ΚΡΥΜΜΕΝΕΣ ΛΕΞΕΙΣ

Α’ ΛΥΚΕΙΟΥ

ΕΡΕΥΝΗΤΙΚΗ ΕΡΓΑΣΙΑ Β ΤΕΤΡΑΜΗΝΟΥ

1^{ο} ΛΥΚΕΙΟ ΕΛΑΣΣΟΝΑΣ

ΣΧ. ΕΤΟΣ 2013-2014

ΠΕΡΙΕΧΟΜΕΝΑ

Πρόλογος

Στη σημερινή εποχή η τεχνολογία έχει αναπτυχθεί ιδιαίτερα σημαντικά και γι' αυτό το λόγο έχει συμβάλλει στην επικοινωνία ανάμεσά μας. Με βάση τα μέσα τεχνολογίας αναπτύχθηκε η κρυπτογραφία με την οποία κρύβουμε στοιχεία και κωδικούς και προστατεύουμε τα προσωπικά μας δεδομένα. Στο τελικό στάδιο η κρυπτογραφία ωθεί στη ραγδαία εξέλιξη και στη ανάπτυξη ασφαλών συναλλαγών.
Στα πλαίσια λοιπόν της ερευνητικής εργασίας μελετήσαμε την ιστορία της κρυπτογραφίας ανά τους αιώνες, βρήκαμε διάφορες μορφές κρυπτογράφησης , φτιάξαμε ένα παιχνίδι κρυπτογράφησης και σας τα παρουσιάζουμε παρακάτω

Εισαγωγή και ορισμός (όπως διατύπωνεται στη Wikipedia)

Η λέξη **κρυπτογραφία** 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 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.

Αρχικά, η Κρυπτογραφία αποτέλεσε την τεχνική της απόκρυψης του περιεχομένου ενός μηνύματος, από μη εξουσιοδοτημένες οντότητες.

Στις μέρες μας η Κρυπτογραφία έχει αναχθεί σε επιστήμη, με τις εφαρμογές τις διαρκώς να πληθαίνουν.

Περιοδοι κρυπτογραφησης

1η περίοδος κρυπτογραφησης 1900 π.χ. -1900 μ.χ
2η περιοδος κρυπτογραφησης 1900 μ.χ. -1950 μ.χ.
3η περίοδος κρυπτογραφησης 1950 μ.χ. – σήμερα

1η περίοδος κρυπτογραφησης

Μια από τις παλαιότερες αναφορές στην αποστολή «κρυφών» μηνυμάτων είναι σίγουρα το περιστατικό που διηγείται ο Ηρόδοτος σχετικά με την κήρυξη της επανάστασης των ιωνικών πόλεων κατά των Περσών, η οποία απετέλεσε και την αφορμή για τους ελληνοπερσικούς πολέμους.

Σύμφωνα λοιπόν με τον Ηρόδοτο, ο Ιστιαίος, πρώην τύραννος της Μιλήτου και «φιλοξενούμενος» στην αυλή του Δαρείου για λόγους προληπτικής επιτήρησης, ήθελε να ειδοποιήσει τον διάδοχό του στη διοίκηση της Μιλήτου, Αρισταγόρα, να κηρύξει επανάσταση κατά των Περσών. Την άνοιξη του 499 π.Χ. λοιπόν κούρεψε έναν έμπιστο δούλο του και έγραψε στο δέρμα του κεφαλιού του το μήνυμα «Ἰστιαῖος Ἀρισταγόρᾳ· Ἰωνίαν ἀπόστησον» (ο Ιστιαίος προς τον Αρισταγόρα: ξεσήκωσε σε αποστασία την Ιωνία). Στη συνέχεια περίμενε να μεγαλώσουν τα μαλλιά του δούλου και τον έστειλε στον Αρισταγόρα, με την προφορική οδηγία να ζητήσει από τον Αρισταγόρα να τον κουρέψει, για να φανεί το μήνυμα που μεταφέρει

Ωστόσο η μέθοδος του Ιστιαίου δεν μπορεί να θεωρηθεί ως κρυπτογραφία με τη στενή έννοια, αφού ο αποστολέας είχε αποκρύψει *το ίδιο* το μήνυμα αντί να το έχει σε κοινή πρόσβαση και να έχει αποκρύψει *το* «κλειδί» της ανάγνωσής του. [http://www.tovima.gr/science/article/?aid=438579]

Σπαρτιατική σκυτάλη

Η πρώτη ιστορική καταγραφή κρυπτογραφικής μεθόδου, και μάλιστα με εφαρμογές σε στρατιωτικές επιχειρήσεις, ήταν η *σκυτάλη*. Το μήνυμα γραφόταν σε οριζόντια διεύθυνση σε μια δερμάτινη λουρίδα, που ήταν τυλιγμένη γύρω από τη σκυτάλη, έναν στενό ξύλινο κύλινδρο γνωστό στη σημερινή εποχή από τη σκυταλοδρομία. Στη συνέχεια η λουρίδα ξετυλιγόταν και στελνόταν στον παραλήπτη του μηνύματος. Αν αυτός είχε μια πανομοιότυπη σκυτάλη, με την ίδια διάμετρο, τότε μπορούσε να διαβάσει το μήνυμα τυλίγοντας τη δερμάτινη λουρίδα γύρω της. Το τύλιγμα της λουρίδας σε σκυτάλη διαφορετικής διαμέτρου έδινε μια σειρά ανακατεμένων γραμμάτων σε, φαινομενικά, τυχαία σειρά. Φυσικά ένας υπομονετικός «εχθρός» μπορούσε να δοκιμάζει διαδοχικά σκυτάλες διαφορετικής διαμέτρου, ώσπου να πετύχει τη «σωστή». [http://www.chemist.gr/2012/01/6660]

Τετράγωνο του Πολύβιου

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 φυλάκια (σκοπιές) μεταξύ τους. Ο λόγος που ο Πολύβιος δημιούργησε αυτό τον πίνακα δεν ήταν άλλος παρά να δημιουργήσει μια μέθοδο που θα μπορούσε με απλό σχετικά τρόπο να μεταδώσει πληροφορίες μεταξύ απομακρυσμένων σημείων

ιδιαίτερα αν τα σημεία αυτά είχαν οπτική επαφή (π.χ. δυο πεντάδες από πυρσούς, 2 πεντάδες από χρωματιστές σημαίες κλπ). Η μορφή που είχε ο πίνακας για την Ελληνική γλώσσα είναι ο παρακάτω:

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

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

Ο τρόπος λειτουργίας του πίνακα είναι απλός: κάθε γράμμα αναπαρίσταται από τις συντεταγμένες του στο πίνακα. Έτσι ανάλογα με τη γλώσσα και το μέγεθος του πίνακα που έχουμε επιλέξει κωδικοποιούνται τα γράμματα και ακολούθως οι λέξεις. Η ελληνική λέξη "ΝΙΚΗ" μετασχηματίζεται στη σειρά "33 24 25 22". [Wikipedia]

Ιερογλυφικά

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.

Δίσκος της Φαιστού

Η Κρητική εικονογραφική ή ιερογλυφική γραφή που αναφέρεται παραπάνω εμφανίζεται στον Δίσκο της Φαιστού (Σχήμα 2.2), 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. Ο Δίσκος διαβάζεται σπειροειδώς, δηλαδή από την περιφέρεια προς το κέντρο. Έχει διάμετρο περίπου 16 εκ. με σημεία γραφής και στις δυο όψεις, τα οποία ανέρχονται σε 242 και διαιρούνται σε 61 ομάδες.

