Κρυπτογραφία
Διάλεξη 1

21-2-2025

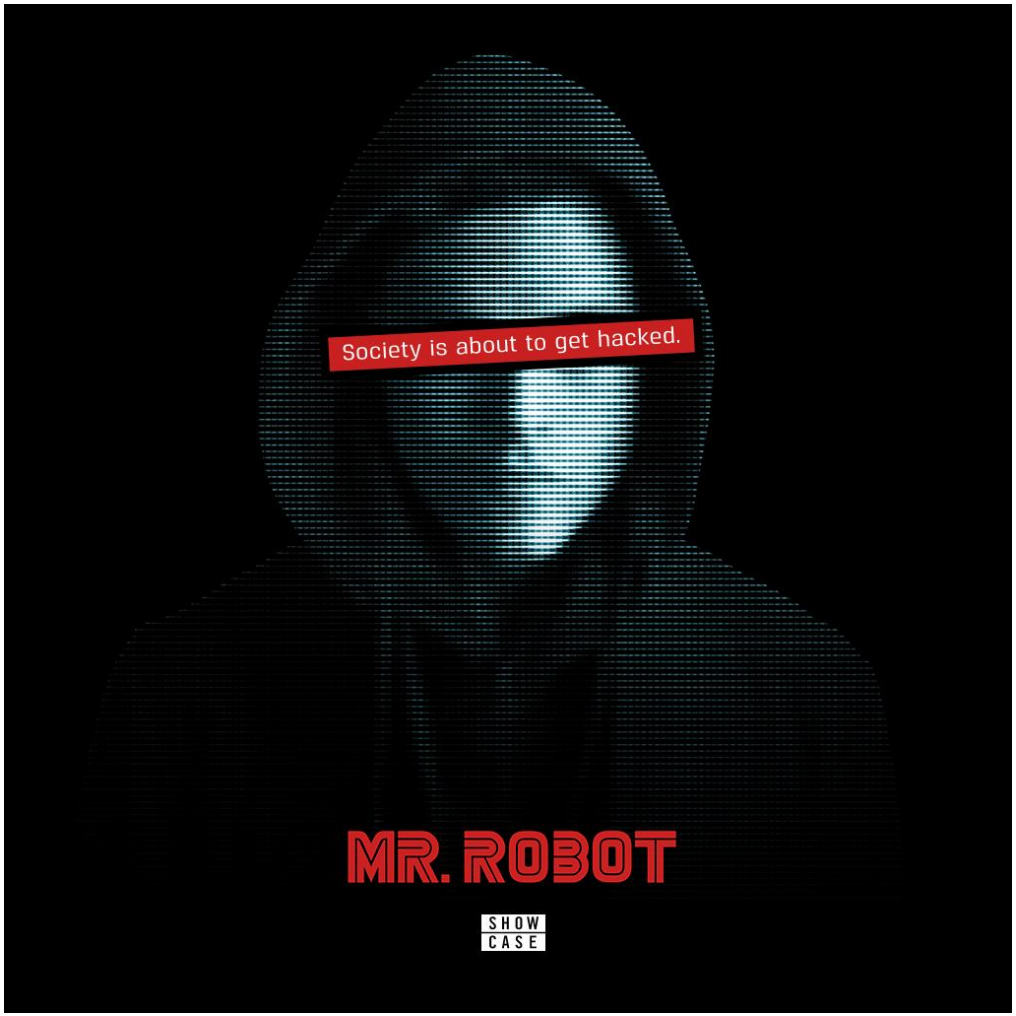
Νίκος Καρανικόλας
E-mail: nkaranik@ceid.upatras.gr
nkaran@gmail.com

Αντικείμενο μαθήματος

- Αντικείμενο του μαθήματος είναι το πεδίο της κρυπτογραφίας και της κρυπτανάλυσης, και ειδικότερα το μαθηματικό υπόβαθρο που διέπει τα αντίστοιχα κρυπτογραφικά πρωτόκολλα
- Θα εξετάσουμε τις αρχές λειτουργίας των παραδοσιακών και των σύγχρονων κρυπτογραφικών πρωτοκόλλων, με έμφαση στην κρυπτογράφηση, τη ψηφιακή υπογραφή, καθώς και πιο εξειδικευμένα πρωτόκολλα, όπως π.χ, τα πρωτόκολλα δέσμευσης
- Θα αναλύσουμε επίσης την σύνδεση της κρυπτογραφίας με τα πεδία του σχεδιασμού αλγορίθμων και της υπολογιστικής πολυπλοκότητας

Πληροφορίες μαθήματος

- Συνεπώς, το μάθημα απαιτεί καλή γνώση μαθηματικών
- Είναι κατά βάση θεωρητικό καθώς ανήκει στο τομέα των εφαρμογών και θεμελιώσεων
- Δεν θα διδαχτείτε να αποκρυπτογραφείτε κωδικούς, ούτε θα γίνεται χάκερ!



