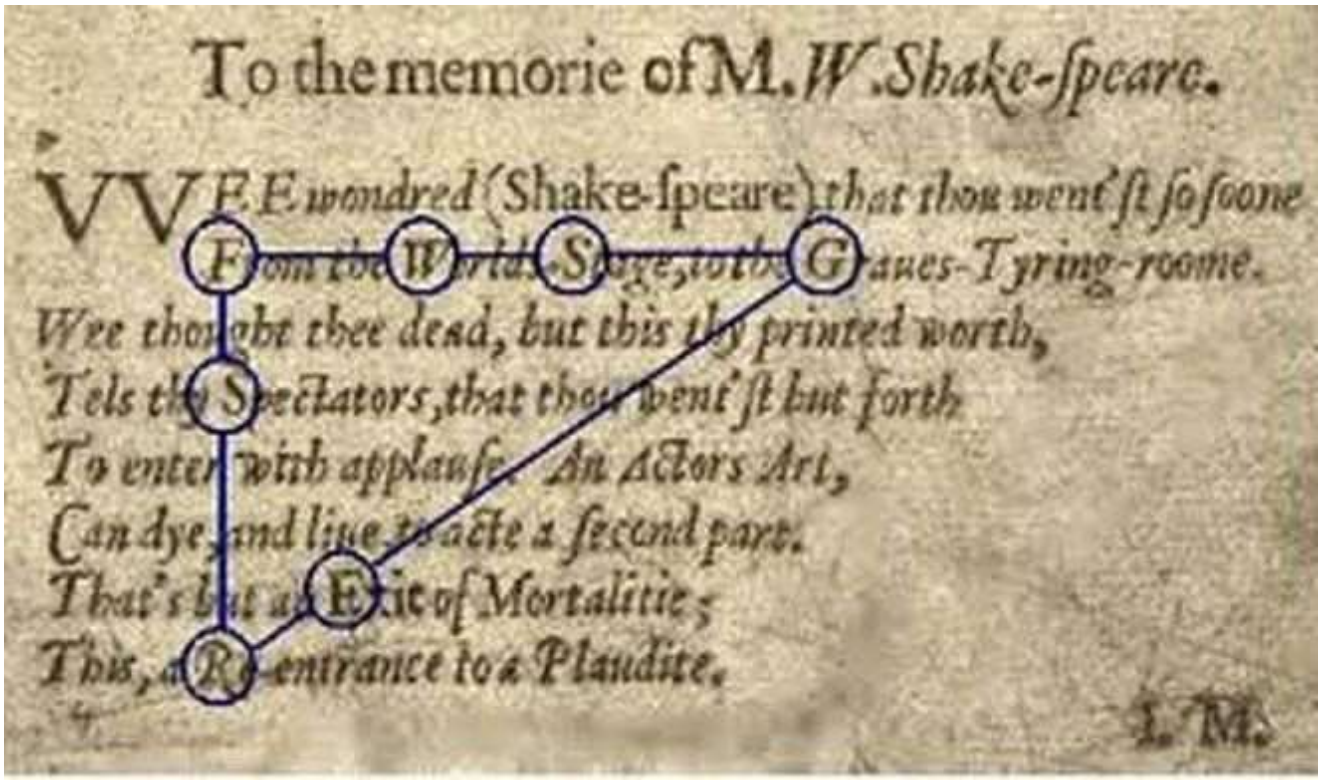
Ανακαλύφθηκαν κατά τη διάρκεια του Β 'Παγκοσμίου Πολέμου σε ένα βομβαρδισμένο κελάρι στο Ανατολικό Λονδίνο. Απεικονίζουν 50 καλλιγραφικά σύμβολα ... πιθανώς του 18ου αιώνα.

24)Η κρυπτογράφηση Vigenere



Η κρυπτογράφηση Vigenere είναι μια μέθοδος κρυπτογράφησης με την μορφή της πολυαλφαβητικής υποκατάστασης και έχει εφευρεθεί εκ νέου πολλές φορές. Η μέθοδος περιγράφηκε αρχικά το 1553 από τον Giovan Battista Bellaso.Η κρυπτογράφηση αυτή είναι γνωστή γιατί, ενώ είναι εύκολο να τη κατανοήσουν και να την εφαρμόσουν, φαίνεται συχνά στους αρχάριους να είναι ακατόρθωτο να την αποκρυπτογραφήσουν.Για την κρυπτογράφηση μπορεί να χρησιμοποιηθεί ένας πίνακας γνωστός ως τετράγωνο ή πίνακας Vigenere.

25)**Κρυπτογραφημένα μηνύματα του Sir Francis Bacon**


To the memorie of M. W. Shake-speare.

VVE E wondred (Shake-speare) that thou went'st so soone
From the World-Stage, to the Graues-Tyring-roome.
Wee thought thee dead, but this thy printed worth,
Tels thy Spectators, that thou went'st but forth
To enter with applause. An Actors Art,
Can dye, and liue to acte a second part.
That's but an Exit of Mortalitie;
This, a Re-entrance to a Plaudite.

I. M.

Λογοτεχνικό έργο του Sir Francis Bacon με κρυπτογραφημένα μηνύματα. Υπήρξε εικασίες ότι ήταν ο υπεύθυνος για τα έργα του Σαίξπηρ.

8. ΠΗΓΕΣ

Simon Singh, «Κώδικες και Μυστικά», Εκδόσεις ΤΡΑΥΛΟΣ

https://en.wikipedia.org/wiki/Enigma_machine

https://en.wikipedia.org/wiki/Alan_Turing

https://en.wikipedia.org/wiki/Code_talker

http://www.pcsteps.gr/

www.easypedia.gr

www,uom.gr

www.uoa.gr