Υπάρχουν 45 διαφορετικού χαρακτήρα σημεία στο Δίσκο, περισσότερα για να απαρτίσουν ένα αλφάβητο και λιγότερα για να αποτελέσουν μια πραγματική ιδεογραφική γραφή, όπως συμβαίνει με τα κινέζικα. [http://www.teicrete.gr/daidalika/pages/page.php?page=phaistos_disk]

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. Αναρίθμητες προσπάθειες έχουν γίνει για την αποκρυπτογράφηση του δίσκου της Φαιστού, χρησιμοποιώντας τελείως διαφορετικές μεθόδους και καταλήγοντας σε εντελώς διαφορετικά συμπεράσματα για το σκοπό, το περιεχόμενο του, και τους δημιουργούς του.

Σύμφωνα με την αποκρυπτογράφησή της, το περιεχόμενο του κειμένου είναι θρησκευτικό. Από την 3η π.Χ. χιλιετία ως τα μέσα της 2ας περίπου με κέντρο την Κρήτη άνθισε ένας Αιγαίος πολιτισμός αυτόφωτος και πρωτότυπος, που όμοιό του σε επίπεδο δεν είχε γνωρίσει μέχρι τότε η ανθρωπότητα!

Ποίοι ακριβώς ήσαν, όμως, οι δημιουργοί του Μινωικού πολιτισμού;

Ποία είναι δηλαδή η φυλετική ταυτότητα και η καταγωγή τους, και ποία γλώσσα εν τέλει κρύβεται πίσω από τα μυστηριώδη Κρητικά ιερογλυφικά, την άγνωστη Γραμμική γραφή Α και την κυπρομινωική;

Κάποιοι μελετητές του δίσκου παρατηρώντας τα σύμβολα κατέληξαν σε συμπεράσματα ότι περιγράφονται οι άθλοι του Ηρακλή αλλά παράλληλα συμβολίζεται και εξέλιξη της φύσεως του ανθρώπου.
Μελετώντας τον δίσκο και συγκρίνοντας με μυθολογικά και άλλα γνωστά στοιχεία της ίδιας εποχής προκύπτουν και αναφορές με το άστρο του Κυνός γνωστό και ως Σείριο.
Ο μελετητής του Μινωικού πολιτισμού Λεόν Πομεράνς πιστεύει ότι ο δίσκος δεν είναι γραμμένος σε καμιά γλώσσα αλλά είναι ένα σύστημα αλληγορικών συμβόλων, προερχόμενα ίσως και από τα ζωδιακά, και έτσι χρειαζόμαστε ερμηνεία και όχι μετάφραση. Με αυτή την άποψη τείνουν να συμφωνήσουν και αρκετοί άλλοι.
Ιδιαίτερα ενδιαφέρον βιβλίο σχετικά με το θέμα είναι 'Η Αποκρυπτογράφηση του δίσκου της Φαιστού' του Θεόδωρου Αξιώτη. Περιέχει πάρα πολλά στοιχεία που περιγράφουν τον πολιτισμό πίσω απ' τον δίσκο, βασιζόμενος και αυτός όχι στην μετάφραση αλλά στον αποσυμβολισμό του δίσκου. Παρατηρεί μεγάλη πιθανότητα να περιγράφονται οι άθλοι του Ηρακλή. [http://www.hellinon.net/ProtesGrafes.htm]

Σύμφωνα όμως με τελευταίες ανακοινώσεις του ΤΕΙ Κρήτης η επιγραφική μελέτη του Δίσκου της Φαιστού πρόκειται να έχει ολοκληρωθεί μέχρι το καλοκαίρι, ενώ πλέον υπάρχουν αποδείξεις ότι πρόκειται για μινωική θρησκευτική επιγραφή που πιθανόν, σύμφωνα με τις εκτιμήσεις του κ. Οουεν διευθυντή Γραφείου Διεθνών Σχέσεων του ΤΕΙ Κρήτης,, μιλά για μία θεότητα ή μητέρα. Οπως ανέφερε, ο ίδιος και οι συνεργάτες του μπορούν να διαβάσουν το 90% του δίσκου με φωνητικές αξίες βάσει της Γραμμικής Β. Ωστόσο, δεν γνωρίζουν ακόμη τι γράφει. Ελπίζει το βήμα της αποκρυπτογράφησης να ξεκινήσει μέσα στο καλοκαίρι.

«Στην Κρήτη έχουμε γραφές με ιδεογράμματα και εικονογράμματα πάνω σε σφραγιδόλιθους που χρονολογούνται στο τέλος της 3ης χιλιετίας π.Χ.», είπε ένας κορυφαίος Ελληνας επιγραφολόγος, ο Χαράλαμπος Κριτζάς, σε ομιλία του στο πλαίσιο των μαθημάτων της Αρχαιολογικής Εταιρείας που είναι αφιερωμένα στην Κρήτη.

Ο κ. Κριτζάς σημειώνει πως η λεγόμενη ιερογλυφική γραφή είναι μια συστηματικότερη μορφή γραφής, με κύριο παράδειγμα τον Δίσκο της Φαιστού, που κρατάει

έως σήμερα το μυστήριό του. Τα τελευταία δείγματα της ιερογλυφικής γραφής φθάνουν έως το 1500 π.Χ. «Η Γραμμική Α παρέμεινε σε χρήση μέχρι το 1450 και ένα τουλάχιστον δείγμα της σώζεται σε ένα ειδώλιο με γραπτή επιγραφή που χρονολογείται στα 1375 π.Χ.».

Η γλώσσα στη Γραμμική Α «είναι η μινωική που δεν έχει αποκρυπτογραφηθεί και η μετεξέλιξη της είναι η Γραμμική Β που σχετίζεται με τη μυκηναϊκή παρουσία στην Κρήτη. Τα παλαιότερα δείγματά της έχουν βρεθεί στην Κνωσό και χρονολογούνται στα 1470-1400 π.Χ. και τα νεότερα στην αρχαία Κυδωνία (σημερινά Χανιά), 1250-1200 π.Χ. Η Γραμμική Β αποκρυπτογραφήθηκε το 1952 και είδαμε ότι η γλώσσα που κατέγραφε ήταν η ελληνική σε μια πρώιμη μορφή της». [www.ethnos.gr- Αγγελική Κώττη]

Γραμμική Γραφή

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.

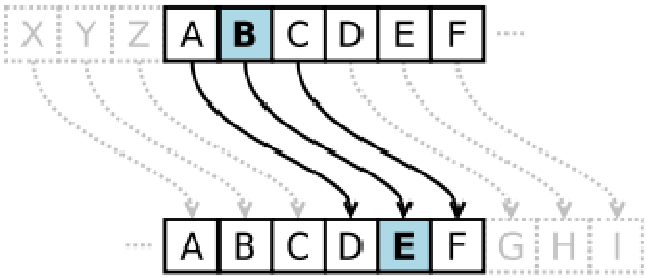
Ο Έβανς κατέγραψε 135 σύμβολα της. Χρησιμοποιήθηκε κυρίως στην Κρήτη, αν και ορισμένα πρόσφατα ευρήματα καταδεικνύουν ότι μπορεί να αποτέλεσε μέσο γραφής και αλλού, αφού επιγραφές με Γραμμική Α έχουν βρεθεί στην Κνωσό και Φαιστό της Κρήτης, αλλά και στη Μήλο και τη Θήρα. Πλάκες με επιγραφές σε γραμμική 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 αποτελούν ένα σύνολο 10.000 τεμαχίων. Τα σχήματα των πινακίδων της γραφής αυτής ποικίλουν, επικρατούν όμως οι φυλλοειδείς και «σελιδόσχημες», οι οποίες διαφέρουν ως προς τις διαστάσεις, ανάλογα με τις προτιμήσεις του κάθε γραφέα. Έπλαθαν πηλό σε σχήμα κυλίνδρου, τον τοποθετούσαν σε λεία επιφάνεια και την πίεζαν μέχρι να γίνει επίπεδη, επιμήκης και συμπαγής πινακίδα, σαφώς διαφοροποιημένη σε δύο επιφάνειες: μία επίπεδη λειασμένη, που επρόκειτο να αποτελέσει την κύρια γραφική επιφάνεια και μία κυρτή, που συνήθως έμενε άγραφη. Πολλές φορές, όταν τα κείμενα απαιτούσαν περισσότερες από μία πινακίδες, έχουμε τις αποκαλούμενες «ομάδες» ή «πολύπτυχα» πινακίδων, οι οποίες εμφανίζουν κοινά χαρακτηριστικά και ως προς την αποξήρανση και το μίγμα του πηλού και κυρίως, ως προς το γραφικό χαρακτήρα του ίδιου του γραφέα. Τα πολύπτυχα αυτά φυλάσσονταν σε αρχειοφυλάκια και ταξινομούνταν κατά θέματα σε ξύλινα κιβώτια. Για να γνωρίζει ο ενδιαφερόμενος το περιεχόμενο των καλαθιών, κυρίως, χρησιμοποιούσαν ετικέτες: ένα σφαιρίδιο πηλού, εντυπωμένο στην πρόσθια πλευρά, στο οποίο καταγράφονταν συνοπτικές πληροφορίες. Συστηματικά, με τη γραφή αυτή, με την οποία είχε πραγματικό πάθος, ασχολήθηκε ο