Πληροφορίες μαθήματος

- Ως βασικό εγχειρίδιο του μαθήματος προτείνεται το εξής:
- Β. Κάτος, Γ. Στεφανίδης. Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης. Ζυγός, 2003.
- Συμπληρωματική βιβλιογραφία:
- J. Katz, Y. Lindell. Introduction to modern cryptography. Chapman and Hall/CRC Press, 2014.
- D. Stinson. Cryptography: Theory and practice. Chapman and Hall/CRC Press, 2006.
- A.J. Menezes, P.C. van Oorshot, S.A. Vanstone. Handbook of applied cryptography. CRC Press, 1996.

Περιεχόμενο μαθήματος

- Οι γενικές θεματικές του μαθήματος είναι οι ακόλουθες:
- Κρυπτογραφικά πρωτόκολλα
- Αλληλεπίδραση αποστολέα παραλήπτη
- DES (Data Encryption Standard) - άλλα Block Ciphers
- Ασφαλείς ψευδοτυχαίες ακολουθίες αριθμών
- Κρυπτογραφία δημόσιου κλειδιού
- Ψηφιακές υπογραφές - πιστοποίηση αποστολέα

Αξιολόγηση μαθήματος

- Η αξιολόγηση του μαθήματος θα γίνει μέσω:
- Γραπτής εξέτασης όπου θα έχετε πρόσβαση στο σύγγραμμα του μαθήματος και στη συμπληρωματική βιβλιογραφία
  - Επιτρέπονται μόνο τυπωμένες σημειώσεις, τίποτα χειρόγραφο και όχι λυμένα θέματα

Κρυπτογραφία- Ορισμός

- Με τον όρο *κρυπτογραφία* εννοούμε τη μελέτη μαθηματικών τεχνικών που **στοχεύουν** στην εξασφάλιση θεμάτων που άπτονται της ασφάλειας μετάδοσης της πληροφορίας
  - Δηλαδή, η εμπιστευτικότητα, η πιστοποίηση ταυτότητας του αποστολέα και η διασφάλιση του αδιάβλητου της πληροφορίας.
- Plaintext : Το αρχικό κομμάτι πληροφορίας
- Κρυπτόγραμμα (ciphertext): Το κρυπτογραφημένο μήνυμα
- Encryption: Η διαδικασία της κρυπτογράφησης ενός μηνύματος
- Decryption: η διαδικασία αποκρυπτογράφησής του μηνύματος

Βασικοί όροι

- Εμπιστευτικότητα ή μυστικότητα (privacy): η διατήρηση της πληροφορίας κρυφής από όλους, εκτός από εκείνους που είναι εξουσιοδοτημένοι να τη δουν
- Ακεραιότητα των δεδομένων (data integrity): διασφάλιση του ότι η πληροφορία δεν έχει παραποιηθεί από μη εξουσιοδοτημένο μέσο
- Πιστοποίηση ταυτότητας (entity authentication ή identification): επιβεβαίωση της ταυτότητας ενός χρήστη
- Πιστοποίηση μηνύματος (message authentication): Επιβεβαίωση της πηγής της πληροφορίας
- Υπογραφή (signature): ένα μέσο προσάρτησης πληροφορίας ενός χρήστη στα μεταδιδόμενα δεδομένα, με στόχο την πιστοποίηση ταυτότητας

Στόχοι της κρυπτογραφίας

- Τα μηνύματα πρέπει να φτάνουν στο σωστό προορισμό
- Εμπιστευτικότητα: Μόνο ο παραλήπτης τους να μπορεί να τα λάβει και να τα δει (confidentiality)
- Πιστοποίηση της ταυτότητας του αποστολέα (authentication)
- Το μήνυμα δεν πρέπει να αλλοιωθεί κατά τη μεταφορά από μη εξουσιοδοτημένη οντότητα (data integrity)
- Όποια ενέργεια κάνει κάποιος (π.χ. πιστοποίηση ταυτότητας) δεν πρέπει αργότερα να μπορεί να την αρνηθεί (Non-repudiation)

