ΤΙΤΛΟΣ ΕΡΕΥΝΗΤΙΚΗΣ ΕΚΘΕΣΗΣ

ΚΩΔΙΚΕΣ

Υπόθεμα: «ΚΡΥΠΤΟΓΡΑΦΙΑ»

ΤΑ ΜΕΛΗ ΤΗΣ ΟΜΑΔΑΣ

ΦΩΤΕΙΝΟΥ ΑΝΔΡΙΑΝΑ
ΣΟΦΟΛΟΓΗ ΑΡΕΤΗ
ΣΠΑΡΤΑΛΗΣ ΝΙΚΟΣ
ΜΕΜΟΣ ΝΙΚΟΣ

Επιβλέπουσα καθηγήτρια: Καλλιόπη Μαγδαληνού, ΠΕ19

ΛΙΓΑ ΛΟΓΙΑ…

Η δική μας ομάδα αποτελείται από τέσσερα μέλη, τους Μέμος Νίκος, Σοφολόγη Αρετή, Σπάρταλης Νικόλας και Φωτεινού Αδριάνα, και ασχολήθηκε με την κρυπτογραφία. Ερευνήσαμε τον όρο της κρυπτογραφίας, αναλύσαμε τη χρησιμότητα της, μοιράσαμε ερωτηματολόγια για την καταμέτρηση στατιστικών και τέλος βρήκαμε στοιχεία για τους κρυπτογραφημένους κωδικούς και για την χρησιμοποίηση της στα πλαίσια του ηλεκτρονικού εμπορίου.

ΟΡΙΣΜΟΣ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Κρυπτογραφία είναι ένα διεπιστημονικό γνωστικό πεδίο, που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης. Σκοπός της είναι η απόκρυψη του περιεχομένου των μηνυμάτων για ασφαλή επικοινωνία (πχ ανθρώπων, προγράμματα υπολογιστών).

ΤΑ ΚΥΡΙΟΤΕΡΑ ΕΥΡΗΜΑΤΑ ΤΗΣ ΕΡΕΥΝΑΣ ΜΑΣ

Κύριο χαρακτηριστικό παλαιότερων μορφών κρυπτογράφησης είναι πως η επεξεργασία γινόταν πάνω στη γλωσσική δομή του μηνύματος. Αντίθετα η νεότερη μορφή κρυπτογράφησης κάνει χρήση του αριθμητικού ισοδύναμου, ενώ η έμφαση έχει μεταφερθεί σε διάφορα πεδία των μαθηματικών.

ΠΕΡΙΟΔΟΙ

Στη πρώτη περίοδο κρυπτογραφίας (1900 π.Χ. – 1900 μ.Χ.) αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, που βασίζονταν κυρίως σε απλές αντικαταστάσεις γραμμάτων. Η δεύτερη περίοδος της κρυπτογραφίας τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950. Καλύπτει τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων αναπτύχθηκε η κρυπτογραφία τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. Η τρίτη περίοδος της κρυπτογραφίας ξεκίνησε το 1950 μ.Χ. και συνεχίζεται ως σήμερα. Εκείνη την εποχή η κρυπτογραφία εξαφανίζεται και φυλάσσεται από τις μυστικές υπηρεσίες κυβερνητικών επικοινωνιών όπως η NSA.

ΛΕΙΤΟΥΡΓΙΚΟΙ ΣΚΟΠΟΙ

Οι λειτουργικοί σκοποί της κρυπτογράφησης είναι η ασφάλεια συναλλαγών σε τράπεζες δίκτυα, η κινητή τηλεφωνία και σταθερή τηλεφωνία, η διασφάλιση Εταιρικών πληροφοριών, τα στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης), τα διπλωματικά δίκτυα (Τηλεγραφήματα), οι ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές), η ηλεκτρονική ψηφοφορία και ηλεκτρονική δημοπρασία, το ηλεκτρονικό γραμματοκιβώτιο, τα συστήματα συναγερμών, τα συστήματα βιομετρικής αναγνώρισης, οι έξυπνες κάρτες, τα ιδιωτικά δίκτυα, το Word Wide Web, οι δορυφορικές εφαρμογές (δορυφορική τηλεόραση), τα ασύρματα δίκτυα, τα συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων και τέλος η τηλεσυνδιάσκεψη - Τηλεφωνία μέσω διαδικτύου.