Άγγλος αρχιτέκτονας και ερασιτέχνης αρχαιολόγος Μ. Βέντρις. Ήταν ο πρώτος που κατάλαβε ότι επρόκειτο για κάποιο είδος ελληνικής γραφής, αλλά η άποψη του αυτή δεν έγινε δεκτή αρχικά από τους ειδικούς. Στη συνέχεια, όμως, αρκετοί προσχώρησαν στην άποψή του. Ένας από αυτούς ήταν ο κρυπταναλυτής Τζον Τσάντγουικ, ο οποίος, στη διάρκεια του πολέμου, είχε εργασθεί στην ανάλυση της γερμανικής κρυπτομηχανής Enigma. Προσπάθησε να μεταφέρει την πείρα του στην κρυπτανάλυση της Γραμμικής Β, αλλά χωρίς επιτυχία μέχρι τότε. Όμως, ο συνδυασμός των δύο επιστημόνων έφερε το πολυπόθητο αποτέλεσμα. Το 1953 κατέγραψαν τα συμπεράσματά τους στο μνημειώδες έργο «Μαρτυρίες για την ελληνική διάλεκτο στα μυκηναϊκά αρχεία», που έγινε το πιο διάσημο άρθρο κρυπτανάλυσης. Η αποκρυπτογράφηση της Γραμμικής Β απέδειξε ότι επρόκειτο για ελληνική γλώσσα, ότι οι Μινωίτες της Κρήτης μιλούσαν ελληνικά και ότι η δεσπόζουσα δύναμη εκείνη την εποχή ήταν οι Μυκήνες. Η αποκρυπτογράφηση της Γραμμικής Β θεωρήθηκε επίτευγμα ανάλογο της κατάκτησης του Έβερεστ, που συνέβη την ίδια ακριβώς εποχή. Για αυτό και έγινε γνωστή σαν το «Έβερεστ της Ελληνικής αρχαιολογίας».

Ο κώδικας του Καισαρα

Ιστορία και χρήση

Ο κώδικας του Καίσαρα πήρε το όνομά του από τον Ιούλιο Καίσαρα, ο οποίος, σύμφωνα με τον Σουητώνιο, τον χρησιμοποιούσε με μετατόπιση τριών θέσεων ώστε να προστατεύσει μηνύματα στρατιωτικής σημασίας. Ενώ η πρώτη καταγεγραμμένη χρήση είναι για τον Καίσαρα, είναι γνωστό ότι χρησιμοποιήθηκαν και άλλοι κώδικες αντικατάστασης νωρίτερα.



Αν είχε κάτι εμπιστευτικό να πει, το έγραφε κωδικοποιημένο, δηλαδή αλλάζοντας την σειρά των γραμμάτων του αλφαβήτου, ώστε ούτε μία λέξη να μην μπορεί να διαβαστεί. Αν οποιοσδήποτε επιθυμεί να τα αποκωδικοποιήσει και να κατανοήσει το νόημα, πρέπει πρώτα να αντικαταστήσει το τέταρτο γράμμα του αλφαβήτου, δηλαδή το D, με το Α και να κάνει το ίδιο με τα υπόλοιπα.

Ο ανηψιός του, Αύγουστος, επίσης χρησιμοποιούσε τον κώδικα, με δεξιά μετατόπιση όμως ενός, και δεν γύριζε στην αρχή του αλφαβήτου:

Όποτε έγραφε κρυπτογραφημένα, έγραφε Β για Α, C για Β, και τα υπόλοιπα γράμματα βάση της ίδιας αρχής, χρησιμοποιώντας όμως ΑΑ στη θέση του Χ.

Υπάρχουν στοιχεία ότι ο Ιούλιος Καίσαρας χρησιμοποιούσε και πιο πολύπλοκα συστήματα, [1]και ένας συγγραφέας, ο Αύλος Γέλλιος, αναφέρεται σε μία (σήμερα χαμένη) διατριβή για την κρυπτογραφία:

Υπάρχει ακόμα μία μάλλον εφευρετικώς γραμμένη διατριβή από τον γραμματικό Πρόβο σχετικά με το μυστικό νόημα των γραμμάτων στη σύνθεση των επιστολών του Καίσαρα.

Είναι άγνωστο το πόσο αποτελεσματικός ήταν ο κώδικας του Καίσαρα τον καιρό του, είναι όμως πιθανό ότι ήταν αρκετά ασφαλής, κυρίως επειδή οι περισσότεροι εχθροί του Καίσαρα ήταν αναλφάβητοι και οι υπόλοιποι θα υπέθεταν ότι τα μηνύματα ήταν γραμμένα σε μία άγνωστη ξένη γλώσσα. Δεν υπάρχουν καταγραφές για τεχνικές λύσης κωδίκων απλής αντικατάστασης. Οι παλαιότερες σωζώμενες καταγραφές χρονολογούνται στον 9ο αιώνα στα έργα του άραβα Αλ Κιντί ο οποίος ανακάλυψε την μέθοδο ανάλυσης συχνοτήτων.

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

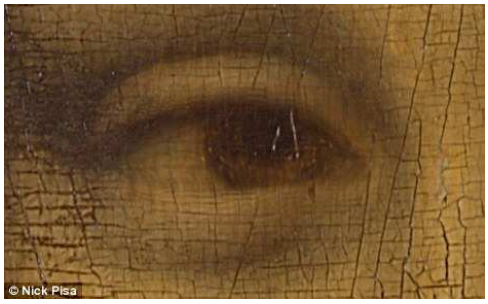
ΚΩΔΙΚΑΣ DA VINCI

Ερευνητές από την Επιτροπή Πολιτιστική Κληρονομιά της Ιταλίας ανακάλυψαν πρόσφατα ότι τα μάτια της Mona Lisa περιέρχουν κάποιον κρυμμένο κώδικα!

Οι ειδικοί ανακάλυψαν με ειδικά όργανα υψηλής ευκρίνειας μικροσκοπικά γράμματα και αριθμούς στα μάτια του διάσημου έργου του Leonardo da Vinci.

Πιστεύουν, επίσης, ότι πρόκειται για έναν μυστικό κώδικα που πιθανόν σύντομα, όταν και αν καταφέρουν να ερμηνεύσουν, να αποκαλύψουν τον πραγματικό κώδικα Da Vinci!

