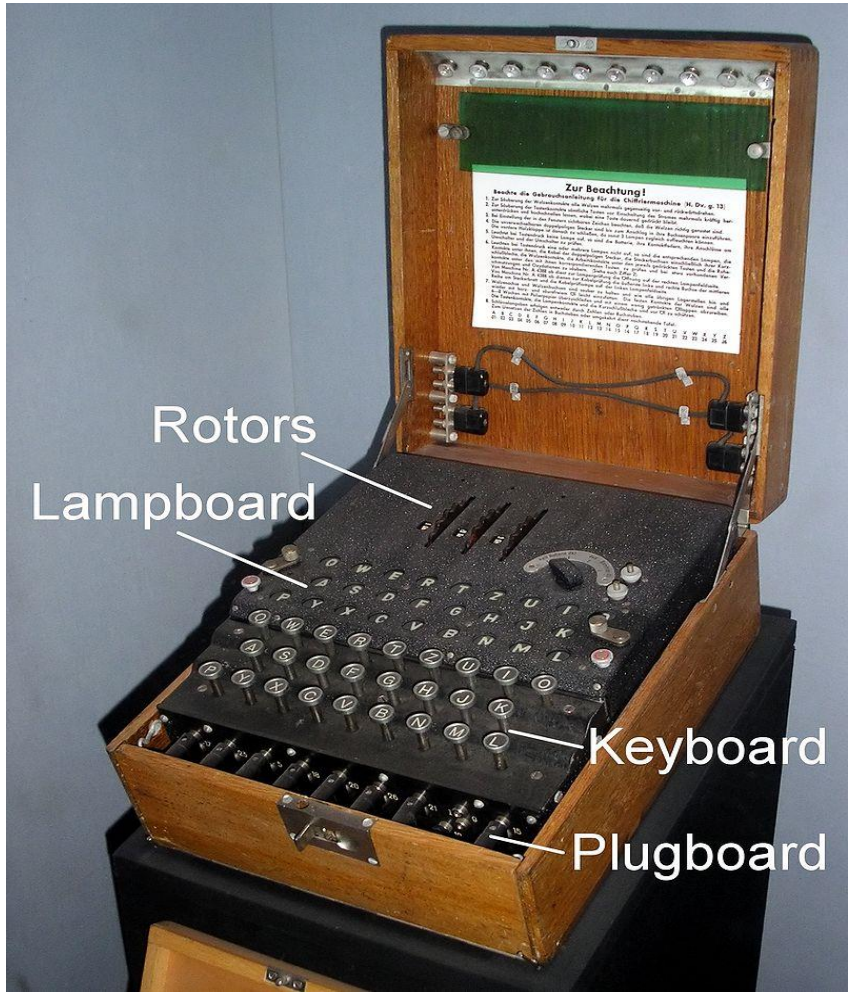
Νεότερη ιστορία κρυπτογραφίας
από το 1950

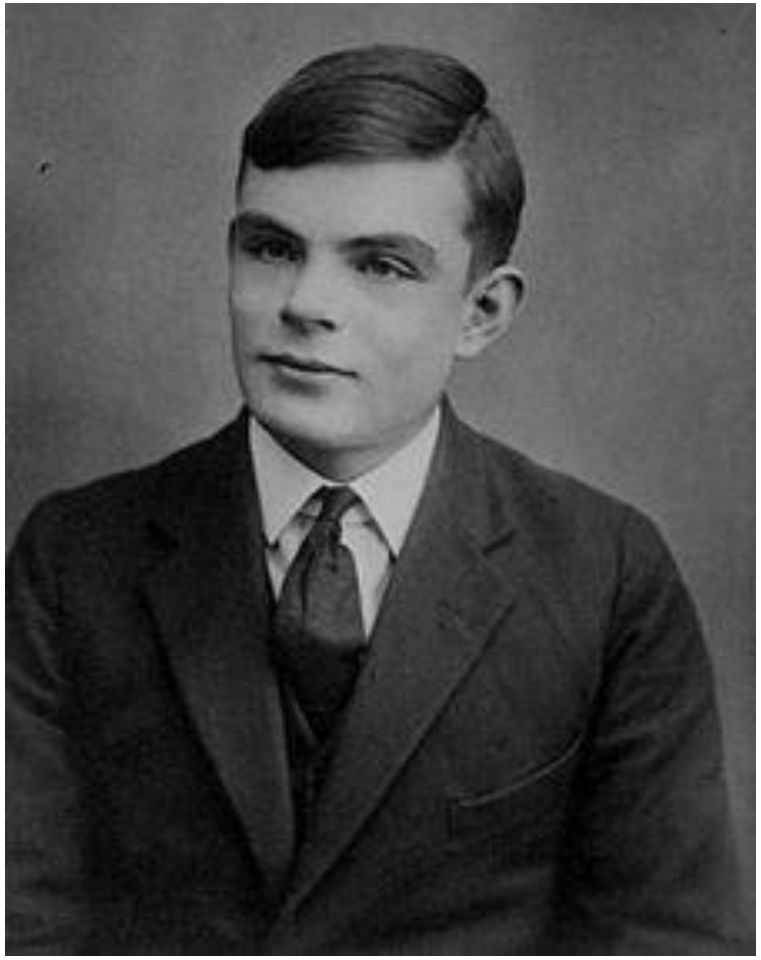
Η στεγανογραφία, μετέπειτα κρυπτογραφία, αναφέρεται από τον Ηρόδοτο κατά τη διάρκεια των Περσικών πολέμων. Ο ρόλος της, στη εξέλιξη της παγκόσμιας ιστορίας, είναι ιδιαίτερα σημαντικός. Σήμερα αποτελεί καθημερινή ανάγκη και για τον απλό άνθρωπο.