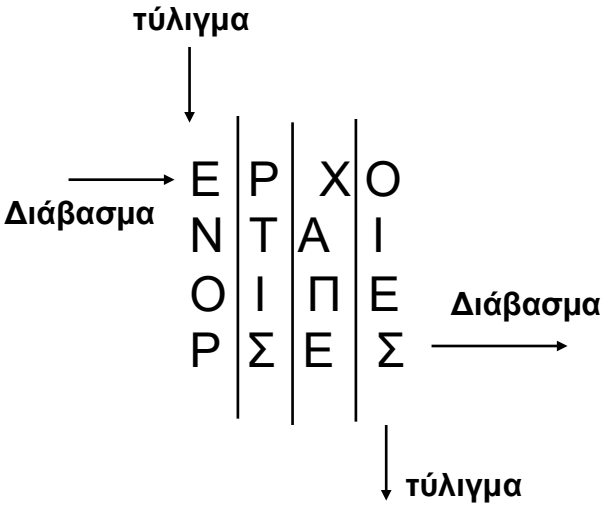
Κρυπτοσυστήματα και Κρυπτολογία

- Κρυπτοσύστημα (cryptosystem)
  - Ένα σύνολο από κρυπτογραφικές τεχνικές που χρησιμοποιείται για να παρέχει υπηρεσίες ασφάλειας
  - Αναφέρεται κυρίως στην εμπιστευτικότητα και στην κρυπτογράφηση (encryption)
- Κρυπτανάλυση (Cryptanalysis)
  - Μελέτη μαθηματικών τεχνικών για τη ματαίωση/ ακύρωση των υπηρεσιών ασφάλειας
- Κρυπτολογία (Cryptology)
  - Είναι η μελέτη της κρυπτογραφίας και της κρυπτανάλυσης

Σταθμοί στην ιστορία της Κρυπτογραφίας

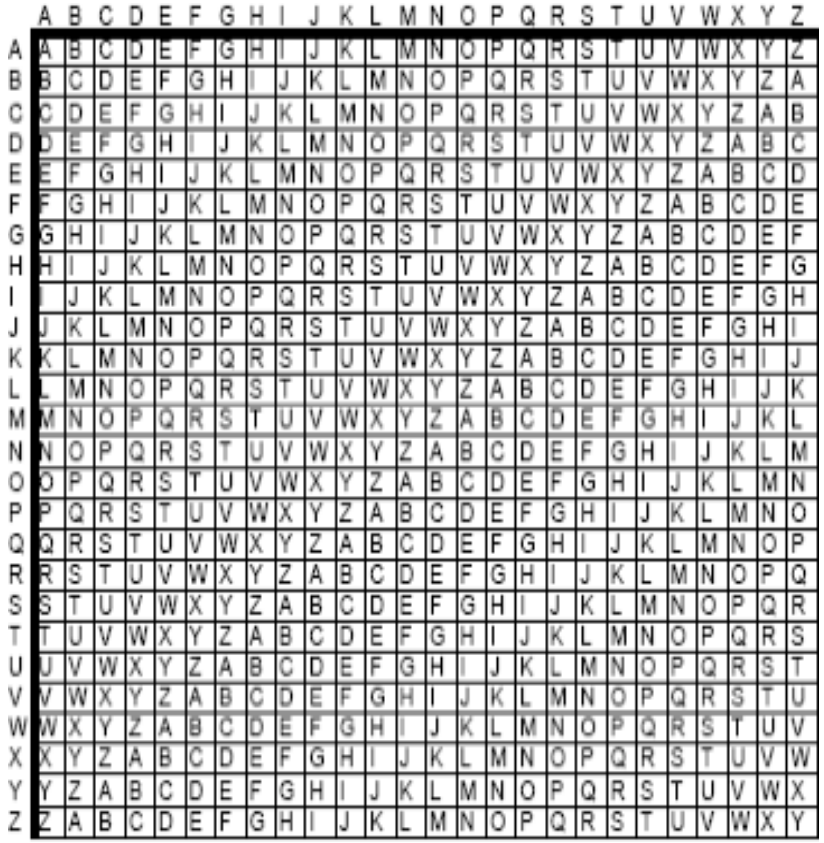
- Αρχ.Ελλάδα: Μέθοδος Σκυτάλης
- 15ος-16ος αιώνας Vigenere cipher – οι πρώτοι πολυαλφαβητικοί ciphers
- **1790 Jefferson** cylinder – ο πρώτος πολυαλφαβητικός και μηχανικός
- **1883 Kerckhoff** desirata – αξιώματα περί κρυπτογραφίας και ασφάλειας
- **1934 B. Hagelin** double-rotor devices (model M-209, 140.000 συσκευές) και **Enigma**
- **1949 C. Shannon** "Communication Theory of Secrecy Systems"
- **1970 – 1980 Feistel**, IBM, Feistel Cycles, Symmetric and Block Cryptography, **DES**
- **1976 Diffie, Hellman**: *New Directions in Cryptography*. Κρυπτογραφία δημοσίου κλειδιού
- **1978** Rivest, Shamir, Adleman (**RSA**) πρακτικό κρυπτοσύστημα δημοσίου κλειδιού + signature scheme
- **1984** C. H. Bennett and G. Brassard: πρωτόκολλο **BB84** (quantum crypto)
- **1994** U.S. Digital Signature Standard (**DSS**), based on the ElGamal scheme
- **2001** Advanced Encryption Standard (**AES**) adopted as US Standard