ΣΗΜΕΡΑ

Όλα αυτά τα συστήματα έχουν κρυπταναλυθεί και έχει αποδειχθεί ότι, εάν είναι γνωστό ένα μεγάλο κομμάτι του κρυπτογραφημένου μηνύματος, τότε το αρχικό κείμενο μπορεί σχετικά εύκολα να επανακτηθεί.

Η ΠΡΩΤΗ ΣΤΡΑΤΙΩΤΙΚΗ ΧΡΗΣΗ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

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. 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. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες.

ΠΕΡΙΣΣΟΤΕΡΑ

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.

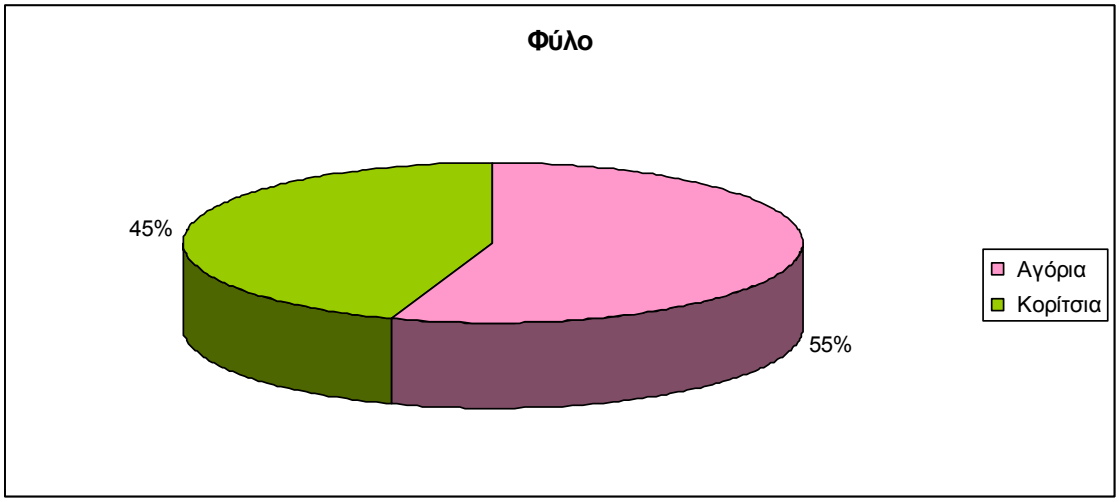
Οι Άραβες είναι οι πρώτοι που επινόησαν αλλά και χρησιμοποίησαν μεθόδους κρυπτανάλυσης. Το κυριότερο εργαλείο στην κρυπτανάλυση, επινοήθηκε από αυτούς γύρω στον 14ο αιώνα. Η κρυπτογραφία, λόγω των στρατιωτικών εξελίξεων, σημείωσε σημαντική ανάπτυξη στους επόμενους αιώνες.

Η 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 σε ιερατική γραφή. Δύο μεγάλοι αποκρυπτογράφοι της εποχής, ο Γιάνγκ και ο Σαμπολιόν.