Θα αναφερθούμε γλαφυρά στην νεότερη ιστορία της κρυπτογραφίας από το 1950, οπότε η συμβολή των μαθηματικών είναι καθοριστική. Θα περιοριστούμε, χωρίς αποδείξεις, στα κομμάτια που έχουν σχέση με τη στοιχειώδη Θεωρία Αριθμών.

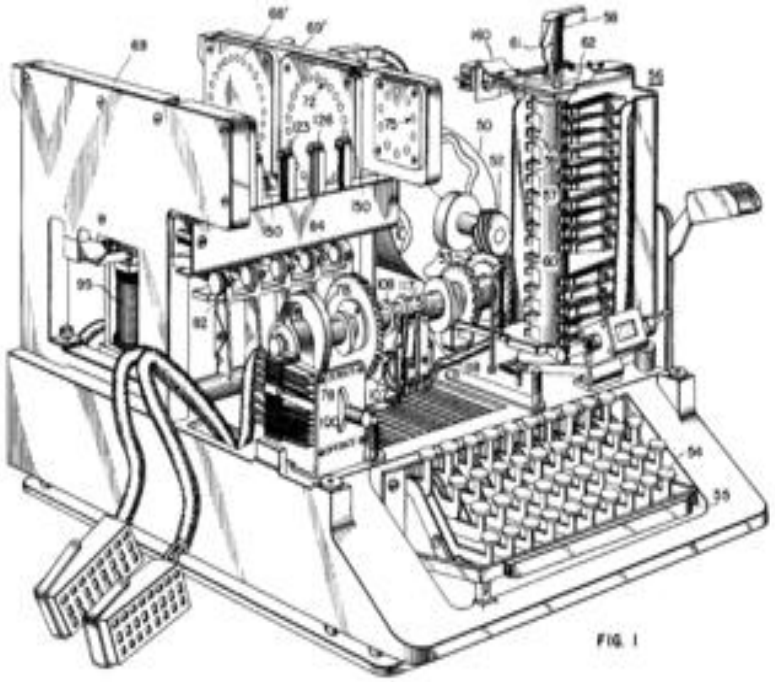


Military Enigma machine

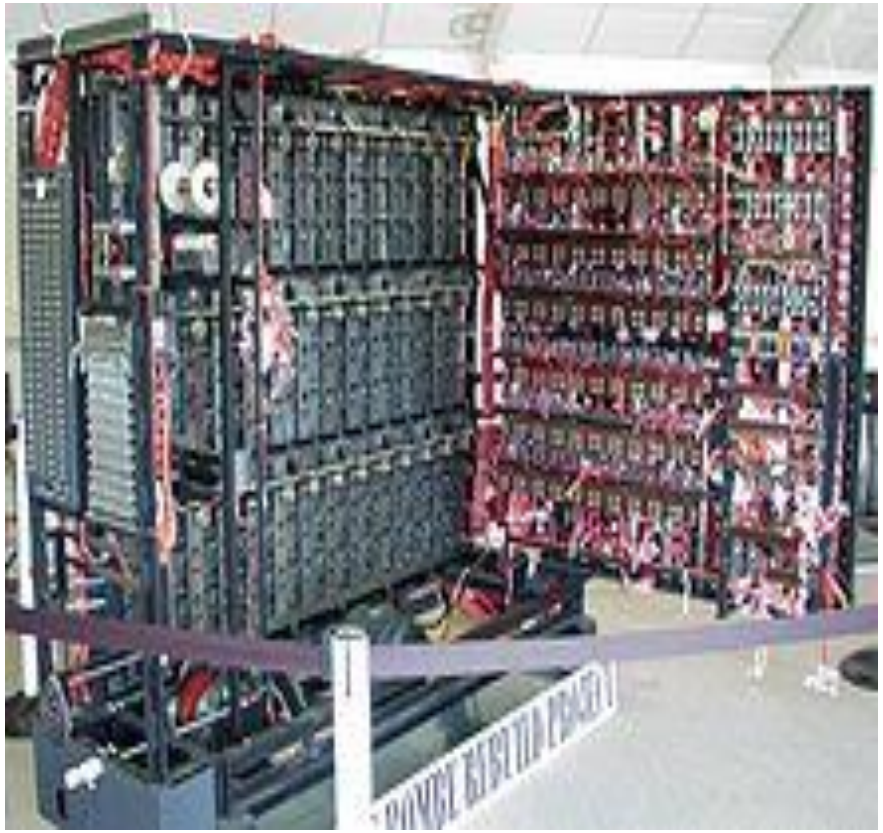
https://www.youtube.com/watch?v=BlLaXxTD2rs



