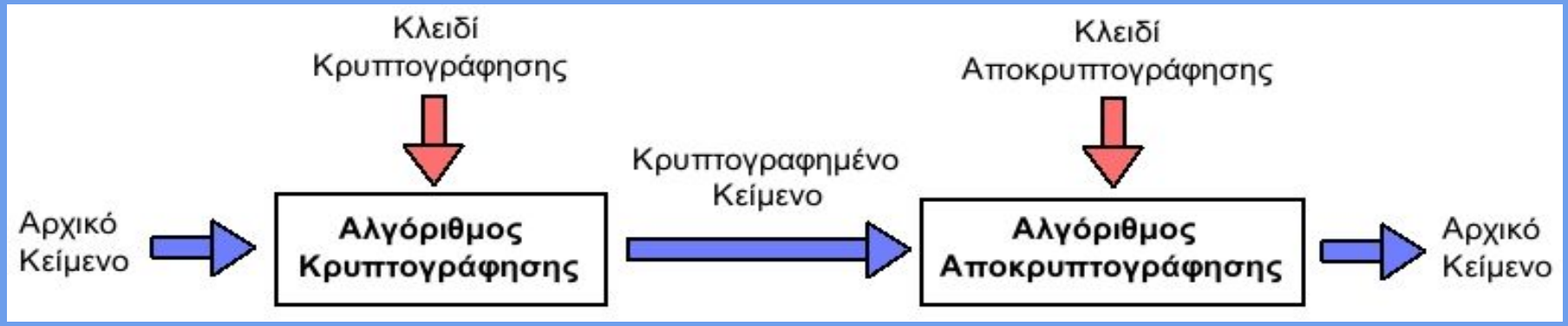
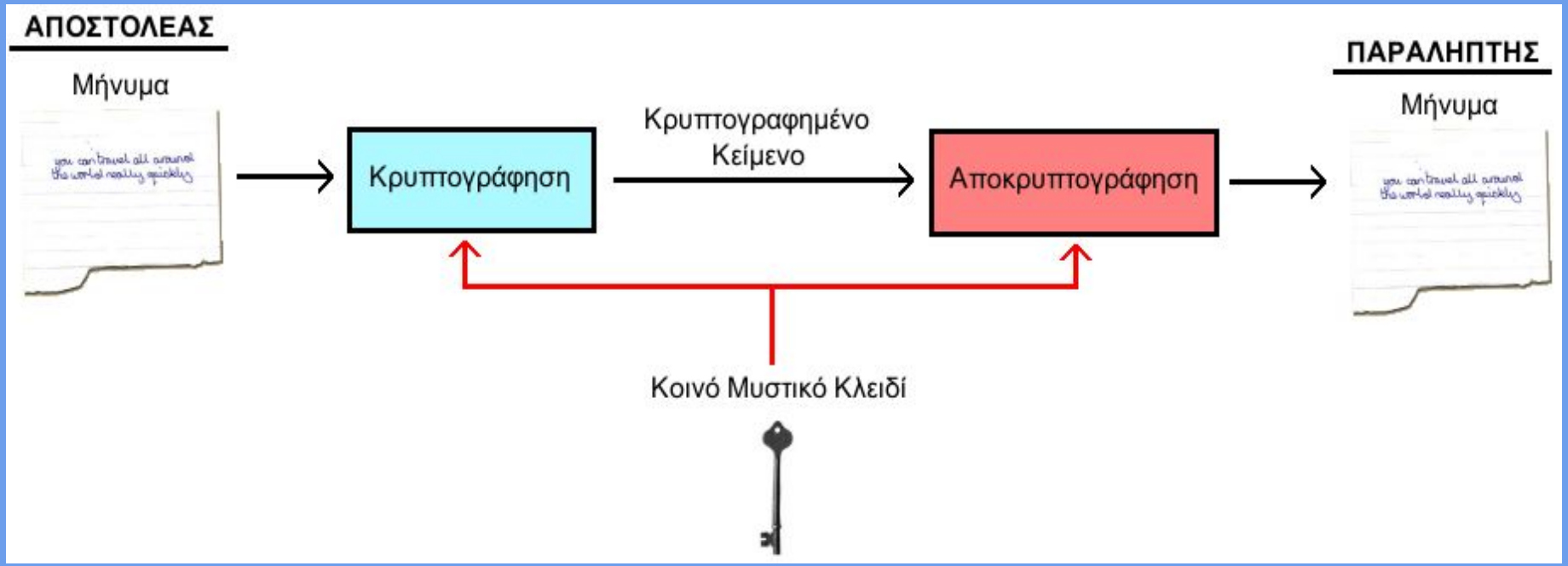
ΚΡΥΠΤΟΓΡΑΦΙΑ