Σύμφωνα με το best seller μυθιστόρημα *Κώδικας Da Vinci* του Dan Brown, η Mona Lisa περιέχει κρυμμένα στοιχεία σχετικά με το Ιερό Δισκοπότηρο. Ο Silvano Vinceti, πρόεδρος της Ιταλικής Εθνικής Επιτροπής Πολιτιστικής Κληρονομιάς που εντόπισε τα κρυμμένα σύμβολα, είπε: «Τα κρυμμένα αυτά σύμβολα δε φαίνονται με γυμνό μάτι, αλλά με ένα ειδικό γυαλί φαίνονται πολύ καθαρά».



Στο δεξί μάτι εμφανίζονται τα γράμματα LV (διπλανή εικόνα) τα οποία πιθανόν συμβολίζουν τα αρχικά του Leonardo da Vinci, ενώ στο αριστερό μάτι υπάρχουν κάποια άλλα σύμβολα τα οποία δε φαίνονται πολύ καθαρά.

«Είναι πολύ δύσκολο να τα διακρίνει κανείς, αλλά πιθανόν είναι τα γράμματα CE ή το γράμμα B. Στο πίσω μέρος διακρίνονται το νούμερο 72 ή το γράμμα L και ο αριθμός 2″.

«Μη ξεχνάμε ότι η ζωγραφιά είναι ηλικίας 500 ετών, γι αυτό δεν είναι πολύ εμφανής και καθαρή όπως ήταν όταν πρωτοδημιουργήθηκε».

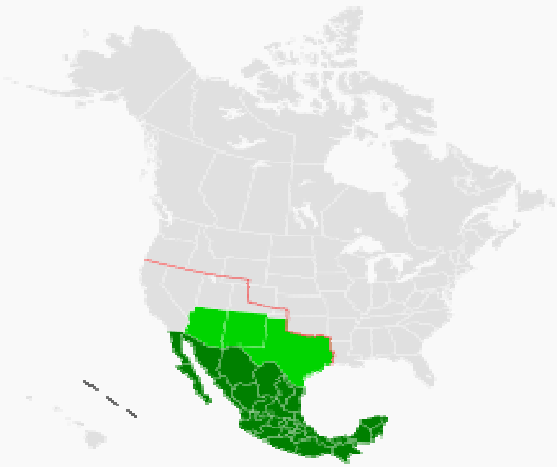
2η περιοδος κρυπτογραφησης

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.

Zimmermann Τηλεγράφημα

Από τη Βικιπαίδεια, την ελεύθερη εγκυκλοπαίδεια

Το τηλεγράφημα του Zimmermann όπως στάλθηκε από την Ουάσιγκτον προς τον Πρέσβη Heinrich von Eckardt (ο οποίος ήταν ο Γερμανός πρεσβευτής στο Μεξικό).



Το **Τηλεγράφημα Zimmermann** ήταν ένα σημείωμα-διπλωματική πρόταση της Γερμανικής Αυτοκρατορίας προς το Μεξικό για να ενταχθούν στην Κεντρικές Δυνάμεις . Το μήνυμα ήρθε ως κωδικοποιημένο τηλεγράφημα το οποίο αποστέλλεται από τον Υπουργό Εξωτερικών της Γερμανικής Αυτοκρατορίας, Arthur Zimmermann , στις 16 Ιανουαρίου 1917. Το μήνυμα στάλθηκε στον Γερμανό πρέσβη στο Μεξικό, Heinrich von Eckardt . Ο Zimmermann έστειλε το τηλεγράφημα εν αναμονή της απρόσκοπτης αποστολής υποβρυχίων από τη Γερμανία την 1η Φεβρουαρίου, μια πράξη η οποία προέβλεψε ότι η Γερμανία θα ήθελε να επιστήσει την ουδέτερη ΗΠΑ σε πόλεμο στο πλευρό των Συμμάχων . [1] Το τηλεγράφημα έδινε εντολή στον πρέσβη Eckardt ότι εάν φαινόταν πιθανό να μπουν οι ΗΠΑ στον πόλεμο, να προσεγγίσει τη μεξικανική κυβέρνηση με πρόταση για στρατιωτική συμμαχία, με χρηματοδότηση από τη Γερμανία. Η Γερμανία είχε υποσχεθεί στο Μεξικό το Τέξας , το Νέο Μεξικό και την Αριζόνα που είχαν χαθεί από τις Ηνωμένες Πολιτείες. Στον Eckardt επίσης δόθηκε εντολή να παροτρύνει το Μεξικό για μια συμμαχία ανάμεσα στη Γερμανία και την Ιαπωνική Αυτοκρατορία . Το Μεξικό, που δεν μπορούσε να ταιριάξει με το στρατό των ΗΠΑ, αγνόησε την πρόταση και αφού οι ΗΠΑ μπήκαν στον πόλεμο, απέρριψε επίσημα την πρόταση των Γερμανών.

Μηχανή Enigma

Μια βελτίωση της μεθόδου αντικατάστασης ήταν οι κρυπτογραφικές μηχανές των Γερμανών κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου. Οι μηχανές αυτές χρησιμοποιούσαν διαδοχικούς δίσκους για την αντικατάσταση των γραμμάτων. Ετσι, για παράδειγμα, το γράμμα «α» αντικαθίσταται από τον πρώτο δίσκο με το «ζ», το «ζ» με τον δεύτερο με το «π» κ.ο.κ. Η θέση των δίσκων άλλαζε με κάθε αντικατάσταση, έτσι ώστε η αποκρυπτογράφηση να γίνεται εξαιρετικά δύσκολη με στατιστική ανάλυση.

Με αυτό τον τρόπο δούλευε η μηχανή Enigma

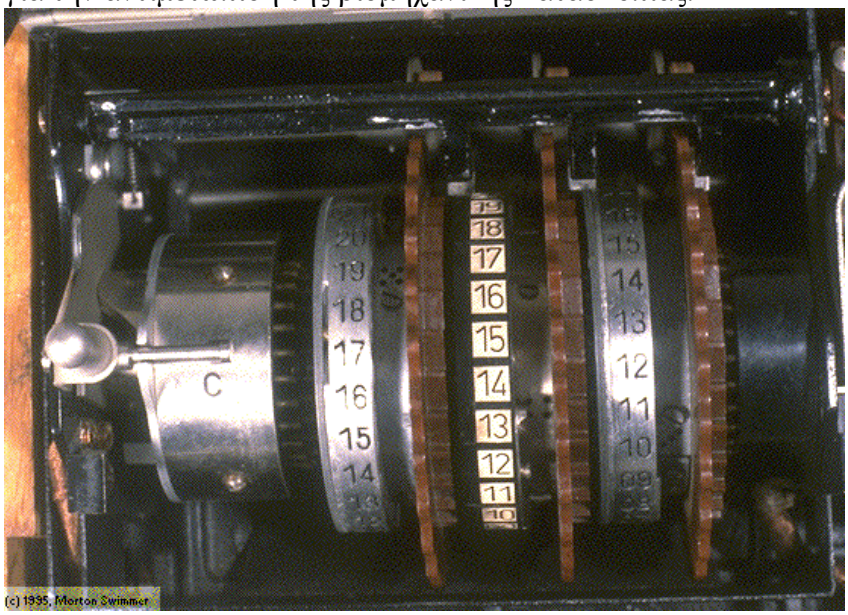
Από τη Wikipedia, την ελεύθερη εγκυκλοπαίδεια

Η πρώτη συσκευή Enigma εφευρέθηκε από τον Γερμανό μηχανικό **Arthur Scherbius** στο τέλος του Πρώτου Παγκοσμίου Πολέμου. Αυτό το μοντέλο και οι παραλλαγές του χρησιμοποιήθηκαν εμπορικά από της αρχές της

δεκαετίας του 1920 και υιοθετήθηκαν από στρατιωτικές και κυβερνητικές υπηρεσίες από διάφορες χώρες, πιο αξιοσημείωτα από την Ναζιστική Γερμανία πριν και κατά τη διάρκεια του Δευτέρου Παγκοσμίου Πολέμου.

