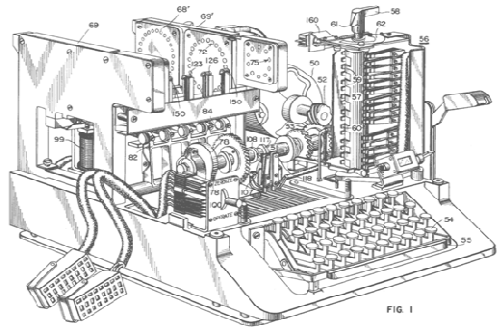
ΚΡΥΠΤΟΓΡΑΦΙΑ



ΤΑ ΟΝΟΜΑΤΑ ΤΩΝ ΜΑΘΗΤΩΝ

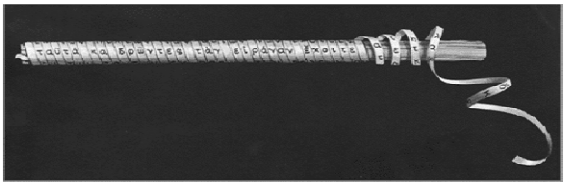
- ΕΛΕΝΗ ΜΑΝΟΥΣΟΥ
- ΕΛΕΥΘΕΡΙΑ ΚΟΝΤΟΓΕΩΡΓΑΚΟΥ
- ΑΓΓΕΛΟΣ ΑΝΑΣΤΑΣΗΣ
- ΜΕΡΑΝ ΑΛΤΑΦ
- ΚΩΣΤΑΣ ΓΕΩΡΓΙΟΥ
- ΝΙΚΟΣ ΚΑΡΑΤΖΑΚΗΣ
- ΧΡΗΣΤΟΣ ΔΙΑΚΟΓΙΑΝΝΗΣ
- ΙΑΣΟΝΑΣ ΑΒΡΑΜΟΠΟΥΛΟΣ
- ΔΕΣΠΟΙΝΑ ΛΕΒΕΝΤΕΛΗ
- ΜΑΡΙΑ ΠΑΠΑΔΟΠΟΥΛΟΥ
- ΓΕΩΡΓΙΟΣ ΔΙΟΝΥΣΑΤΟΣ
- ΔΗΜΗΤΡΗΣ ΔΑΜΙΓΟΣ
- ΦΩΤΗΣ ΝΤΙΜΕΡΗΣ
- ΑΛΕΞΑΝΔΡΟΣ ΓΚΟΒΙΛΑΣ
- ΑΓΓΕΛΟΣ ΧΑΤΣΗΣ

Περιεχόμενα

Εισαγωγη

- Ετοιμολογία της λέξης « κρυπτογραφία»
- Η κρυπτογραφία είναι ένας κλάδος της επιστήμης
- Η θέση της κρυπτογραφίας στην ιστορία
- Οι 4 βασικές λειτουργίες (αντικείμενοι σκοποι)

ΣΠΑΡΤΙΑΤΙΚΗ ΣΚΥΤΑΛΗ



Γύρω από την σκυτάλη τυλίγεται ταινία υφάσματος ή δέρματος . Κατά μήκος της 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 στην σκυτάλη ίδιου μήκους και διαμέτρου ,με τον τρόπο που είχε προ-συμφωνηθεί με τον αποστολέα , προκειμένου να αποκαλύψει το μήνυμα . Τα μηνύματα 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. Το αυθεντικό Τετράγωνο του Πολυβίου βασίστηκε στην ελληνική αλφάβητο , ύστερα ακολούθησαν στα Ιαπωνικά και στα Αγγλικά.