Εισαγωγή

Γρηγοράκης Στέλιος
Δημητρίου Αφροδίτη
Ιβανόβ Τόνι
Κωσταντουράκης Γρηγόρης
Τσιμινικάκη Ελένη

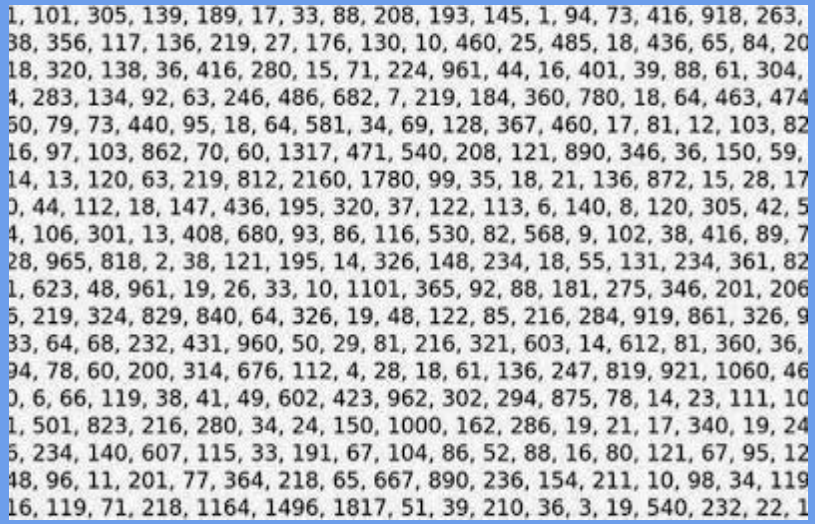
Η κρυπτογραφία είναι ένας τρόπος που δίνει τη δυνατότητα σε δύο πρόσωπα να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο, μη εξουσιοδοτημένο (ένας αντίπαλος), να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων. Στις μέρες μας η Κρυπτογραφία έχει αναχθεί σε επιστήμη, με τις εφαρμογές τις διαρκώς να πληθαίνουν.


Κλειδί
Κρυπτογράφησης
Κλειδί
Αποκρυπτογράφησης
Αρχικό
Κείμενο
Αλγόριθμος
Κρυπτογράφησης
Κρυπτογραφημένο
Κείμενο
Αλγόριθμος
Αποκρυπτογράφησης
Αρχικό
Κείμενο


ΑΠΟΣΤΟΛΕΑΣ
Μήνυμα
Κρυπτογράφηση
Κρυπτογραφημένο
Κείμενο
Αποκρυπτογράφηση
ΠΑΡΑΛΗΠΤΗΣ
Μήνυμα
Κοινό Μυστικό Κλειδί