Αρκετά διαφορετικά μοντέλα συσκευών Enigma παρήχθησαν, αλλά τα Γερμανικά στρατιωτικά μοντέλα, τα **Wehrmacht Enigmas**, είναι τα πιο πολυσυζητημένα

Το όνομα της Γερμανικής κρυπτογραφικής μηχανής ήταν «Enigma». Η πρώτη απο αυτές παρήχθη το 1923 στη Γερμανία απο τον 45χρονο μηχανικό Αρθουρ Σέρμπιους και διατίθεντο αρχικά απο τον όμιλο κρυπτογραφικών μηχανών του Βερολίνου στην τιμή των 350 μάρκων. Αρχικά είχε σχεδιαστεί για την αντιμετώπιση της βιομηχανικής κατασκοπίας.

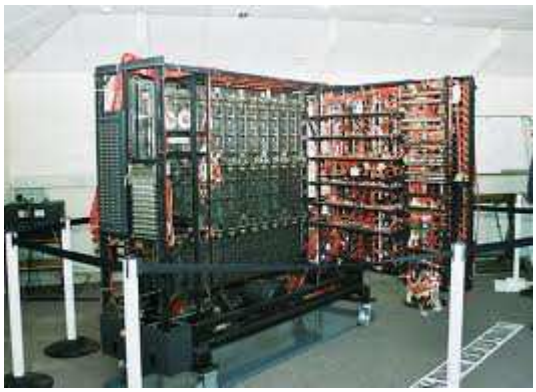


Το σύστημα της Enigma το οποίο αποτελείτο από τρεις στροφείς μπορούσε να παράσχει 17.576 κρυπτογραφημένα αλφάβητα. Μεταγενέστερες εκδόσεις ανέβαζαν

αυτόν τον αριθμό σε 456.976! Για να λάβει κανείς μήνυμα μέσω της Enigma θα έπρεπε όχι μόνο να διαθέτει τη συσκευή αλλά και να γνωρίζει ποιον στροφέα να εισάγει στη μηχανή, με ποια σειρά αλλά και την προρύθμιση του καθενός. Μεταγενέστερες καινοτομίες ανέβαζαν τους πιθανούς συνδυασμούς του μηχανήματος σε αστρονομικά ύψη, καθιστώντας το έτσι πρακτικά απαραβίαστο. Για να σπάσει την κρυπτογραφική κωδικοποίηση της μηχανής κάποιος κατάσκοπος που δεν γνώριζε τις ρυθμίσεις της, θα έπρεπε να δοκιμάσει 22 δισεκατομμύρια συνδυασμούς σύνδεσης στροφέων και ηλεκτρικών συνδέσεων. Δικαιολογημένα έτσι ο επινοητής της μηχανής καυχιόταν πως «αν κάποιος εργαζόταν μέρα και νύχτα δοκιμάζοντας έναν διαφορετικό κωδικό για κάθε λεπτό της ώρας, θα χρειαζόταν 42.000 χρόνια για να δοκιμάσει όλους τους πιθανούς κωδικούς. [

http://www.ww2.gr/index.php?option=articles&search=Enigma]

Το σπάσιμο των κωδικών της μηχανής Enigma



Το σπάσιμο των κωδικών της μηχανής Enigma δεν ήταν καθόλου απλή υπόθεση και είχε ξεκινήσει χρόνια νωρίτερα.

Στην Πολωνία ο Marian Rejewski, παραβίασε την πρώτη μορφή του συστήματος Enigma χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ο Rejewski είχε κατασκευάσει μια ηλεκτρομηχανική συσκευή που αποκρυπτογραφούσε τα μηνύματα της Enigma από τον Οκτώβριο του 1938, την οποία είχε επονομάσει “Bomba” λόγω θορύβου. Οι Πολωνοί συνέχισαν να παραβιάζουν τα μηνύματα που βασιζόταν στην κρυπτογράφηση με τον Enigma μέχρι το 1939. Τότε ο Γερμανικός στρατός έκανε κάποιες αλλαγές και οι Πολωνοί δεν μπόρεσαν να ακολουθήσουν γιατί η παραβίαση 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

Με τη βοήθεια των Πολωνών οι Γάλλοι έστησαν μια επιχείρηση αποκρυπτογράφησης στα περίχωρα του Παρισιού που επονομάστηκε “PC Bruno” , αλλά λόγω της κατάληψης της Γαλλίας, αυτή άντεξε μέχρι τις 9 Ιουνίου 1940. Στις πληροφορίες που πήραν οι Βρετανοί περιλαμβανόταν και μια απομίμηση της συσκευής Enigma και έτσι απέκτησαν πλέον το απαιτούμενο υπόβαθρο για τη μελέτη και την επινόηση τρόπων αποκρυπτογράφησης των Γερμανικών μηνυμάτων: Μπορούσαν να κατανοήσουν τη λειτουργία της, να μελετήσουν τον τρόπο καλωδίωσης των στροφέων (rotors). Αυτό που έλειπε ήταν οι ρυθμίσεις που άλλαζαν καθημερινά: Ποια ήταν η ακολουθία και ο αρχικός προσανατολισμός των αρχικά τριών στροφέων και ποια βύσματα είχαν τοποθετηθεί στον αντίστοιχο πίνακα. Ο Ρεγιέβσκι είχε ασφαλώς κατανοήσει τον τρόπο λειτουργίας της Enigma και κατάφερε να βρει τον τρόπο καλωδίωσης των στροφέων. Απέμενε στους Βρετανούς να λύσουν το τρίτο πρόβλημα, κάτι που κατάφεραν στις αρχές του 1940. Ωστόσο, τα κωδικοποιημένα μηνύματα ήταν πολλά και σε καθημερινή βάση, απαιτώντας την ταχύτερη αποκρυπτογράφηση προκειμένου το περιεχόμενό τους να είναι χρησιμοποιήσιμο. Αναφέρεται ότι ο μέσος όρος μηνυμάτων που κατέγραφαν οι σταθμοί ακροάσεως ήταν 3.000 την ημέρα. Βασιζόμενος στην ιδέα του Rejewski, ο Άλαν Τούρινγκ σχεδίασε τη δική του μηχανή, η οποία μπορούσε να δοκιμάζει συνδυασμούς γραμμάτων σε χρόνο που ήταν

αδύνατο να επιτευχθεί από οποιοδήποτε άνθρωπο ή ομάδα ανθρώπων. Μετά από συνεχείς βελτιώσεις η μηχανή άρχισε να χρησιμοποιείται από τα μέσα Αυγούστου 1940. Η μηχανή αυτή ονομάστηκε the bombe και χρησιμοποιήθηκε απέναντι στη μηχανή Enigma.

Αν και το Enigma είχε κάποιες κρυπτογραφικές αδυναμίες, στην πράξη αυτές αυτό ήταν αποτέλεσμα σε συνδυασμό με τις διαδικαστικές ατέλειες, τα λάθη των χειριστών ή τα σφάλματα υλικού. Η ακριβής επιρροή της Ultra στην πορεία του πολέμου αξιολογείται διαφορετικά. Η αποκρυπτογράφηση των γερμανικών αλγόριθμων κρυπτογράφησης επιτάχυνε το τέλος του ευρωπαϊκού πολέμου κατά δύο έτη, ενώ ο Winston Churchill είπε στον βασιλιά της Βρετανίας George VI μετά τον πόλεμο "Ήταν χάρη στην Ultra ότι κερδίσαμε τον πόλεμο".