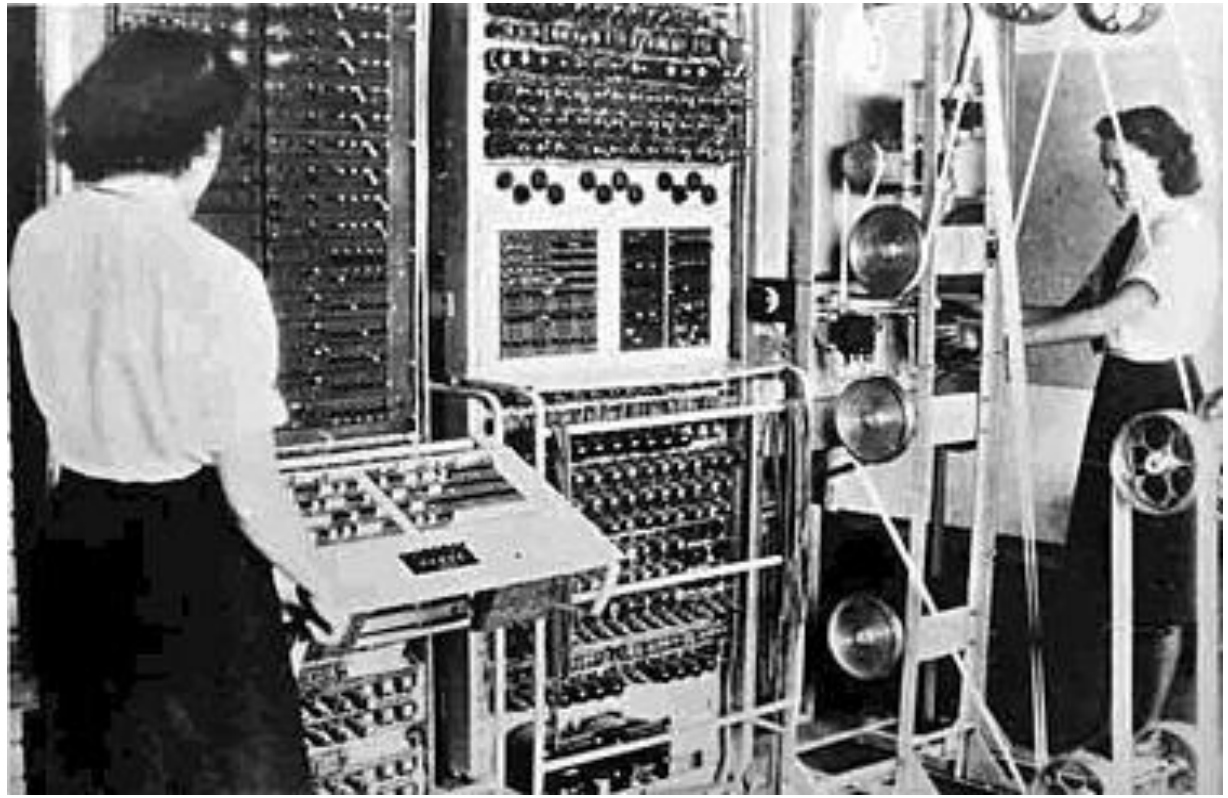
Alan Mathison Turing (23 June 1912 – 7 June 1954) was a pioneering English computer scientist, mathematician, logician, cryptanalyst and theoretical biologist.



SIGABA is described in U.S. Patent 6,175,625, filed in 1944 but not issued until 2001.