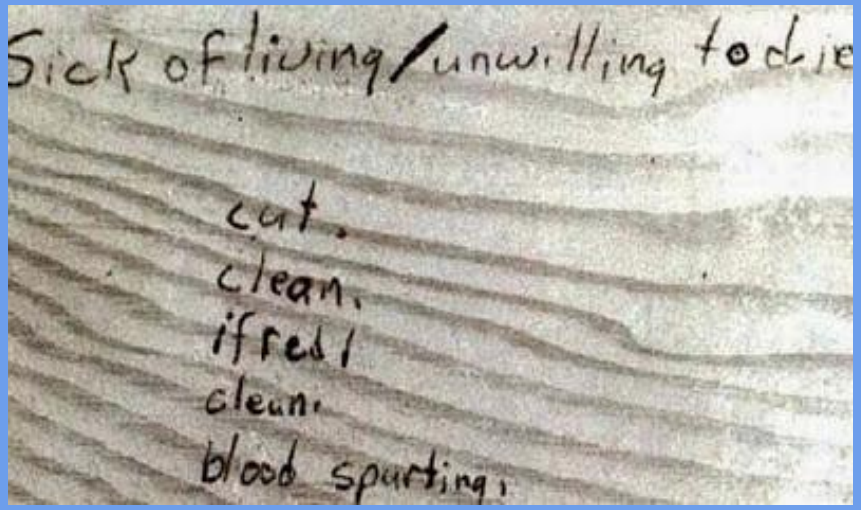
Τα ακόλουθα αινιγματικά μηνύματα - κώδικες δεν έχουν αποκρυπτογραφηθεί

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
5, 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
5, 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.

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. 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.

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. 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.

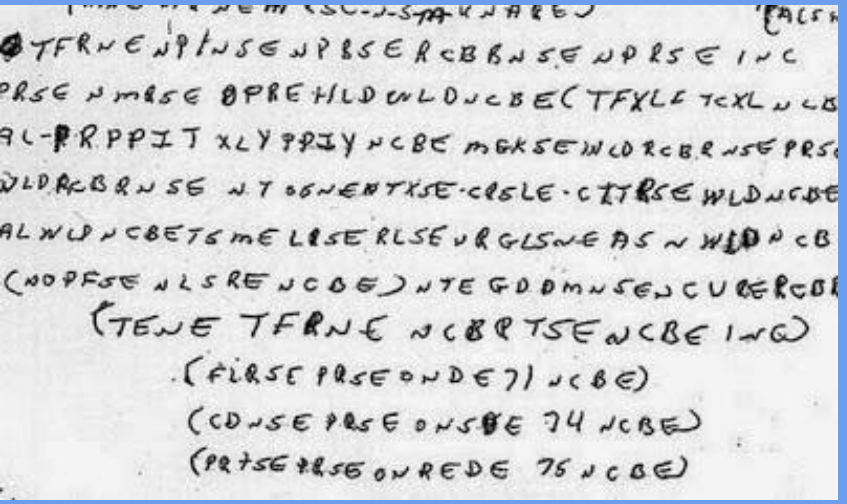
Γραμμική Α

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

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.