Αρχαία Ελλάδα – Σκυτάλη



- Αναφέρεται από τον Απολλώνιο το Ρόδιο
- Μια σκυτάλη και μια λωρίδα δέρματος με το μήνυμα
- Περίμετρος σκυτάλης: ίδια σε αποστολέα και παραλήπτη
- Μυστικό (ή Κλειδί): Περίμετρος σκυτάλης
- Για να κρυπτογραφηθεί ένα μήνυμα ο αποστολέας τυλίγει μια λωρίδα δέρματος ελικοειδώς στη σκυτάλη και το γράφει
- Ο παραλήπτης λαμβάνει τη λωρίδα με το μήνυμα και την τυλίγει στην σκυτάλη. Διαβάζει την μια πλευρά μετά την άλλη και αποκρυπτογραφεί

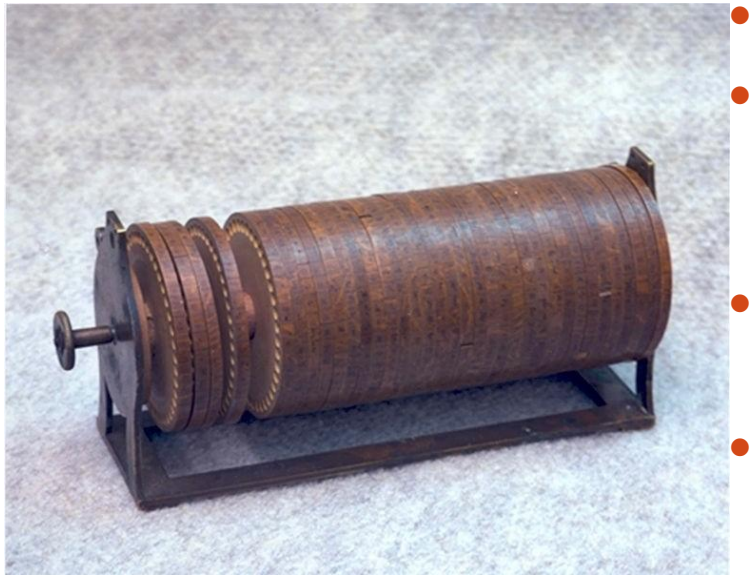
16ος Αιώνας Vigenère Cipher



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

- Ένας πίνακας αντικατάστασης λατινικών χαρακτήρων, διαστάσεις 26x26
- Κάθε γραμμή/στήλη ξεκινά απαρίθμηση γραμμάτων από το γράμμα που αντιστοιχεί
- Ο αποστολέας επιλέγει ένα κείμενο π.χ. plaintextmessage
- Ο αποστολέας επιλέγει μυστική λέξη και παράγει ακολουθία ίδιου μήκους με το κείμενο
- π.χ. Μυστική λέξη ΚΕΥ οπότε ακολουθία η ΚΕΥΚΕΥΚΕΥΚΕΥΚΕΥΚ
- Μυστικό (ή κλειδί) : η μυστική λέξη
- το παραγόμενο κρυπτοκείμενο προκύπτει από το περιεχόμενο του πίνακα που τέμνει η γραμμή του κειμένου και η στήλη του κλειδιού
- ZPYSRROBRWIQCEEO