A complete and working replica of a bombe at the National Codes Centre at Bletchley Park



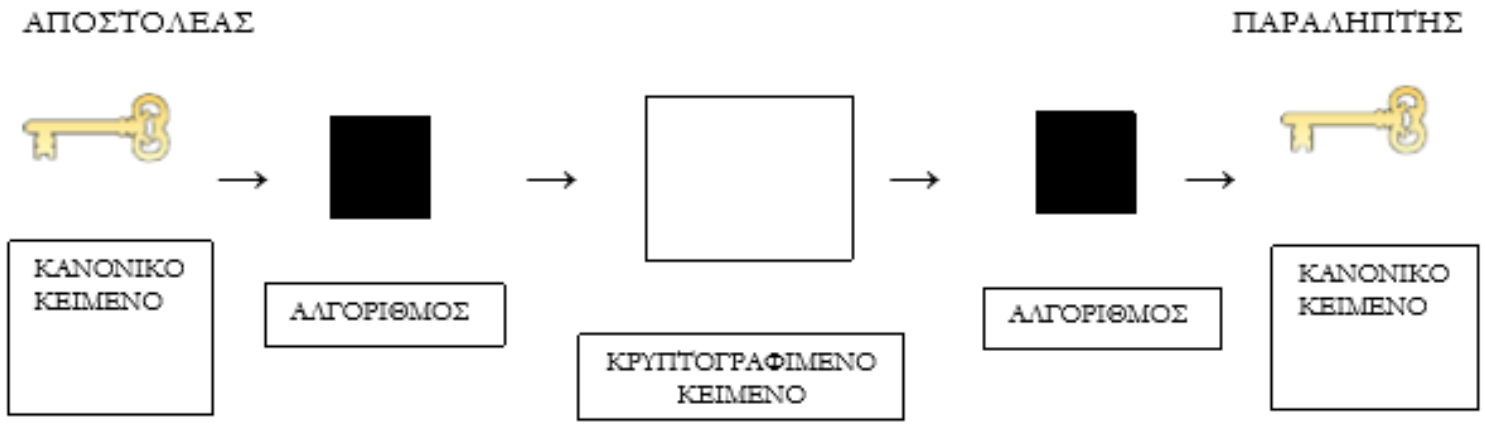
Colossus Mark 1,

Οι κρυπταναλυτές συνέβαλαν στην ανάπτυξη του σύγχρονου υπολογιστή.

- Μέχρι το 1950 η κρυπτογράφηση ήταν σημαντική για της κυβερνήσεις και τους στρατιωτικούς. Ο ρόλος της στην κατασκοπία και την έκβαση των πολέμων, ιδιαίτερα του δευτέρου, ήταν καθοριστικός.
- Σήμερα είναι απαραίτητη: Εταιρείες, εμπορικοί σκοποί, επικοινωνία.
- Κλασικός τρόπος, ταχυδρομείο.
- E-mail. Πότε είναι ασφαλές;

- Σκοπός της κρυπτογραφίας είναι όχι η απόκρυψη της ύπαρξης ενός μηνύματος αλλά του νοήματός του.
- Η πληροφορία και η ασφάλεια της πληροφορίας αποτελούν το πιο πολύτιμο αγαθό της εποχής μας.
- Για να καταστεί ένα μήνυμα μη κατανοητό, μετασχηματίζεται σύμφωνα με ένα ειδικό πρωτόκολλο (κρυπτογράφηση) που έχει συμφωνηθεί εκ των προτέρων μεταξύ του αποστολέα και του παραλήπτη.
- Η ασφάλεια της πληροφορίας εξαρτάται από την κρυπτογράφηση.

- Για να κρυπτογραφηθεί ένα κείμενο, ο αποστολέας το περνάει μέσα από έναν αλγόριθμο κρυπτογράφησης. Ο αλγόριθμος είναι ένα γενικό σύστημα κρυπτογράφησης και πρέπει να εξειδικευθεί με ακρίβεια μέσω ενός κλειδιού.
- Το κρυπτογραφημένο κείμενο μπορεί να υποκλαπεί από τον εχθρό. Είναι άχρηστο, αν ο εχθρός δεν κατέχει το κλειδί.



ΑΠΟΣΤΟΛΕΑΣ

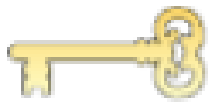
ΠΑΡΑΛΗΠΤΗΣ

ΚΑΝΟΝΙΚΟ ΚΕΙΜΕΝΟ

ΑΛΓΟΡΙΘΜΟΣ

ΚΡΥΠΤΟΓΡΑΦΙΜΕΝΟ ΚΕΙΜΕΝΟ

ΑΛΓΟΡΙΘΜΟΣ



ΚΑΝΟΝΙΚΟ ΚΕΙΜΕΝΟ

- Οι κρυπταναλυτές συνέβαλαν στην ανάπτυξη του σύγχρονου υπολογιστή.
- Η ιδέα ήταν να χρησιμοποιηθεί η ταχύτητα του Η. Υ. ώστε να ελεγχθούν όλα τα πιθανά κλειδιά μέχρι να βρεθεί το σωστό.
- Κύρια διαφορά μεταξύ κλασικής και σύγχρονης κρυπτογράφησης: Χρήση δυαδικού συστήματος. ASCII American Standard Code for Information Interchange
- Κώδικας Mors.