Το μυστήριο McCormick

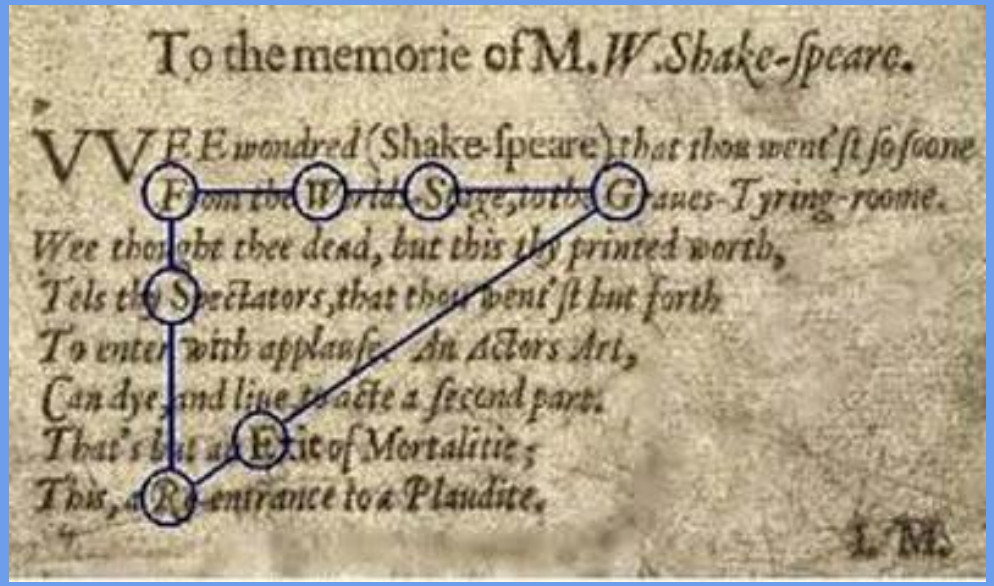


Το 1999, το πτώμα του Ricky McCormick βρέθηκε στο ανατολικό Μιζούρι. Στις τσέπες του είχε δυο αλγόριθμους κρυπτογραφημένους.

Blitz

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

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's 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.

Η κρυπτογραφία τον 20ο αιώνα

Θεοχαρακης Γιαννης, Δρακακης Γιαννης, Κουρουπακης Γιαννης, Αντωνακη Μαρια, Μπατσολακη Φωτεινη

Η δεύτερη περίοδος κρυπτογραφίας

Η δεύτερη περίοδος της κρυπτογραφίας τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950 επομένως,στους δύο παγκόσμιους πολέμους. Τότε αναπτύχθηκε η κρυπτογραφία όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. 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. Οι Πολωνοί είχαν προετοιμαστεί για την εμπόλεμη περίοδο κατασκευάζοντας την κρυπτομηχανή LCD Lacida, η οποία κρατήθηκε μυστική ακόμη και από τον Rejewski.

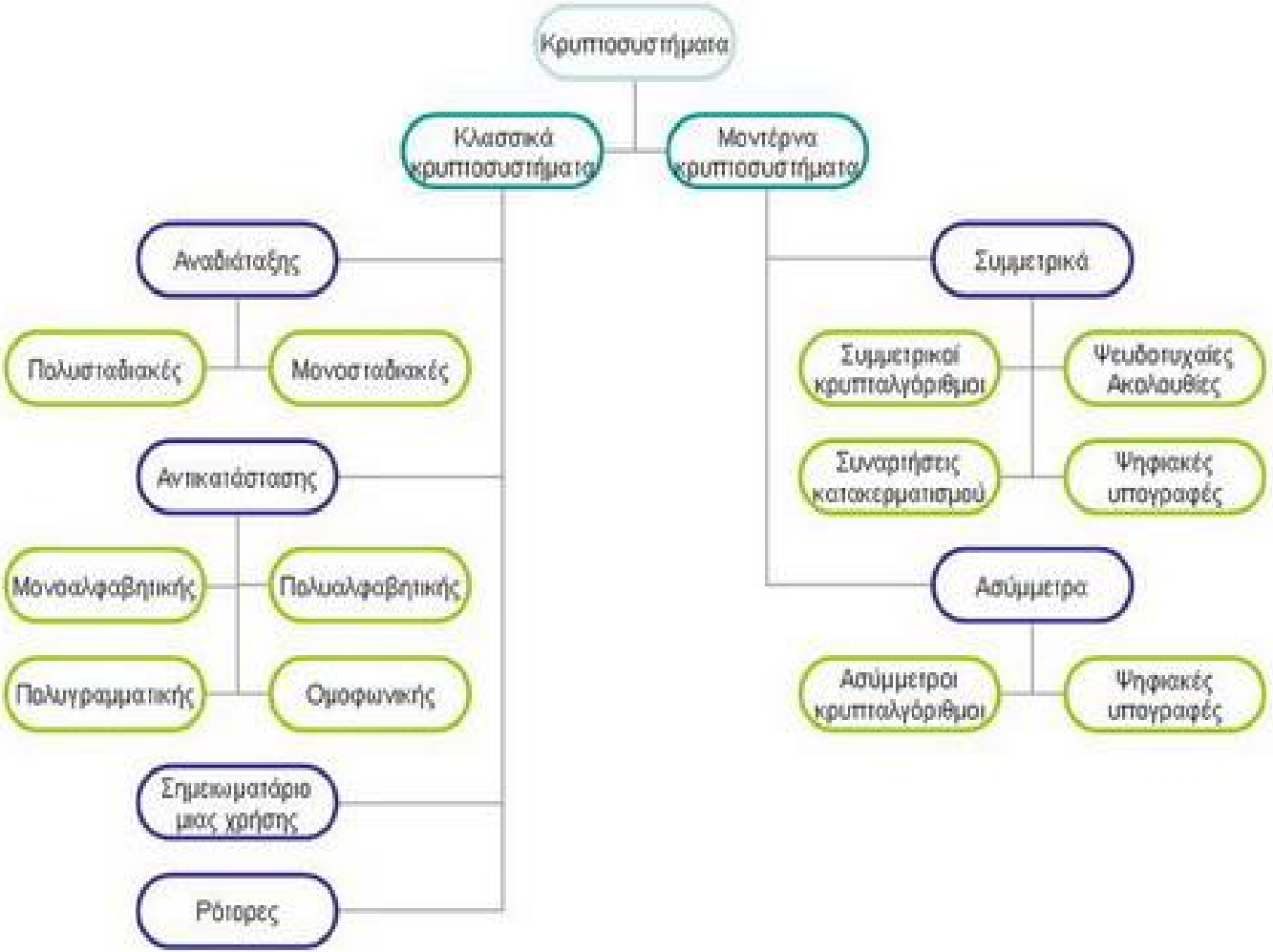
Η μηχανή Αίνιγμα χρησιμοποιήθηκε ευρέως στη Γερμανία