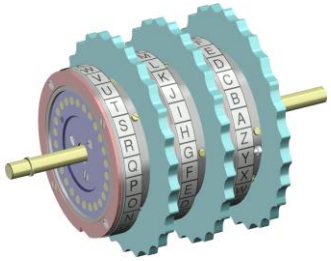
1790 – Κύλινδρος (ρότορας) Jefferson



- Περιστρεφόμενοι κύλινδροι
- Κάθε ένας: 26 γράμματα (τυχαία τοποθετημένα)
- Κύλινδροι στοιβαγμένοι με την ίδια σειρά σε αποστολέα και παραλήπτη
- Μυστικό (ή κλειδί) : η διάταξη της στοίβας
- Για να κρυπτογραφηθεί ένα ΜΗΝΥΜΑ ο αποστολέας περιστρέφει τους κυλίνδρους μέχρι να σχηματιστεί η λέξη σε μια γραμμή
- Κατόπιν επιλέγει να στείλει έξι γράμματα (π.χ., ΔΟΧΕΛΚ) από μία άλλη γραμμή που σχηματίζεται
- Ο παραλήπτης λαμβάνει το μήνυμα ΔΟΧΕΛΚ, και προσπαθεί να περιστρέψει (διατάξει) τους κυλίνδρους του για να το σχηματίσει
- Αν τα καταφέρει θα δει ότι σε μια άλλη γραμμή σχηματίζεται η λέξη ΜΗΝΥΜΑ την οποία και θεωρεί ως το κείμενο που ήθέλε να στείλει ο αποστολέας

1930-40 – Μηχανές Enigma

Οι συνεχόμενοι 3 ρότορες



Το βιβλίο κωδικών

- Η Enigma είναι μια ηλεκτρομηχανική συσκευή κρυπτογράφησης βασισμένη σε ρότορες, που χρησιμοποιήθηκε ευρέως στον Β' Παγκόσμιο Πόλεμο.
- Δομή και Συστατικά:

1. Μηχανικό μέρος:
   - Πληκτρολόγιο: Εισαγωγή των γραμμάτων προς κρυπτογράφηση
   - Ρότορες (3 - 8): Περιστρεφόμενοι κύλινδροι σε άξονα, ο καθένας με 26 θέσεις (A-Z).
   - Ανακλαστήρας: Αντανακλά το ηλεκτρικό σήμα, επιτρέποντας διπλή διέλευση μέσα από το σύστημα των ρότορων.
2. Ηλεκτρολογικό μέρος:
   - Κυκλώματα: Τα μονοπάτια του ρεύματος αλλάζουν δυναμικά ανάλογα με τη θέση των ρότορων.
   - Λαμπτήρες: Φωτίζουν το γράμμα που αντιστοιχεί στο κρυπτογραφημένο μήνυμα.

- Μυστικό (ή κλειδί) : αλλάζει από το codebook (π.χ., κάθε μέρα) και αφορά τη θέση των κυλίνδρων

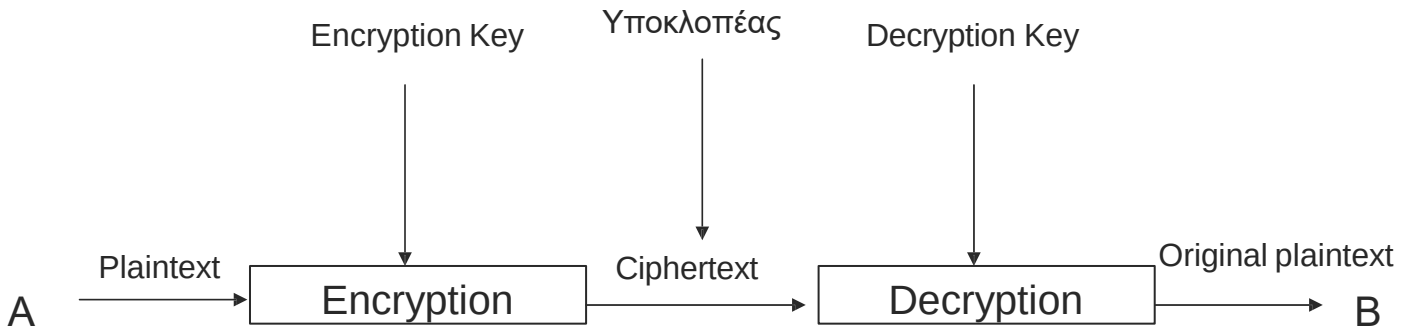
1930-40 – Μηχανές Enigma

- Πώς Λειτουργεί η Enigma

1. Ο χρήστης πατάει ένα γράμμα στο πληκτρολόγιο.
2. Το ηλεκτρικό σήμα περνά μέσα από:
   - Τον **πίνακα σύνδεσης (plugboard)**, αλλάζοντας το γράμμα σε άλλο (αν έχει οριστεί).
   - Τους **ρότορες**, οι οποίοι μεταβάλλουν τη διαδρομή του ρεύματος ανάλογα με τη θέση τους.
   - Τον **ανακλαστήρα**, που ανακατευθύνει το σήμα πίσω από τους ρότορες.
3. Το σήμα καταλήγει σε έναν λαμπτήρα, φωτίζοντας το τελικό κρυπτογραφημένο γράμμα.
4. Με κάθε πάτημα πλήκτρου, ο πρώτος ρότορας περιστρέφεται, αλλάζοντας τη διαμόρφωση του κυκλώματος.
5. Οι ρότορες αλλάζουν θέσεις σύμφωνα με το κλειδί της ημέρας, που ορίζεται από το codebook.