ΤΟ ΤΕΤΡΑΓΩΝΟ ΤΟΥ ΠΟΛΥΒΙΟΥ

	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	

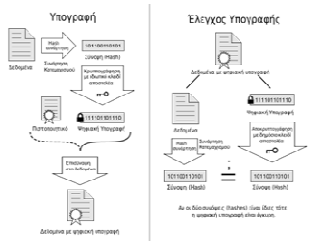
ΤΟ ΚΡΥΠΤΟΓΡΑΜΜΑ ΠΛΕΪΦΕΑΡ

Στις αρχές του 1854 ο Σκοτσέζος επιστήμονας και πολιτικός Λάιον Πλέιφεαρ περιέγραψε ένα ασφαλές μέσον τηλεγραφικής επικοινωνίας Το κρυπτόγραμμα ήταν το πρώτο που χρησιμοποιούσε την τεχνική δίγραφου, στην οποία τα γράμματα υποκαθίστανται δύο δύο και όχι ανεξάρτητα. Επιλέγεται μία λέξη κλειδί γνωστή τόσο στον αποστολέα όσο και στον παραλήπτη π.χ., η λέξη ΠΟΤΑΜΙ. Σε ένα παραλληλόγραμμο 4Χ6, γράφεται το κλειδί ακολουθούμενο από τα υπόλοιπα γράμματα του αλφάβητου στη σειρά

Κρυπτογράφηση Δημόσιου Κλειδιού

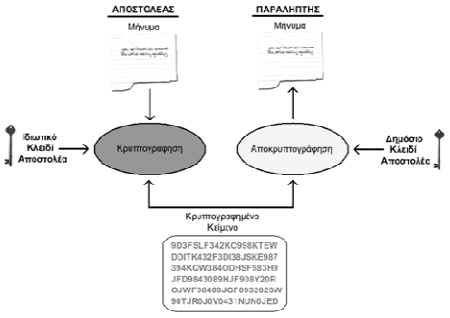
Κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται ιδιωτικό κλειδί και το άλλο δημόσιο κλειδί . Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να το ανακοινώνει σε όλη την διαδικτυακή κοινότητα ή σε συγκεκριμένους παραλήπτες

Κρυπτογράφηση Δημόσιου Κλειδιού



Κρυπτογράφηση Δημόσιου Κλειδιού

Κρυπτογράφηση Δημόσιου Κλειδιού



Ετοιμολογια της λεξης « κρυπτογραφία»

- Η λέξη **κρυπτογραφία** προέρχεται από τα συνθετικά "κρυπτός" + "γράφω" και είναι ένας επιστημονικός κλάδος που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων.

Η κρυπτογραφια είναι ενας κλαδος της επιστήμης

- Η κρυπτογραφία είναι ένας κλάδος της επιστήμης της κρυπτολογίας, η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς για 2 ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάζει την πληροφορία εκτός από τα μέλη. Η λέξη κρυπτολογία αποτελείται από την ελληνική λέξη "κρυπτός" και τη λέξη "λόγος" και χωρίζεται σε δύο κλάδους: Την **Κρυπτογραφία** και την**Κρυπτανάλυση** με παρεμφερή κλάδο την **Στεγανογραφία** και αντίστοιχα την **Στεγανοανάλυση**.

η θεση της κρυπτογραφιας στην ιστορια

- Ιστορικά η κρυπτογραφία χρησιμοποιήθηκε για την κρυπτογράφηση μηνυμάτων δηλαδή μετατροπή της πληροφορίας 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. Στις νεότερες μορφές η κρυπτογραφία κάνει χρήση του αριθμητικού ισοδύναμου, η έμφαση έχει μεταφερθεί σε διάφορα πεδία των μαθηματικών, όπως διακριτά μαθηματικά, θεωρία αριθμών, θεωρία πληροφορίας, υπολογιστική πολυπλοκότητα, στατιστική και συνδυαστική ανάλυση.

Οι 4 βασικες λειτουργειες (αντικειμενοι σκοποι)

Η κρυπτογραφία παρέχει τέσσερις βασικές λειτουργίες (Αντικειμενικοί σκοποί):

- *Εμπιστευτικότητα*: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- *Ακεραιότητα*: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.
- *Μη απάρνηση*: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- *Πιστοποίηση*: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

Η ΓΡΑΜΜΙΚΗ Β

- Ο αρχιτέκτονας Μάικλ Βέντρις και ο φίλος του Τζων Τσάντγουικ αποκρυπτογράφησαν 65 από τους 88 τότε βασικούς κανόνες ορθογραφίας.
- Η Γραμμική β περιλαμβάνει 89 συλλαβογράμματα και 260 ιδεογράμματα που αναπαριστούν και αποδίδουν έννοιες όπως άνδρα, γυναίκα κλπ. Και σύμβολα για αριθμούς.