Η τρίτη περίοδος

Η τρίτη 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. 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 Στα μέσα της δεκαετίας του '70, όλα άλλαξαν

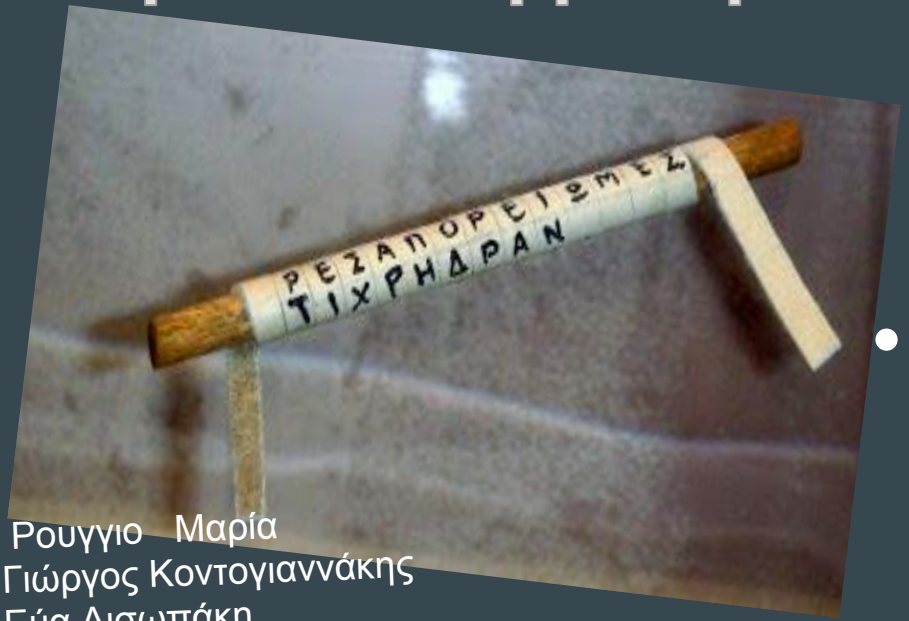
Εγιναν δύο σημαντικές δημόσιες (δηλ. μη-μυστικές) πρόοδοι. Πρώτα ήταν η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES στον ομοσπονδιακό κατάλογο της Αμερικής στις 17 Μαρτίου 1975. Μετά από τις συμβουλές και την τροποποίηση από την NSA, αυτό το πρότυπο υιοθετήθηκε και δημοσιεύθηκε ως ένα ομοσπονδιακό τυποποιημένο πρότυπο επεξεργασίας πληροφοριών το 1977. Ο DES ήταν ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης που εγκρίνεται από μια εθνική αντιπροσωπεία όπως η NSA .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.