Αλγόριθμοι βασισμένοι σε κλειδιά (1970+)

- Οι αλγόριθμοι κρυπτογράφησης χρησιμοποιούν ένα ή περισσότερα κλειδιά (keys).



Η ασφάλεια έγκειται στο ότι δεν είναι γνωστό το κλειδί – οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης μπορούν να είναι ευρέως γνωστοί (αρχή του Kerchoff)

Βασικές αρχές του Shannon

- Οι αρχές αυτές εφαρμόζονται στην πράξη, αφού λαμβάνονται υπόψιν στην κατασκευή κρυπτογραφικών αλγορίθμων
- Διάχυση (Diffusion): κάθε γράμμα του αρχικού μηνύματος πρέπει να επηρεάζει όσο γίνεται περισσότερα γράμματα του κρυπτογράμματος
- Σύγχυση (Confusion): Η σχέση μεταξύ αρχικού μηνύματος και κρυπτογράμματος πρέπει να είναι σύνθετη, έτσι ώστε ο επιτιθέμενος να μην είναι σε θέση να προβλέψει αλλαγές στο κρυπτόγραμμα, με δεδομένες κάποιες μεταβολές στο αρχικό μήνυμα

Ένας απλός αλγόριθμος βασισμένος σε κλειδί

Κρυπτογράφηση

Πολλαπλασίασε το αρχικό μήνυμα επί 2 και πρόσθεσε το κλειδί

Αποκρυπτογράφηση

Αφαίρεσε το κλειδί και διαίρεσε το κρυπτόγραμμα διά 2

plaintext = **SECRET** = 19 5 3 18 5 20

Key = 3

Ciphertext = 41 13 9 39 13 43

Κατηγορίες αλγορίθμων ως προς το είδος του κλειδιού

- Αλγόριθμοι συμμετρικού (ή κρυφού) κλειδιού (symmetric key algorithms)
  - Χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση
- Αλγόριθμοι ασύμμετρου (ή δημοσίου) κλειδιού (Asymmetric (or public key) algorithms)
  - Χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση
  - Το κλειδί κρυπτογράφησης δεν μπορεί να εξαχθεί από το κλειδί αποκρυπτογράφησης

Μαθηματικός φορμαλισμός

Αν E και D συμβολίζουν τις συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης αντίστοιχα, τότε:

- $E_{K1}(m) = c$
- $D_{K2}(c) = m$

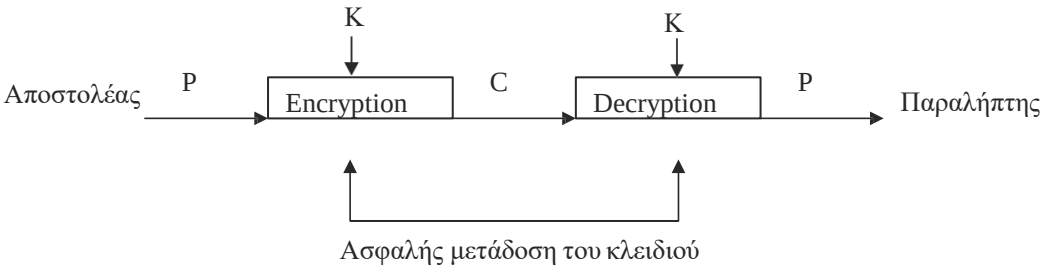
όπου m και c υποδηλώνουν το αρχικό και το κρυπτογραφημένο μήνυμα αντίστοιχα.

Οι δείκτες Ki υποδηλώνουν την εξάρτηση των συναρτήσεων από το κλειδί.

Οι συναρτήσεις έχουν την ιδιότητα: $D_{K2}(E_{K1}(m)) = m$

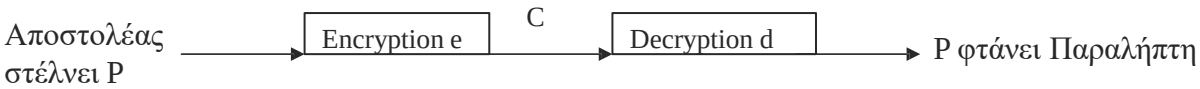
Σε αλγόριθμους συμμετρικού κλειδιού, ισχύει K1 = K2

Συμμετρικά κρυπτοσυστήματα



- Ο αποστολέας και ο παραλήπτης πρέπει από την αρχή να συμφωνήσουν στη χρήση ενός κοινού κλειδιού Κ.
- Ένα «ασφαλές κανάλι επικοινωνίας» πρέπει να υπάρχει για την επικοινωνία τους προκειμένου να ενημερώσει ο ένας τον άλλον για τον κλειδί.