ΔΙΣΚΟΣ ΤΗΣ ΦΑΙΣΤΟΥ

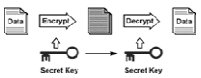
- Ο δίσκος της Φαιστού είναι ένα αρχαιολογικό εύρημα από την Μινωική πόλη της Φαιστού στην νότια Κρήτη και χρονολογείται πιθανώς στον 17ο αιώνα πχ.
- Συνολικά υπάρχουν 241 σύμβολα, 122 στην 1η πλευρά και 119 στην 2η .Ο σκοπός της κατασκευής του και το νόημα των όσων αναγράφονται σε αυτό παραμένουν άγνωστα.
- Ο δίσκος της Φαιστού ανακαλύφθηκε στης 3 Ιουνίου 1908 από τον Λουϊτζι Περνιέ.

ΙΕΡΟΓΛΥΦΙΚΑ-ΣΤΗΛΗ ΤΗΣ ΡΟΖΕΤΑΣ

- Τα ιερογλυφικά είναι αρχαία εικονιστικά στοιχεία που χρησιμοποιούνται στην αρχαία Αιγυπτιακή γραφή.
- Η γραφή αυτή αποκρυπτογραφήθηκε από τον Σαμπολιόν το 1822.
- Η στήλη της ροζέτας είναι μια πέτρινη πλάκα από γρανοδιορίτη από τον ναό του Πτολεμαίου Ε΄ του επιφανούς.
- Χρονολογείται στον 2ο αιώνα πχ. Και φέρει εγχάρακτη μια επιγραφή σε δυο γλώσσες [αιγυπτιακά+ ελληνικά].

ΜΥΣΤΙΚΟ ΚΛΕΙΔΙ-ΚΑΙΣΑΡΑΣ

- Το κλειδί καθορίζει το ακριβές κρυπτογραφικό αλφάβητο που πρέπει να χρησιμοποιηθεί για μια συγκεκριμένη κρυπτογράφηση.
- Αν το κρυπτογραφικό αλφάβητο, έχει τηρηθεί απόλυτα μυστικό ,τότε ο εχθρός δεν μπορεί να αποκρυπτογραφήσει το υποκλαπέν μήνυμα.
- Ο Καίσαρ χρησιμοποιούσε τη μυστική γραφή τόσο συχνά ώστε ο Πρόβος έγραψε μια ολόκληρη πραγματεία για τα κρυπτογράμματα του.
- Ένας από τους τύπους κρυπτογραφίας που χρησιμοποιούσε ο Ιούλιος Καίσαρ: απλώς αντικαθιστούσε κάθε γράμμα του μηνύματος με το κατά τρεις θέσεις επόμενο του στο αλφάβητο.



ΣΤΕΓΑΝΟΓΡΑΦΙΑ
Η ΤΕΧΝΗ ΤΗΣ ΑΠΟΠΛΑΝΗΣΗΣ

Ο άνθρωπος σε όλη τη διαδρομή της ιστορίας ανακάλυπτε συνεχώς νέες μεθόδους για να κρύψει μηνύματα άλλα και να αποκωδικοποιήσει μηνύματα.Μια παρά πολύ σημαντική τεχνική ήταν η μέθοδος της στεγανογραφίας.Σε αντίθεση με την κρυπτογράφηση στην οποία το μήνυμα φαίνεται, ενώ στη στενογραφία έχεις την δυνατότητα να κρύψεις ένα μήνυμα μέσα σ' ένα άλλο αθώο μηνυμα.Επισης στις μέρες μας η τεχνική της στενογραφίας έχει αναπτυχτεί θετικά και στην τεχνική της επικοινωνίας όπου εκεί μπορείς να κρύψεις ίδια την ύπαρξη της πληροφορίας.

ΚΡΥΠΤΟΓΡΑΦΗΜΑ VIGENERE

Vigenere 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 λόγους 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.Χρησιμοποίησε τα μαθηματικά και την αποκωδικοποίηση προκειμένου να αποκρυπτογραφήσει μηνύματα που αντάλλαισαν 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. I peg

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- συνομωσιών και η συμβολή κυριότερα της κατασκοπίας άνοιξαν το δρόμο για τις μετέπειτα υπηρεσίες κατασκοπείας όπου είχε αρχίσει ο Ουολσινχαμ.