- 100 0001 A
- 100 0010 B
- 100 0011 C
- 100 0100 D
- 100 0101 E
- 100 0110 F
- 100 0111 G
- 100 1000 H
- 100 1001 I
- 100 1010 J
- 100 1011 K
- 100 1100 L
- 100 1101 M
- 100 1110 N
- 100 1111 O
- 101 0000 P
- 101 0001 Q
- 101 0010 R
- 101 0011 S
- 101 0100 T
- 101 0101 U
- 101 0110 V
- 101 0111 W
- 101 1000 Y
- 101 1010 Z

- Η κρυπτογράφηση γίνεται με συνδυασμούς, υποκαταστάσεις, ή και μεταθέσεις:
- κάποια στοιχεία υποκαθιστούν κάποια άλλα ή αλλάζουν αμοιβαία θέση ή και οι δύο περιπτώσεις ταυτόχρονα.

- Παράδειγμα
- Κείμενο HELLO: 100 1000 100 0101 100 1100 100 1100 100 1111
- Κλειδί DAVID: 100 0100 100 0001 101 0110 100 1001 100 0100
- Κρυπτογραφημένο 000 1100 000 0100 001 1010 000 0101 000 1011

- 1960. Κάθε εταιρεία χρησιμοποιούσε τη δική της κρυπτογράφηση. Έπρεπε να ορισθεί κοινή.
- NSA: National Security Agency
- Απασχολεί τους περισσότερους μαθηματικούς, αγοράζει τους ισχυρότερους υπολογιστές και υποκλέπτει τα περισσότερα μηνύματα στο κόσμο.
- 1975. Κρυπτογράφηση Εωσφόρος, IBM.
- **Horst Feistel** (1915-1990) cryptographer, worked on the ciphers
- initiating research that culminated in the development of the
- Data Encryption Standard (DES).

- Εωσφόρος.
- Η σειρά των δυαδικών ψηφίων διασπάται σε 64-άδες.
- Τα ψηφία της κάθε 64-άδας αναδιατάσσονται σε 32-άδες.
- Στη δεξιά αλλάζει η σειρά των ψηφίων με μια μετάθεση.
- Η νέα προστίθεται στην παλαιά και καλείται «δεξιά».
- Αυτό γίνεται 16 συνολικά φορές.
- Το Κλειδί είναι ο τρόπος που ακολουθείται για να φτάσουμε στην τελευταία 64-άδα.

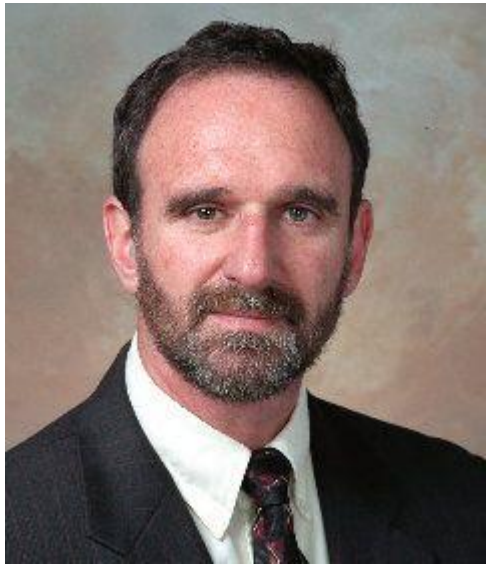
- Η NSA δεν μπορούσε να σπάσει την κρυπτογράφηση λόγω της πληθώρας των πιθανών κλειδιών. Γι' αυτό και απαγόρευσε να υπάρχουν περισσότερα από 10^{19} κλειδιά ώστε αυτή να είναι σε θέση να σπάσει τον κώδικα αλλά καμία εμπορική ή πολιτική οργάνωση να είναι σε θέση να το κάνει.
- Αυτός ο τρόπος κρυπτογράφησης καλείται
- DES Data Encryption Standard
- Δεν σπάει, αλλά ;;;;;

- Πως διανέμονται τα κλειδιά;;;;;;;;;
- Τράπεζες,
- Πολυεθνικές,
- Στρατός.
- Κυρίαρχο πρόβλημα της κρυπτογραφίας είναι η διανομή των κλειδιών.
- Η μεγαλύτερη επανάσταση στην κρυπτογραφία του εικοστού αιώνα ήταν η υπέρβαση του προβλήματος της διανομής κλειδιών.

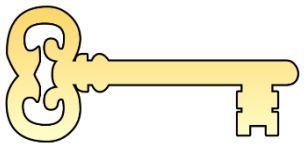
Whitfield Diffie, 1944 (MIT). Αφιέρωση τη ζωή του στο κυριότερο πρόβλημα της κρυπτογραφίας. «Η μεταφορά του κλειδιού».

- Πρώτο project: Επικοινωνία στρατιωτικών υπολογιστών.
- Γέννηση του ARPA Net, Advanced Research Projects Agency. Αποτέλεσμα το Internet.
- Η ανάγκη ασφαλούς μεταφοράς του κλειδιού γίνεται πιο επιτακτική από ποτέ.