Κρυπτοσυστήματα Δημοσίου κλειδιού (ασύμμετρα)



- 70s
- Κάθε συμμετέχων στο σύστημα κατέχει ένα ζευγάρι κλειδιών e και d, που το ένα αντιστρέφει το άλλο: $D_d(E_e(m))=m$
- Το κλειδί e σε κάθε χρήστη είναι ευρέως γνωστό σε όλους, ενώ το d κρατείται μυστικό και το ξέρει μόνο ο κάτοχός του. Απαραίτητη προϋπόθεση για την ασφάλεια του συστήματος είναι το εξής: η γνώση του δημοσίου κλειδιού δεν πρέπει να επιτρέπει τον προσδιορισμό του ιδιωτικού κλειδιού.
- Σύγκριση με τους αλγορίθμους συμμετρικού κλειδιού: Η ανταλλαγή κλειδιών μεταξύ αποστολέα και παραλήπτη αντικαθίσταται από την ύπαρξη ενός διαφανούς καταλόγου, στον οποίο όλοι έχουν πρόσβαση, και περιέχει τα δημόσια κλειδιά e όλων των συμμετεχόντων.

Τρόπος λειτουργίας συστημάτων δημοσίου κλειδιού

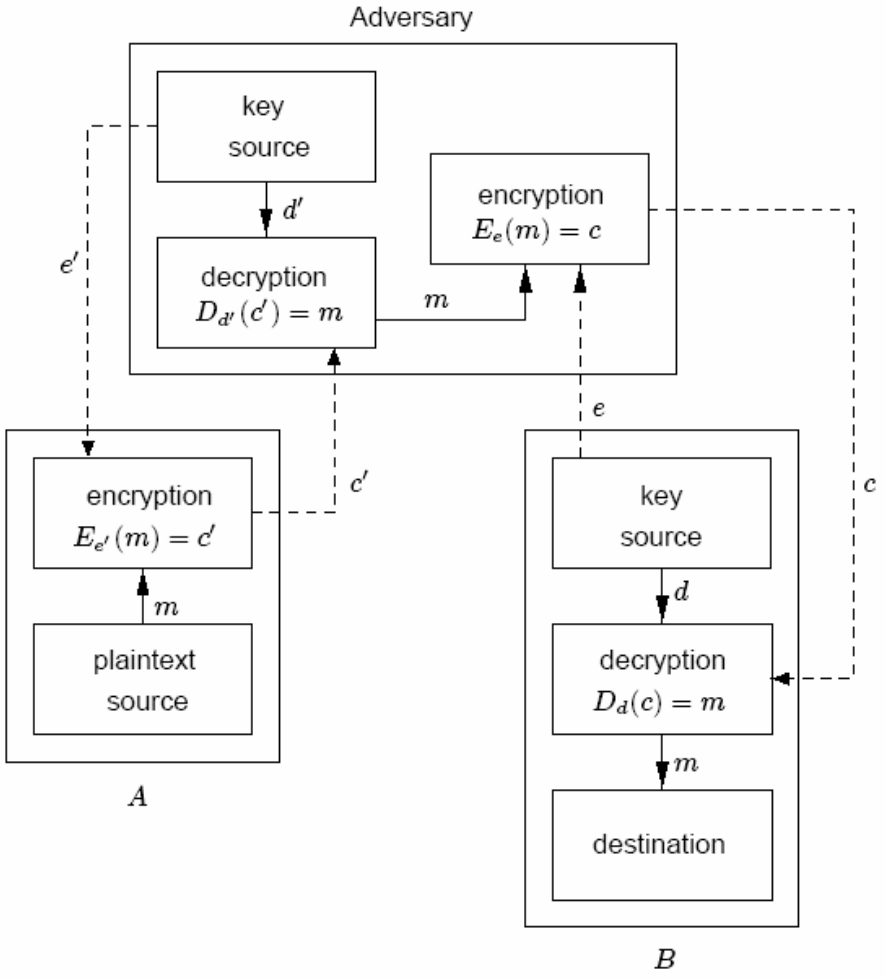
- Έστω e_A, d_A και e_B,d_B τα δημόσια και ιδιωτικά κλειδιά των Α, Β αντίστοιχα.
- Όταν ο Α θέλει να στείλει ένα μήνυμα m στον Β, το δημόσιο κλειδί κρυπτογράφησης του παραλήπτη Β χρησιμοποιείται για τη δημιουργία του κρυπτογράμματος $E_{eB}(m)$
- Αφού το e_B είναι πλήρως διαθέσιμο σε κάποιον δημόσιο κατάλογο στον οποίο έχουν όλοι πρόσβαση, ο οποιοσδήποτε μπορεί να κρυπτογραφήσει ένα μήνυμα με προορισμό τον Β
- Ωστόσο, μόνο ο Β, ο οποίος έχει πρόσβαση στο ιδιωτικό του κλειδί αποκρυπτογράφησης d_B μπορεί να ανακατασκευάσει το αρχικό μήνυμα, εφαρμόζοντας τον αντίστροφο μετασχηματισμό:
    - $D_{dB}(E_{eB}(m))$.