Κρυπτογραφία από τον 2ο παγκόσμιο πόλεμο μέχρι σήμερα

- **Άλαν Μάθισον Τούρινγκ**
- **Πρώτη περίοδος κρυπτογραφίας (1900 π.Χ.-1900 μ.Χ.)**
- **Δεύτερη περίοδος κρυπτογραφίας (1900 μ.Χ.-1950 μ.Χ.)**
- **Τρίτη περίοδος κρυπτογραφίας (1950 μ.Χ.-Σήμερα)**
- **ΚΩΔΙΚΑΣ ΝΑΒΑΧΩΝ**

- ***Άλαν Μάθισον Τούρινγκ***
- ***Κρυπτογραφική ανάλυση***
- ***Εργασία για τους πρώτους υπολογιστές και τη δοκιμή Turing***

Άλαν Μάθισον Τούρινγκ

- Ο **Άλαν Μάθισον Τούρινγκ** (Alan Matheson Turing, 23 Ιουνίου, 1912 - 7 Ιουνίου, 1954) ήταν Βρετανός μαθηματικός. Καθηγητής της λογικής, κρυπτογράφος και θεωρείται συχνά πατέρας της επιστήμης των υπολογιστών. Με τη δοκιμή*Τούρινγκ*, είχε μια σημαντική και χαρακτηριστική συμβολή στη συζήτηση σχετικά με τη τεχνητή νοημοσύνη: εάν είναι δυνατό να ειπωθεί ότι μια μηχανή γνωρίζει και μπορεί να σκεφτεί. Παρείχε μία επίσημη έννοια του αλγορίθμου και των υπολογίσιμων αριθμών με τη μηχανή Τούρινγκ, διατυπώνοντας την ευρέως αποδεκτή έκδοση "Τούρινγκ" με την διατριβή του για την *καθολική* μηχανή Τούρινγκ, δηλαδή ότι οποιοδήποτε πρακτικό πρότυπο υπολογισμού έχει είτε ένα ισότιμο είτε ένα υποσύνολο των ικανοτήτων μιας μηχανής Τούρινγκ.
- Οι 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 κωδικών, όντας ο προϊστάμενος της ομάδας 8. Η ομάδα αυτήν ήταν που επιφορτίστηκε με την αποκωδικοποίηση της Γερμανικής κρυπτογραφικής συσκευής Enigma.
- Μετά από τον πόλεμο, σχεδίασε έναν από τους πρώτους ηλεκτρονικούς προγραμματίσιμους ψηφιακούς υπολογιστές στο εθνικό φυσικό εργαστήριο, όπως λεγόταν, και κατασκεύασε και μια άλλη μηχανή, στο πανεπιστήμιο του Μάντσεστερ. ΤοΒραβείο Τούρινγκ δημιουργήθηκε προς τιμή του.

Κρυπτογραφική ανάλυση

- 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 "καταλύματος 8", τμήματος αρμόδιου για τα γερμανικά ναυτικά σήματα. Ο Τούρινγκ εφηύρε επίσης την τεχνική **Banburismus** για 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 Thomas Flowers το 1943.
- Στο τελευταίο μέρος του πολέμου, ο Τούρινγκ ανέλαβε (με το μηχανικό 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 ράδιο μεταδόσεις. 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.