Martin Hellman, 1945 (Stanford).



- Εκλαΐκευση του προβλήματος.
- Η Γεωργία προσπαθεί να στείλει ένα μήνυμα στον Κώστα και η Εύα προσπαθεί να το υποκλέψει.
- Με ποιο ασφαλή τρόπο θα στείλει ένα ή πολλά κλειδιά στον Κώστα χωρίς να μπορεί να το υποκλέψει η Εύα;



- Η Γεωργία κρυπτογραφεί το μήνυμά της με το κλειδί της και το στέλνει στον Κώστα.
- Ο Κώστας το παραλαμβάνει και το επανακρυπτογραφεί με το δικό του κλειδί και το ξαναστέλνει στη Γεωργία.
- Η Γεωργία το αποκρυπτογραφεί με το δικό της κλειδί και το ξαναστέλνει στον Κώστα.
- Αυτός το αποκρυπτογραφεί με το δικό του κλειδί και διαβάζει το μήνυμα.
- Είναι όλα εντάξει;;;;
- Ας το δούμε με μαθηματικά.

- Γεωργία Κώστας Γεωργία Κώστας Κώστας
- $M \xrightarrow[K_\Gamma]{} K_\Gamma M \xrightarrow[K_K]{} K_K K_\Gamma M \longrightarrow^{K_\Gamma^{-1}} K_\Gamma^{-1} K_K K_\Gamma M \longrightarrow^{K_K^{-1}} K_K^{-1} K_\Gamma^{-1} K_K K_\Gamma M$???? M

- Είναι μαθηματικά σωστό;;;;;
  - $g^{-1} f^{-1} g f =$;;;; 1 Ταυτοτική

- Οι Diffie και Hellman αναζητούσαν συναρτήσεις οι οποίες δεν ήταν 1-1 και μπορούσαν να αντιστραφούν όταν κάποιος γνώριζε κάτι που δεν γνώριζε κάποιος άλλος.

- Η Γεωργία και ο Κώστας ανακοινώνουν δυο αριθμούς Υ και Ρ(πρώτος) και η Εύα τους γνωρίζει.

- Γεωργία Υ=7, Ρ=11

Κώστας Υ=7, Ρ=11

Επιλέγει έναν αριθμό Γ=3 μυστικά.

Υπολογίζει

$Υ^{Γ} mod Ρ = 7^{3} mod 11 = 2$.

Στέλνει το 2 στον Κώστα. →

← Στέλνει το 4 στη Γεωργία.

Υπολογίζει το 4 που πήρε από τον Κώστα $4^{3} mod 11 = 9$.

Επιλέγει έναν αριθμό Κ=6 μυστικά.

Υπολογίζει

$Υ^{Κ} mod Ρ = 7^{6} mod 11 = 4$.

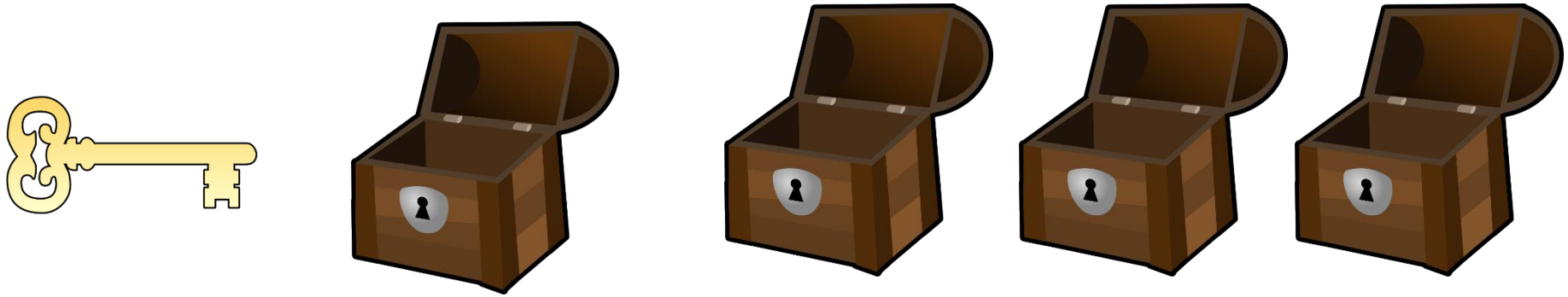
Υπολογίζει το 2 που πήρε από τη Γεωρ. $2^{6} mod 11 = 9$.

Το 9 είναι το κοινό κλειδί.

Η Εύα γνωρίζει το Υ=7, Ρ=11, και αυτά που έστειλαν η Γεωργία και ο Κώστας αλλά δεν ξέρει τι να τα κάνει.