ΚΩΔΙΚΑΣ ΝΑΒΑΧΟ

Κατά τη διάρκεια του Β Παγκόσμιου Πόλεμου στις μάχες του Ειρηνικού, οι Ιάπωνες κατάφερναν διαρκώς να σπάνε τα κρυπτογραφημένα μηνύματα, προκαλώντας σημαντικές απώλειες στη στρατιωτική μηχανή των ΗΠΑ. Η λύση βρέθηκε το 1942. Το Πεντάγωνο στρατολόγησε εκατοντάδες ινδιάνους Ναβάχο οι οποίοι εκπαιδεύτηκαν να χρησιμοποιούν έναν μυστικό στρατιωτικό κώδικα επικοινωνίας βασισμένο στη μητρική τους γλώσσα. Ο κώδικας των Ναβάχο ήταν τελικά ο μοναδικός που δεν κατάφεραν να σπάσουν ποτέ οι Γιαπωνέζοι και θεωρείται ότι έπαιξε καθοριστικό ρόλο στην εξέλιξη του πολέμου. Το 2002 γυρίστηκε η ταινία Windtalkers: Ο Κώδικας Των Νάβαχο βασισμένη στην ιστορία της σγτρατολόγησης των Ναβάχο. [http://cinema.pathfinder.gr/movies/793806]

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.

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.

3η περίοδος κρυπτογράφησης

Η κρυπτογραφία στις μέρες μας

Κρυπτογραφια και υπολογιστες

Η τεράστια ανάπτυξη των δικτύων υπολογιστών και η επικοινωνία πληροφοριών κάθε μορφής έφερε ένα τεράστιο πρόβλημα στην επιφάνεια, την ανάγκη για προστασία αυτής της πληροφορίας.

Κρυπτογράφηση (encryption) είναι ο μετασχηματισμός των δεδομένων σε μορφή που δεν μπορεί να διαβαστεί από κανένα παρά μόνο από αυτόν που διαθέτει ένα κατάλληλο κλειδί. Υπάρχουν δύο

μεγάλες οικογένειες αλγόριθμων κρυπτογράφησης, οι συμμετρικοί αλγόριθμοι (ή αλγόριθμοι μυστικού κλειδιού) και οι ασύμμετροι (ή αλγόριθμοι δημόσιου κλειδιού).

Συμμετρικοί αλγόριθμοι
Στους συμμετρικούς αλγόριθμους το κλειδί κρυπτογράφησης μπορεί να υπολογιστεί από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση και το ανάποδο. Μάλιστα στις περισσότερες περιπτώσεις τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης είναι τα ίδια. Αυτοί οι αλγόριθμοι χρειάζονται την συμφωνία μεταξύ του αποστολέα και του παραλήπτη για το κλειδί που θα χρησιμοποιηθεί, για να μπορέσουν να επικοινωνήσουν με ασφάλεια. Η ασφάλεια των αλγόριθμων βασίζεται στην μυστικότητα αυτού του κλειδιού. Για όσο καιρό επιθυμούμε η επικοινωνία να παραμείνει μυστική, για τον ίδιο καιρό πρέπει και το κλειδί να παραμείνει μυστικό.

Οι συμμετρικοί αλγόριθμοι μπορούν να διαιρεθούν σε δύο υποκατηγορίες: α) αλγόριθμοι ροής (stream ciphers) οι οποίοι λειτουργούν bit προς bit και β) μπλοκ αλγόριθμοι (block ciphers) οι οποίοι λειτουργούν πάνω σε κομμάτια δεδομένων (συνήθως των 64 bit).

Παραδείγματα συμμετρικών αλγορίθμων είναι οι DES, IDEA, RC5 και SAFER.

Ασύμμετροι αλγόριθμοι

Οι ασύμμετροι αλγόριθμοι ή αλγόριθμοι δημόσιου κλειδιού είναι σχεδιασμένοι έτσι ώστε το κλειδί που χρησιμοποιείται για την κρυπτογράφηση να είναι διαφορετικό από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση. Πέρα από αυτό, το κλειδί αποκρυπτογράφησης δεν μπορεί να υπολογιστεί από το κλειδί κρυπτογράφησης. Οι αλγόριθμοι αυτοί καλούνται και "δημόσιου κλειδιού" γιατί το κλειδί κρυπτογράφησης μπορεί να δημοσιοποιηθεί. Ο καθένας μπορεί να κρυπτογραφήσει ένα μήνυμα με το δημόσιο κλειδί αλλά μόνο αυτός που διαθέτει το αντίστοιχο ιδιωτικό κλειδί μπορεί να το αποκρυπτογραφήσει.

Παραδείγματα ασύμμετρων αλγορίθμων είναι οι RSA, ElGamal και DSA.

Οι συμμετρικοί αλγόριθμοι είναι πολύ πιο γρήγοροι, εφαρμοσμένοι είτε σε υλικό είτε σε λογισμικό. από τους ασύμμετρους αλγόριθμους. Ως εκ τούτου οι συμμετρικοί αλγόριθμοι χρησιμοποιούνται για την κρυπτογράφηση του κυρίου μέρους των δεδομένων, ενώ οι αλγόριθμοι δημόσιου κλειδιού βρίσκουν κατάλληλη εφαρμογή σε πρωτόκολλα ανταλλαγής κλειδιών και ψηφιακών υπογραφών.

Διαχείριση κλειδιού

Η διαχείριση του κλειδιού είναι η διαδικασία παραγωγής, διανομής, επαλήθευσης, χρησιμοποίησης, ενημέρωσης, αποθήκευσης και καταστροφής κλειδιών σε ένα σύστημα κρυπτογράφησης. Η ασφαλής μέθοδος διαχείρισης των κλειδιών είναι πάρα πολύ σημαντική. Στην πράξη οι περισσότερες επιθέσεις σε συστήματα ασφαλείας έχουν ως στόχο τις διαδικασίες διαχείρισης των κλειδιών και όχι τους ίδιους τους αλγόριθμους.

Οι αλγόριθμοι δημόσιου κλειδιού καθιστούν την διαχείριση πολύ πιο εύκολη. Το ιδιωτικό κλειδί δεν χρειάζεται να μεταδοθεί ποτέ. Βέβαια παρουσιάζεται ένα πρόβλημα ο κάθε χρήστης πρέπει να διαθέτει ένα δικό τους ζεύγος κλειδιών. Στα συστήματα που χρησιμοποιούν ασύμμετρη κρυπτογραφία χρειάζονται μέθοδοι διανομής και επαλήθευσης κλειδιών. Τα πρωτόκολλα CCITT X.509 παρέχουν κανόνες για τις διαδικασίες αυτές.