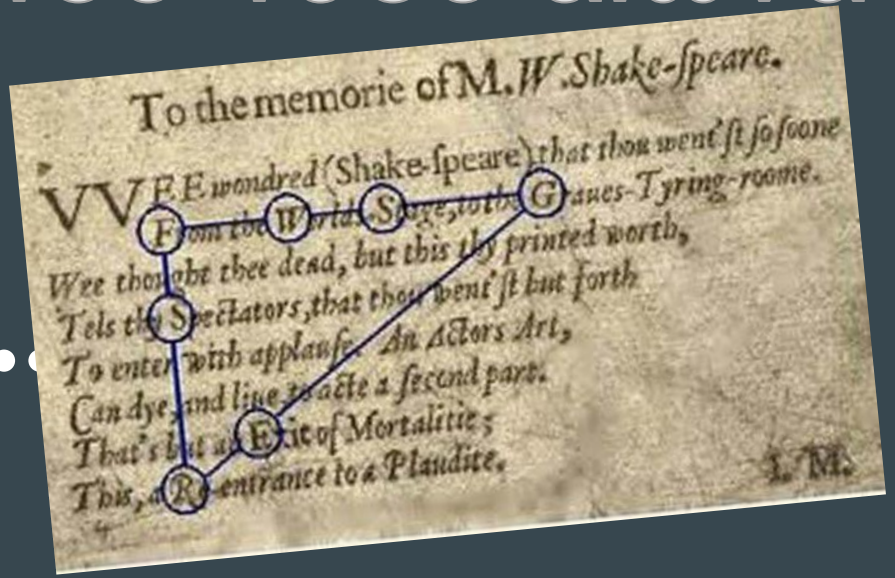
Η χρήση απλής κρυπτογράφησης με τον DES είναι τώρα χωρίς την αμφιβολία επισφαλής για χρήση στα νέα σχέδια των κρυπτογραφικών συστημάτων και μηνύματα που προστατεύονται από τα παλαιότερα κρυπτογραφικά συστήματα που χρησιμοποιούν DES , και όλα τα μηνύματα που έχουν αποσταλεί από το 1976 με τη χρήση DES , διατρέχουν επίσης σοβαρό κίνδυνο αποκρυπτογράφησης. Υπήρξε επίσης η υποψία ότι κυβερνητικές οργανώσεις είχαν ακόμα και τότε ικανοποιητική υπολογιστική δύναμη ώστε να σπάσουν μηνύματα που είχαν κρυπτογραφηθεί με τον DES.