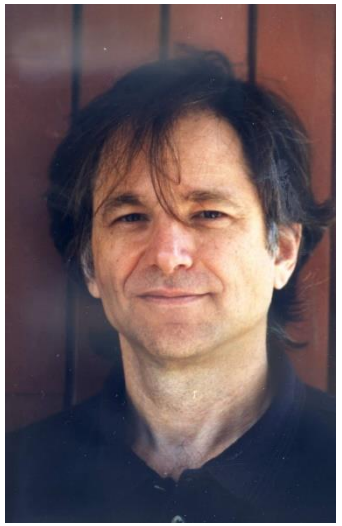
- 1976, Diffie και Hellman, Βραβείο Διεθνές Συνέδριο Πληροφορικής.

- Λύθηκε το πρόβλημα;
- Δυστυχώς ΟΧΙ. Πρέπει να επικοινωνούν ταυτόχρονα!!!



- Ανάγκη για Ασύμμετρο Κλειδί (Diffie).
- Η Γεωργία έχει το δικό της κλειδί και ο Κώστας το δικό του.
- Η Γεωργία έχει δυο κλειδιά, ένα για κρυπτογράφηση (δημόσιο) και ένα για αποκρυπτογράφηση (ιδιωτικό). Μόνο η Γεωργία μπορεί να αποκρυπτογραφήσει τα μηνύματά της.

- Ξεπεράστηκε το πρόβλημα της ανταλλαγής κλειδιών.
- Παρότι η Εύα γνωρίζει το δημόσιο κλειδί της Γεωργίας, δεν μπορεί να αποκρυπτογραφήσει ούτε αυτή αλλά ούτε και ο Κώστας.
- Πως θα γίνει αυτό μαθηματικά;;;;;;
- Ron **R**ivest, Adi **S**hamir and Len **A**dleman. (MIT)



- Η Γεωργία επιλέγει δύο γιγάντιους πρώτους π και ρ.
- Κρατά μυστικούς τους π και ρ και ανακοινώνει δημόσια το γινόμενό τους $\nu=\pi\rho$.
- Βρίσκει έναν αριθμό ε ο οποίος είναι πρώτος με το γινόμενο $(\pi-1)(\rho-1)=\varphi(\nu)$.
- $ΜΚΔ(\varepsilon, (\pi-1)(\rho-1))=1$.
- Ανακοινώνει επίσης και τον ε. Δηλαδή το ζεύγος ν και ε αποτελούν το δημόσιο κλειδί της Γεωργίας.
- Προφανώς η Εύα, όπως όλοι, γνωρίζει το δημόσιο κλειδί της Γεωργίας.

- Ο Κώστας θέλει να στείλει ένα γράμμα στην Γεωργία.
- Μετατρέπει το γράμμα σε αριθμό, ας είναι το κ ώστε
- $(\kappa, \nu)=1$.
- Ο Κώστας στέλνει το αποτέλεσμα της πράξης
- $\kappa^{\varepsilon} \mathrm{mod} \nu=\mu$ στη Γεωργία. Προφανώς η Εύα φροντίζει και τον υποκλέπτει.
- Η Γεωργία επέλεξε το ε έτσι ώστε να μπορεί να βρει έναν αριθμό α με την ιδιότητα $\varepsilon\alpha=1 \mathrm{mod}((\pi-1)(\varrho-1))$.
- Υπολογίζει λοιπόν, $\mu^{\alpha} \mathrm{mod} \nu=\kappa$. Δηλαδή ο αριθμός=γράμμα που ήθελε να της στείλει ο Κώστας.

- $\pi=61$ και $\rho=53$.
- $\nu=61\text{x}53=3233$, $\varphi(3233)=60\text{x}52=3120$.
- $\varepsilon=17$ και $(17, 3120)=1$.
- Κώστας $\kappa=65$, $65^{17}\text{mod}3233=2790$.
- Στέλνει ο Κώστας το 2790 στη Γεωργία.
- $(17, 3120)=1$ δίνει ακεραίους $\alpha=2753$ και $\beta=-15$ με
- $1=-15\text{x}3120+17\text{x}2753$.
- Η Γεωργία υπολογίζει $2790^{2753}\text{mod}3233=65$.

- Η Εύα παρότι γνωρίζει το 3233, το 17 και το 2790 δεν μπορεί να τα χρησιμοποιήσει αποτελεσματικά.
- Αν οι π και ρ είναι πρώτοι τάξης 10^{65} , τότε ο ν είναι τάξης 10^{130} . Ένας προσωπικός υπολογιστής για να τον παραγοντοποιήσει χρειάζεται 50 χρόνια.
- Αν συνδεθούν ταυτόχρονα 100.000.000 προσωπικοί υπολογιστές θα χρειασθούν 15 δευτερόλεπτα.
- Για τις τραπεζικές συναλλαγές το ν είναι τάξης 10^{310} .
- Με 100.000.000 υπολογιστές χρειάζονται περισσότερα από 100 χρόνια.