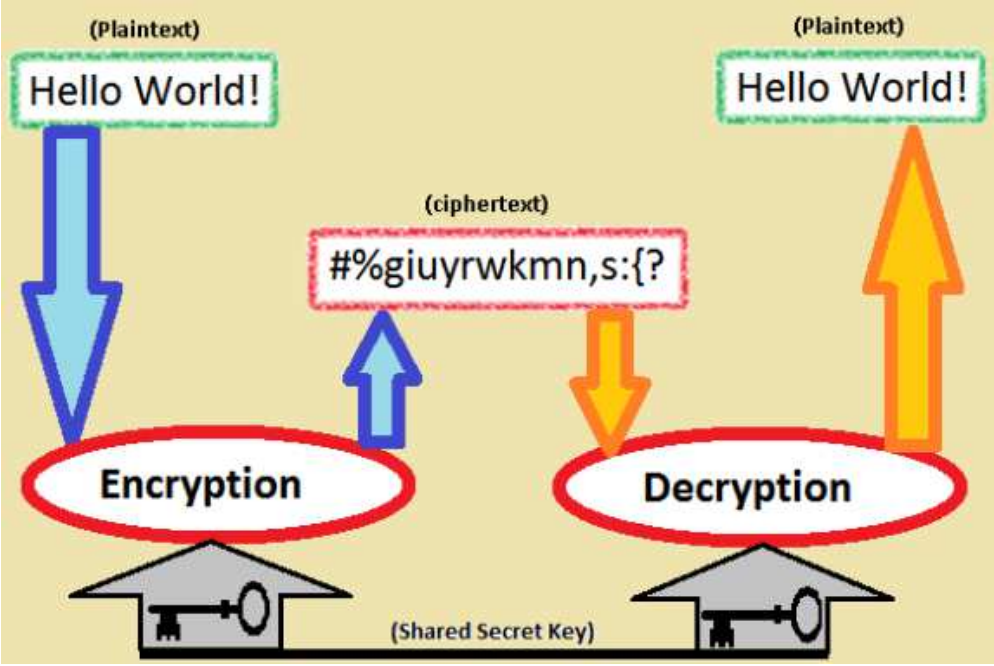
Πρωτόκολλα

Ένα πρωτόκολλο είναι μια σειρά κανόνων που πρέπει να ακολουθηθούν για την εκτέλεση μιας δεδομένης εργασίας. Τα πρωτόκολλα ασφάλειας δεδομένων συχνά περιέχουν την χρήση κάποιων αλγορίθμων κρυπτογράφησης αλλά σε γενικές γραμμές αυτό που προσπαθούν να επιτύχουν δεν είναι μόνο η μυστικότητα αλλά και να παρέχουν όλες τις βασικές υπηρεσίες ασφαλείας που αναφέρθηκαν.

Η κρυπτογράφηση δεδομένων στους υπολογιστές

Σήμερα, κάθε κρυπτογράφηση δεδομένων βασίζεται σε υπολογιστές.

Πολύ απλά, όποιον αλγόριθμο κι αν επινοήσει κάποιος άνθρωπος, όσο περίπλοκος κι αν είναι, είναι υπερβολικά εύκολο να τον σπάσει ένας κατάλληλα προγραμματισμένος υπολογιστής.



Η κρυπτογράφηση δεδομένων μέσω υπολογιστή γενικά ανήκει σε δύο κατηγορίες:

- Symmetric key encryption (συμμετρικό κλειδί)
- Public key ή Asymmetric key encryption (Δημόσιο κλειδί)

Symmetric key encryption- Συμμετρικό κλειδί

Στην κρυπτογράφηση symmetric key, όπως και οι Σπαρτιάτες στρατηγοί, και οι δύο υπολογιστές που επικοινωνούν χρειάζεται να έχουν το ίδιο κλειδί κρυπτογράφησης.

Στην περίπτωση των υπολογιστών το κλειδί είναι ένας αριθμητικός κωδικός, το μέγεθος του οποίου ορίζεται από το πόσα bits τον αποτελούν.

Ο πρώτος σημαντικός αλγόριθμος για κρυπτογράφηση δεδομένων μέσω υπολογιστή ήταν ο Data Encryption Stantard (DES) που αναπτύχθηκε από την IBM στις ΗΠΑ και εγκρίθηκε για χρήση το 1970.

Ο DES χρησιμοποιεί κλειδί μήκους 56-bit, που διαθέτει πάνω από 72 τετράκις εκατομμύρια πιθανούς συνδυασμούς (72.057.594.037.927.936, για την ακρίβεια).

Μπορεί να ακούγονται ατέλειωτοι, όμως το 1998 δημιουργήθηκε η συσκευή EFF DES cracker ("Deep Crack"), με ειδικά κατασκευασμένα τσιπάκια, που επέτρεπαν σε έναν υπολογιστή να δοκιμάσει 90 δισεκατομμύρια κλειδιά το δευτερόλεπτο.

Θεωρητικά, θα χρειάζονταν 9 ημέρες για να δοκιμάσει κάθε πιθανό συνδυασμό.

Στην πράξη, ο Deep Crack κατάφερε να σπάσει τον DES σε δύο ξεχωριστά τεστ, στο πρώτο σε 56 ώρες και στο δεύτερο σε 22 ώρες, αποδεικνύοντας πως ο συγκεκριμένος αλγόριθμος είναι ανεπαρκής για την κρυπτογράφηση δεδομένων σε πραγματικές συνθήκες.

Πλέον, ο DES έχει αντικατασταθεί από τον αλγόριθμο Advanced Encryption Standard (AES), που χρησιμοποιεί κλειδιά 128, 192 ή 256-bit.

Με την αύξηση των bit, οι πιθανοί συνδυασμοί ανεβαίνουν εκθετικά. Ένα κλειδί 128-bit μπορεί να έχει πάνω από 300.000.000.000.000.000.000.000.000.000.000.000 πιθανούς συνδυασμούς.

Ο μεγαλύτερος υπερυπολογιστής αυτή τη στιγμή στον κόσμο, που μπορεί να εκτελέσει 33,86 petaflop/s (τετράκις εκατομμύρια υπολογισμούς το δευτερόλεπτο) και θα μπορούσε θεωρητικά να σπάσει τον DES σε 2 δευτερόλεπτα, θα χρειαζόταν περίπου 250 δισεκατομμύρια χρόνια για να ελέγξει όλους τους συνδυασμούς του AES-128.

Γνωστοί Αλγόριθμοι Symmetric key encryption

Εκτός από τον AES που προαναφέραμε, άλλοι γνωστοί αλγόριθμοι Symmetric key που χρησιμοποιούνται ευρέως για την κρυπτογράφηση δεδομένων είναι οι RC4, 3DES, IDEA, CAST5, Twofish, Serpent, Blowfish.

Public/asymmetric key encryption – Δημόσιο κλειδί

Υπάρχει ένα σημαντικό πρόβλημα με την κρυπτογράφηση δεδομένων μέσω της μεθόδου symmetric key, ανεξαρτήτως αλγόριθμου, ειδικά όσον αφορά τη χρήση της στο Internet.

Το πρόβλημα είναι πως αν κάποιος θέλει να μας στείλει κάτι κρυπτογραφημένο με αυτή τη μέθοδο, για να το ανοίξουμε πρέπει με κάποιο τρόπο να μας στείλει και ένα αντίγραφο του κλειδιού.

Αν όμως μας στείλει το κλειδί μέσω του Internet, που είναι ένα δημόσιο δίκτυο, θα μπορούσε οποιοσδήποτε να το υποκλέψει κατά την αποστολή, και να έχει πρόσβαση στα κρυπτογραφημένα δεδομένα.

Αυτό το πρόβλημα λύνει η μέθοδος Public/asymmetric key encryption.

Ουσιαστικά, σε αυτή τη μέθοδο κρυπτογράφησης υπάρχουν δύο κλειδιά:

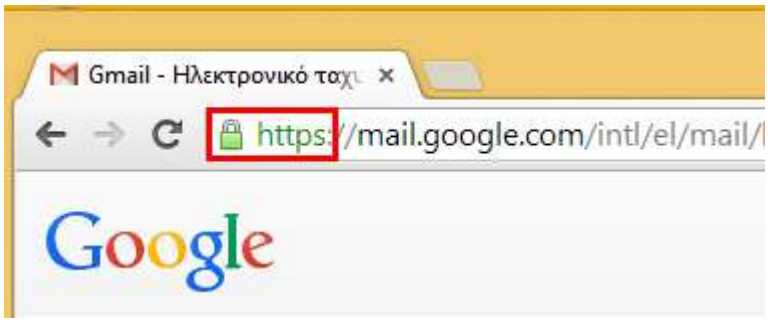
- Το Public key, είναι δημόσιο και μπορεί να το χρησιμοποιήσει οποιοσδήποτε για την κρυπτογράφηση δεδομένων.
- Το Private Key που είναι μυστικό. Συνδέεται μαθηματικά με το Public key και είναι απαραίτητο για την αποκρυπτογράφηση.