Κατηγορίες κρυπτοσυστημάτων

Κρυπτογραφια του 19ου αιωνα



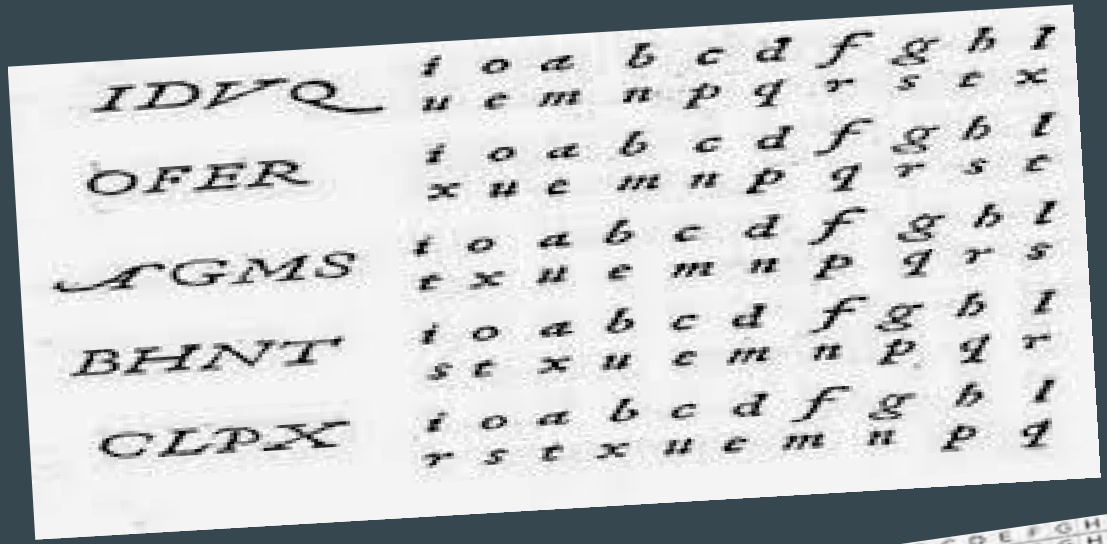


Ρουγγιο Μαρία
Γιώργος Κοντογιαννάκης
Εύα Αισωπάκη
Μάνος Φραγκούλης
Γεωργία Κωστάκη

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.

Κρυπτογραφια του Vigenere

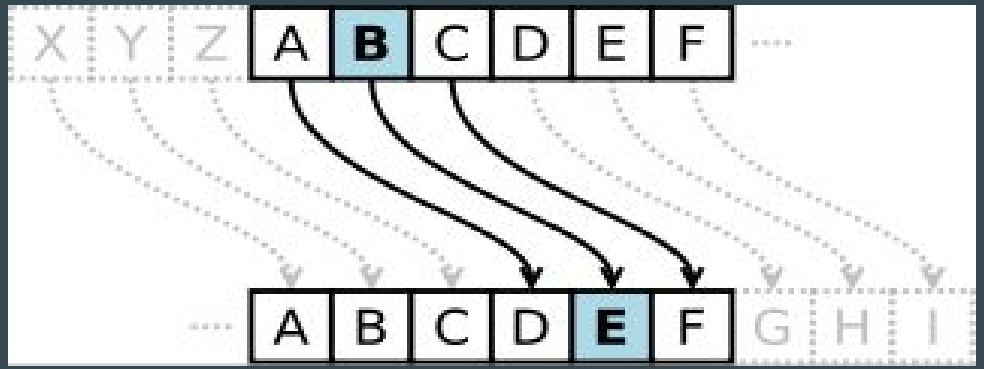
Ο αλγόριθμος κρυπτογράφησης Vigenère είναι μία μέθοδος κρυπτογράφησης σε αλφαβητικό κείμενο στο οποίο εφαρμόζονται διαφορετικοί αλγόριθμοι κρυπτογράφησης Καίσαρα με βάση τη θέση των γραμμάτων μιας λέξης ή φράσης κλειδί. Είναι μια απλή μορφή της πολυαλφαβητικής υποκατάστασης. Η κρυπτογράφηση Vigenère έχει εφευρεθεί εκ νέου πολλές φορές. Τη μέθοδο αρχικά περιέγραψε ο Giovan Battista Bellaso το 1553.


IDVQ
i o a b c d f g h l
u e m n p q r s t x
OFER
i o a b c d f g h l
x u e m n p q r s t
AGMS
i o a b c d f g h l
t x u e m n p q r s
BHNT
i o a b c d f g h l
s t x u e m n p q r
CLPX
i o a b c d f g h l
r s t x u e m n p q

Κωδικας του Καισαρα κατα τον 19ο αιωνα

Ο **Κώδικας του Καίσαρα** είναι μία από τις απλούστερες και πιο γνωστές τεχνικές κωδικοποίησης στην κρυπτογραφία. Είναι κώδικας αντικατάστασης στον οποίο κάθε γράμμα του κειμένου αντικαθίσταται από κάποιο άλλο γράμμα με σταθερή απόσταση κάθε φορά στο αλφάβητο. Η μέθοδος πήρε το όνομά της από τον Ιούλιο Καίσαρα, ο οποίος την χρησιμοποιούσε στην προσωπική του αλληλογραφία.