ΤΑΥΤΟΤΗΤΑ ΕΡΕΥΝΑΣ

Περίοδος διεξαγωγής: 18/3/2014
Περιοχή διεξαγωγής: 2^{ο} Γ. Ε. Λ. Ελευθερίου Κορδελιού
Πληθυσμός: Όλη η Β' Γυμνασίου και Α'4 Γυμνασίου Ελ. Κορδελιού
Δείγμα: 30 Ερωτηματολόγια
Τεχνικές συλλογής στοιχείων: Χρησιμοποιήθηκε ερωτηματολόγιο κλειστού τύπου και ένα είδος παιχνιδιού
Υπεύθυνη καθηγήτρια: κα Καλλιόπη Μαγδαληνού

Αποτελέσματα ερωτηματολογίου:

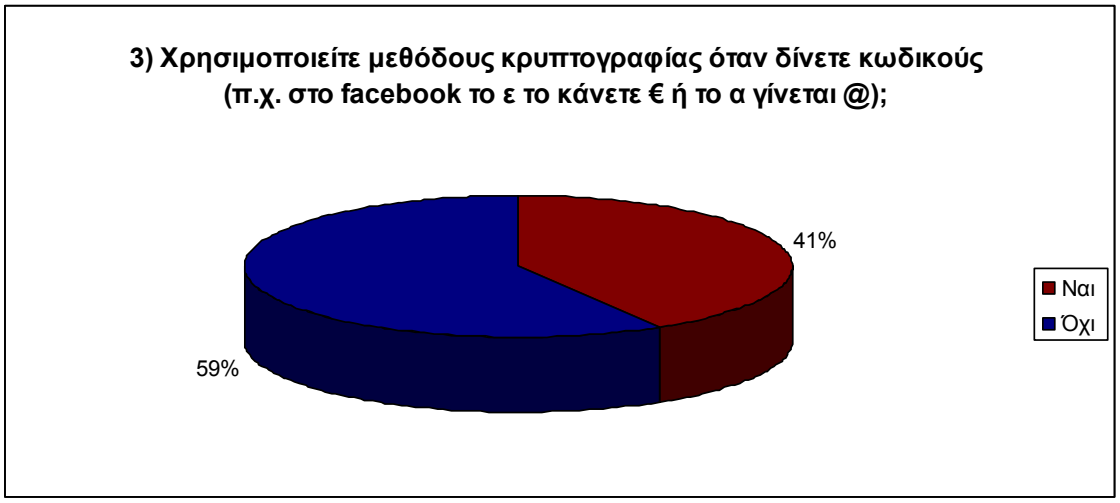


Συμπέρασμα: Τα αγόρια ήταν περισσότερα

.

Συμπέρασμα: Απ' ότι φαίνεται λίγοι γνώριζαν την έννοια της αποκρυπτογράφησης.

Συμπέρασμα: Σύμφωνα με τα αποτελέσματα μικρή ήταν η διαφορά μεταξύ εκείνων που προσέχουν την https σύνδεση και εκείνων που όχι.



Συμπέρασμα: Λίγοι είναι αυτοί που χρησιμοποιούν περίπλοκους κωδικούς.

ΤΟ ΣΥΜΠΕΡΑΣΜΑ

Με βάση τα αποτελέσματα του ερωτηματολογίου πως ελάχιστοι τελικά είναι εκείνοι που γνωρίζουν την έννοια της κρυπτογραφίας αλλά και περεταίρω στοιχεία σχετικά με αυτή.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Οι διαδικτυακές πηγές: International Association for Cryptologic Research, The Code Book on CD-ROM, Simon Singh και Δωρεάν Βιβλίο, Handbook of Applied Cryptography.

Οι ερωτήσεις που θέσαμε στο ερωτηματολόγιο είναι : α)Αν γνωρίζουν την έννοια της αποκρυπτογράφησης, β)Αν προσέχουν ποτέ αν η σύνδεσή τους είναι https ή http όταν καταχωρούν δεδομένα γ)Αν χρησιμοποιούν μεθόδους κρυπτογραφίας όταν δίνουν κωδικούς και δ) Δώσαμε τον κώδικα ASCII προκειμένου να γράψουν κωδικοποιημένα τ ’όνομά τους.