Γνωστοί Αλγόριθμοι Public/Asymmetric key encryption

Ο ποιο γνωστός αλγόριθμος Public/Asymmetric key όσον αφορά το Internet είναι ο RSA, την ακριβή λειτουργία του οποίου θα αναλύσουμε παρακάτω..

Από εκεί και πέρα, γνωστές και διαδεδομένες τεχνικές public/asymmetric key για διάφορες εφαρμογές είναι το πρωτόκολλο ανταλλαγής κλειδιών Diffie-Hellman, το Digital Signature Standard που περιλαμβάνει τον Digital Signature Algorithm, η κρυπτογράφηση ElGamal, το σύστημα Paillier, το σύστημα Cramer-Shoup και το πρωτόκολλο YAK.

Πως υλοποιείται η κρυπτογράφηση δεδομένων στο Internet



Το κύριο πρωτόκολλο κρυπτογράφησης του Internet είναι το Transport Layer Security (TLS), που είναι ο διάδοχος του Secure Socket Layer (SSL). Είναι το πρωτόκολλο που ακολουθείται όποτε μπαίνουμε σε μια σελίδα που ξεκινάει με https:// και με λουκέτο.

Να σημειωθεί πως το TLS δεν είναι το ίδιο ένας αλγόριθμος κρυπτογράφησης. Είναι το πρωτόκολλο που υπαγορεύει τα βήματα που πρέπει να ακολουθηθούν για να πραγματοποιηθεί μια ασφαλής σύνδεση.

Τα βήματα αυτά συμπεριλαμβάνουν, μεταξύ άλλων:

- ποια στοιχεία χρειάζεται να ανταλλάξουν ο υπολογιστής μας και ο server πριν δημιουργηθεί η ασφαλής σύνδεση
- ποιος αλγόριθμος Public/Asymmetric key θα χρησιμοποιηθεί και για την κρυπτογράφηση ποιών δεδομένων.
- ποιος αλγόριθμος θα χρησιμοποιηθεί για το Symmetric key
- Πόσο διάστημα θα διαρκέσει η σύνδεση (session) πριν χρειαστεί να ανανεωθεί

Επίσης, ο TSL ορίζει και ένα επιπλέον μέτρο ασφαλείας, που ονομάζεται Digital Certificate.

Digital Certificate

Υπάρχουν κάποιες εταιρείες που ονομάζονται Certificate Authorities, όπως πχ η VeriSign, η DigiCert, το Comodo Group, και άλλες.

Οι εταιρείες αυτές εκδίδουν ένα ψηφιακό πιστοποιητικό (Digital Certificate). Ουσιαστικά πρόκειται για ένα μοναδικό κομμάτι κώδικα που επιβεβαιώνει πως ένα συγκεκριμένο Public key ανήκει σε μια συγκεκριμένη ιστοσελίδα και μια συγκεκριμένη επιχείρηση.

Έτσι, είναι αδύνατον κάποιος να πλαστογραφήσει πχ το Public key του Facebook. Εφόσον υπάρχει το https:// και το λουκέτο, βρισκόμαστε στο πραγματικό facebook...

...και όχι κάποια ψεύτικη σελίδα που παριστάνει πως είναι το Facebook για να κλέψει τον κωδικό μας.

Αν μπούμε σε κάποια ιστοσελίδα με https:// αλλά χωρίς Digital Certificate από κάποια Certificate Authority, ο browser θα μας προειδοποιήσει.

Στα πλαίσια της ερευνητικής εργασίας οι τέσσερις ομάδες των μαθητών πήραν από μια από τις παρακάτω τέσσερις σελίδες και αποκρυπτογράφησαν το μήνυμα. Σημαντικό λόγο στην αποκρυπτογράφηση έπαιξε η συνεργασία μεταξύ των ομάδων. Έτσι ενώ κάθε ομάδα από μόνη της δε μπορεί να αποκρυπτογραφήσει το μήνυμα όταν συνεργάστηκαν όλες μαζί κατάφεραν να βρουν τη φράση.

Κωδικοποιημένη λέξη

Οδηγίες
Κάθε ομάδα είναι μέλος μιας μεγαλύτερης ομάδας
Καθένας μόνος του δε μπορεί να τα καταφέρει όλα
Κάθε σύμβολο σημαίνει πάντα το ίδιο
Το θερμόμετρο βρίσκεται πάντα στην αρχή …
Το αεροπλάνο κάποιοι δε μπορούν να το προφέρουν…

Επίσης:

	σ
	η
	γ
	ι

Κωδικοποιημένη λέξη

Οδηγίες
Κάθε ομάδα είναι μέλος μιας μεγαλύτερης ομάδας
Καθένας μόνος του δε μπορεί να τα καταφέρει όλα
Κάθε σύμβολο σημαίνει πάντα το ίδιο
Το θερμόμετρο βρίσκεται πάντα στην αρχή …
Το αεροπλάνο κάποιοι δε μπορούν να το προφέρουν…

Επίσης

	τ
	φ
	κ

Κωδικοποιημένη λέξη-λεξεις

Οδηγίες
Κάθε ομάδα είναι μέλος μιας μεγαλύτερης ομάδας
Καθένας μόνος του δε μπορεί να τα καταφέρει όλα
Κάθε σύμβολο σημαίνει πάντα το ίδιο
Το θερμόμετρο βρίσκεται πάντα στην αρχή …
Το αεροπλάνο κάποιοι δε μπορούν να το προφέρουν…

Επίσης

	ε
	ν

Κωδικοποιημένη λέξη-λεξεις

Οδηγίες
Κάθε ομάδα είναι μέλος μιας μεγαλύτερης ομάδας
Καθένας μόνος του δε μπορεί να τα καταφέρει όλα
Κάθε σύμβολο σημαίνει πάντα το ίδιο
Το θερμόμετρο βρίσκεται πάντα στην αρχή …
Το αεροπλάνο κάποιοι δε μπορούν να το προφέρουν…

Επίσης

	υ
	λ
	χ

Εργάστηκαν οι μαθητές:

Καρμίρης Δημήτρης
Καραγιάννης Νίκος
Ξενίδης Κων/νος
Μουστάκας Σωκράτης
Φωτίου Σπύρος
Παπαγεωργίου Γιώργος
Πρακατέ Δήμητρα
Σαχίνι Σολιόν
Βελώνης Ιάσονας
Λάλος Γιώργος
Νάκας Στέλιος
Παρλάτζας Γιώργος
Παπαχρήστος Ευθύμιος
Μπατσίλα Αικατερίνη
Βαίτση Θεοδώρα
Χατζή Ελένη

Βιβλιογραφία

- http://www.pcsteps.gr/
- http://cinema.pathfinder.gr
- http://www.ww2.gr
- www.ethnos.gr
- http://www.pcsteps.gr/
- http://www.hellinon.net
- http://www.teicrete.gr/
- Wikipedia
- http://www.chemist.gr
- http://www.tovima.gr
- [http://diktya-epal-g.ggia.info/wp-content/uploads/Kefalaio_8_Diaxeirish_kai_asfaleia_diktyou_8_3_4_Texnikes_Asfaleias_Symmetrikh_Asymmetrikh_Kryptografish_Pshfiakes_Ypografes.pdf]
- ΤΟ ΒΗΜΑ
- Ελληνική Αγωγή
- Ίδρυμα Μείζονος Πολιτισμού