Το βήμα κωδικοποίησης που εκτελείται από τον κώδικα του Καίσαρα συχνά ενσωματώνεται ως τμήμα ενός πιο πολύπλοκου πλαισίου όπως ο κώδικας Vigenère (Βιζενέρ). Όπως με όλους τους μονοαλφαβητικούς κώδικες αντικατάστασης, ο κώδικας του Καίσαρα σπάει εύκολα και στη σύγχρονη εφαρμογή του δεν παρέχει ουσιαστικά κάποια ασφάλεια επικοινωνίας.



Κρυπτογραφια (Σπαρτιατικη σκυταλη)

Το σύστημα κρυπτογράφησης της Σπαρτιατικής σκυτάλης ανήκει στον κλάδο της μετάθεσης. Περνώντας στο κυρίως θέμα λοιπόν,η σκυτάλη ήταν το κύριο μέσο μεταφοράς κρυπτογραφημένων μηνυμάτων των Σπαρτιατών κυρίως σε περιόδους πολεμικών συρράξεων για προφανείς λόγους!Η πρώτη σκυτάλη μας έρχεται απο τον 5ο αιώνα.

Σύγχρονη κρυπτογραφία

Κατερίνα Αϊλαμάκη
Πάολα Πίρια
Εμμανουέλα Λεβεντέρη
Γιάννης Ζουριδάκης
Σταύρος Λαμπράκης

Σήμερα, η Σύγχρονη Κρυπτογραφία παρέχει εφαρμογές σε κάθε τομέα της καθημερινής μας ζωής: από το ξεκλείδωμα ενός αυτοκινήτου από απόσταση και την παρακολούθηση ενός επί πληρωμή δορυφορικού καναλιού, έως την αγορά προϊόντων με χρήση πιστωτικών και χρεωστικών καρτών, την εγκατάσταση μιας ενημέρωσης λογισμικού, τη χρήση ενός δικτύου κινητής επικοινωνίας ή του Διαδικτύου και την αξιοποίηση Κάρτας Πολίτη σε διάφορες χώρες και σύντομα και στην Ελλάδα. Στο εγγύς μέλλον αναμένουμε πολλές νέες συναρπαστικές εφαρμογές της Κρυπτογραφίας, όπως η Αναγνώριση μέσω Ραδιοσυχνοτήτων (RFID) για την καταπολέμηση της παραποίησης και απομίμησης προϊόντων και τα έξυπνα περιβάλλοντα.

Υπάρχουν διάφορες τεχνικές αλγορίθμων στις οποίες βασίζονται και οι αντίστοιχοι κώδικες κρυπτογραφίας, εδώ θα αναφέρουμε τις δυο βασικότερες κατηγορίες τεχνικών αλγορίθμων οι οποίες είναι: 1) Συμμετρικοί αλγόριθμοι 2) Ασύμμετροι αλγόριθμοι.
Στους συμμετρικούς αλγόριθμους συγκαταλέγονται οι DES, IDEA, RCS, BLOWFISH ενώ στην κατηγορία των ασύμμετρων ένα τυπικό δείγμα είναι ο RSA.

Το ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημοσίου κλειδιού δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Χαρακτηριστικό του είναι ότι έχει δυο είδη κλειδιών, ένα ιδιωτικό και ένα δημόσιο. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό. Η βασική σχέση μεταξύ τους είναι : ό,τι κρυπτογραφεί το ένα, μπορεί να το αποκρυπτογραφήσει μόνο το άλλο .

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη τη μεταφορά της πληροφορίας για διάφορους λειτουργικούς σκοπούς όπως :

Ασφάλεια συναλλαγών σε τράπεζες δίκτυα - ΑΤΜ

Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)

Σταθερή τηλεφωνία (cryptophones)

Διασφάλιση Εταιρικών πληροφοριών

Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)


REGISTERED IDENTITY