- Τελικά οι **R**ivest, **S**hamir και **A**dleman είχαν λύσει πρώτοι το πρόβλημα;

- GCHQ: UK Government Communications Headquarters 1960.
- **Clifford Christopher Cocks** (1950) (Cambridge)

is a British mathematician and cryptographer.
In 1973 he invented a public key crytography algorithm now known as the RSA algorithm, while working at the GCHQ.

MARCH 28, 2016

TIME

Apple CEO **Tim Cook** on his fight with the FBI and why he won't back down

BY LEV GROSSMAN

9 770928 843102 13 >

time.com

- «Ουδέν καλόν αμιγές κακού»
- Η κρυπτογράφηση προστατεύει και τους εγκληματίες:
- τρομοκρατία, διακίνηση ναρκωτικών, πορνεία, αγορά όπλων, εκβιασμοί.
- *Σκοπός*. Διευκόλυνση εμπορίου, πολιτών, αποτροπή εγκλήματος.
- Philip R. "Phil" Zimmermann, Jr., 1954. Flodida
- Επιχείρησε να ενθαρρύνει την ισχυρή

κρυπτογράφηση προς όφελος του προσωπικού απορρήτου. Η NSA κινήθηκε νομικά εναντίον του.

- Το RSA το οποίο εγγυάται απολύτως ασφαλή μηνύματα απαιτεί μεγάλη υπολογιστική ισχύ. Όταν ξεκίνησε το 1980 μόνο οι στρατιωτικοί και οι κυβερνήσεις είχαν αυτή τη δυνατότητα. Τότε η NSA μπορούσε να ελέγχει όλα τα μη-στρατιωτικά μηνύματα.
- Ο Zimmermann επινόησε ένα σύστημα κρυπτογράφησης το οποίο συνδυάζει το RSA με το κλασικό DES. Αυτό ήταν το Pretty Good Privacy PGP (1990).
- Ο κόσμος της πληροφορικής το υποδέχτηκε με μεγάλη θέρμη.

- Με την κλασική κρυπτογράφηση πρέπει τα δύο μέρη να έχουν το κλειδί. Τότε η κρυπτογράφηση γίνεται ασφαλής και σύντομη. Στην PGP χρησιμοποιούμε το RSA μόνο για να στείλουμε το κλειδί και το μήνυμα κρυπτογραφείται με τον κλασικό τρόπο DES.
- Με την PGP υπάρχει η δυνατότητα ψηφιακής υπογραφής. Δηλαδή πιστοποιείται η αληθινή ταυτότητα του συντάκτη.
- Ο Zimmermann κατόρθωσε και δημιούργησε ένα φιλικό περιβάλλον κρυπτογράφησης για προσωπικό υπολογιστή με πολύ καλά αποτελέσματα.

- Το FBI οδηγεί τον Zimmermann στα δικαστήρια για προδοσία. Το RCA έχει καταχωρηθεί σαν εξοπλιστικό πρόγραμμα και ο Zimmermann το εξήγαγε μέσω του PGP.
- ΔΙΛΛΗΜΑ. Εξασφαλίζει το απόρρητο των προσωπικών ψηφιακών επικοινωνιών αλλά και οι τρομοκράτες επικοινωνούν με ασφάλεια.

- *Οι κυβερνήσεις θα πρέπει να θεσπίσουν νόμους κατά της κρυπτογραφίας;;;;*

- Το μόνο όπλο εναντίον του εγκλήματος είναι η αποκρυπτογράφηση των μηνυμάτων και η παγίδευση των τηλεφωνικών συνδιαλέξεων. Το βαλιτσάκι της ΕΥΠ (NSA).
- Το PGPfone κρυπτογραφεί τις τηλεφωνικές συνδιαλέξεις.
- Οι τρομοκράτες επικοινωνούν στο διαδίκτυο με χρήση του RSA.
- Κατασκοπία. ΗΠΑ-Καναδάς-Αγγλία-Αυστραλία-Ισραήλ έχουν δημιουργήσει ένα παγκόσμιας εμβέλειας κατασκοπευτικό σύστημα με κέντρο το Yorkshire. Είναι το γνωστό Echelon. Με το PGP είναι άχρηστο.

Άρθρο 12 της Παγκόσμιας Διακήρυξης Ανθρωπίνων Δικαιωμάτων.

- *Κανείς δεν μπορεί να υφίσταται αυθαίρετες παραβιάσεις του ιδιωτικού, οικογενειακού, οικιακού και επικοινωνιακού απορρήτου, ούτε επιθέσεις κατά της τιμής και υπόληψής του. Όλοι έχουν δικαίωμα της προστασίας του νόμου εναντίον τέτοιων παραβιάσεων ή επιθέσεων.*