Εργασία για τους πρώτους υπολογιστές και τη δοκιμή Turing

- Ο Τούρινγκ ήταν πολύ καλός αθλητής μαραθωνίου. Ο καλύτερος χρόνος του, 2 ώρες, 46 λεπτά και 3 δευτερόλεπτα, ήταν μόλις 11 λεπτά πιο αργός από τον αντίστοιχο του νικητή στους Ολυμπιακούς Αγώνες του 1948. Από το 1945 ως το 1947, εργάστηκε στο εθνικό φυσικό εργαστήριο, πάνω στο σχέδιο της αυτόματης μηχανή υπολογισμού. Παρουσίασε μια εργασία στις 19 Φεβρουαρίου του 1946, η όποια ήταν το πρώτο πλήρες σχέδιο ενός υπολογιστή. Αν και πέτυχε το σχεδιασμό της αυτόματης μηχανής υπολογισμού, υπήρξαν καθυστερήσεις στην έναρξη του προγράμματος και απογοητεύτηκε. Στα τέλη του 1947 επέστρεψε στο Καίμπριτζ για ένα έτος. Ενώ ήταν στο Καίμπριτζ, η κατασκευή της αυτόματης μηχανής υπολογισμού σταμάτησε προτού αρχίσει.
- Το 1949 έγινε αναπληρωτής διευθυντής του εργαστηρίου υπολογισμού στο πανεπιστήμιο του Μάντσεστερ, και εργαζόμενος στο λογισμικό για έναν από τους πρώτους αληθινούς υπολογιστές - τον Μάντσεστερ Mark Η. Κατά τη διάρκεια αυτής της περιόδου συνέχισε να κάνει περισσότερη αφηρημένη εργασία και στα *μηχανήματα υπολογισμού* και τη νοημοσύνη. Ο Τούρινγκ αντιμετώπισε το πρόβλημα της τεχνητής νοημοσύνης, και πρότεινε ένα πείραμα γνωστό σήμερα ως δοκιμή Τούρινγκ, μια προσπάθεια να καθοριστούν πρότυπα για μια μηχανή που καλείται **νοήμων**.
- Το 1948 ο Τούρινγκ συνεργάζεται με τον προηγούμενο προπτυχιακό συνάδελφό του, Champernowne και αρχίζει ένα πρόγραμμα σκακιού για έναν υπολογιστή που δεν έχει υπάρξει ακόμα. Το 1952, χωρίς έναν υπολογιστή αρκετά ισχυρό να εκτελέσει το πρόγραμμα, ο Τούρινγκ έπαιξε ένα παιχνίδι στο οποίο μιμήθηκε τον υπολογιστή, σκεπτόμενος για μισή ώρα ανά κίνηση. Το παιχνίδι καταγράφηκε και το πρόγραμμα έχασε από έναν συνάδελφο του Τούρινγκ. Εντούτοις, λέγεται ότι το πρόγραμμα κέρδισε ένα παιχνίδι ενάντια στη σύζυγο του Champernowne.

1η ΠΕΡΙΟΔΟΣ

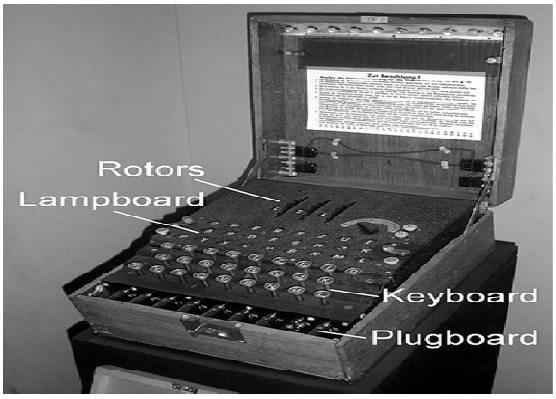
- Κατά την διάρκεια αυτής της περιόδου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, που βασίζονταν κυρίως σε απλές αντικαταστάσεις γραμμάτων. Όλες αυτές δεν απαιτούσαν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές, αλλά στηρίζονταν στην ευφυΐα και την ευρηματικότητα των δημιουργών 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 στην 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 την 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 στην 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 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.

2η ΠΕΡΙΟΔΟΣ

- 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 την 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 την 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).

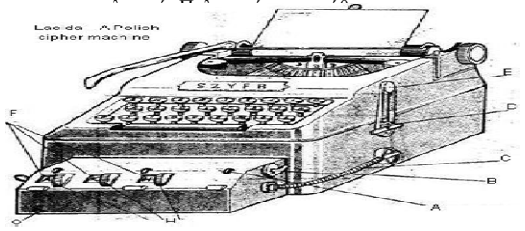
Η μηχανή Αίνιγμα χρησιμοποιήθηκε ευρέως από την Γερμανία



- 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 βασίζονταν 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 απο/κρυπτογράφησης και οδήγησε σε συνεχείς αποκρυπτογραφήσεις των διαφόρων παραλλαγών του Enigma, με την 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 στην Ναυμαχία της Μιντγουέι καθώς και στην εξόντωση του Αρχηγού του Ιαπωνικού Στόλου Ίζορόκου 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 προανήγγελλε 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



Τρίτη περίοδος κρυπτογραφίας (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 ομοσπονδιακό 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 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. Άλλοι πέντε από τους Code Talkers απεβίωσαν φέτος, γεγονός που οδήγησε το Ίδρυμα 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.