Μειονέκτημα συστημάτων δημοσίου κλειδιού

- Ο οποιοσδήποτε μπορεί να προσποιηθεί ότι είναι κάποιος άλλος χρήστης
- Αν ο επιτιθέμενος «σταματήσει» το μήνυμα που στέλνει ο Α στον Β, γράψει ένα δικό του και το στείλει στον Β κρυπτογραφημένο με το δημόσιο κλειδί του Β, ο Β δεν θα γνωρίζει τον πραγματικό αποστολέα του μηνύματος που λαμβάνει
- Άρα υπάρχει ανάγκη πιστοποίησης της ταυτότητας κάθε χρήστη

Σχηματική αναπαράσταση υποκλοπής σε σύστημα Δημοσίου Κλειδιού

- Ο επιτιθέμενος ξεγελά τον Α ότι είναι ο Β, στέλνοντάς του το δικό του δημόσιο κλειδί e'. Έτσι, ο Α στέλνει τα μηνύματα κρυπτογραφημένα ως προς το e'. Συνεπώς, ο επιτιθέμενος μπορεί και «διαβάζει» όλα τα μηνύματα που στέλνει ο Α στον Β
- Ο Β δεν μπορεί να αντιληφθεί την παρουσία του επιτιθέμενου, μια που αυτός του στέλνει κανονικά το μήνυμα. Ο Β, λαμβάνοντας ένα μήνυμα, δεν μπορεί να ξέρει με σιγουριά ποιος του το έστειλε



«Επιθέσεις» εναντίον κρυπτογραφικών αλγορίθμων (Κρυπτανάλυση)

- Κρυπτανάλυση είναι η μελέτη μαθηματικών τεχνικών που στοχεύουν στην ακύρωση των κρυπτογραφικών μεθόδων, καθιστώντας τις έτσι μη κατάλληλες για κρυπτογραφικούς σκοπούς
  - ουσιαστικά η προσπάθεια για την εύρεση του μυστικού κλειδιού
- Ένας αλγόριθμος θεωρείται μη ασφαλής αν είναι δυνατή η ανάκτηση του αρχικού μηνύματος ή του **κλειδιού** από το κρυπτόγραμμα

«Επιθέσεις» εναντίον κρυπτογραφικών αλγορίθμων (Κρυπτανάλυση)

- Είδη «επιθέσεων»
  - Ciphertext attack: ο επιτιθέμενος γνωρίζει το κρυπτόγραμμα: στόχος η εύρεση είτε του αρχικού μηνύματος είτε του **κλειδιού**
  - Known-plaintext attack: ο επιτιθέμενος γνωρίζει το κρυπτόγραμμα και το αντίστοιχο (μη κρυπτογραφημένο) μήνυμα – στόχος του η εύρεση του **κλειδιού**
  - Chosen-plaintext attack: ο επιτιθέμενος είναι σε θέση να επιλέξει συγκεκριμένα ζεύγη «αρχικό μήνυμα – κρυπτόγραμμα» που θα γνωρίζει. Στόχος του η εύρεση του **κλειδιού**

Κατηγοριοποίηση κρυπτογραφικών συστημάτων

- Block ciphers (αλγόριθμοι τμήματος/μπλοκ): Το αρχικό μήνυμα χωρίζεται σε blocks, όπου το καθένα κρυπτογραφείται ξεχωριστά.
  - Πλεονεκτήματα:
  - Πιο εύκολη στην υλοποίηση σε σχέση με τους stream
  - Ο επιτιθέμενος δεν μπορεί να προσθέσει bits (λόγω του σταθερού μήκους μπλοκ που έχουν αυτοί οι αλγόριθμοι)
- Stream ciphers (αλγόριθμοι ροής): Το μήνυμα κρυπτογραφείται bit προς bit (ή byte προς byte)
  - Πλεονεκτήματα:
  - Πολύ υψηλή ταχύτητα (εφαρμογή σε τηλεδιασκέψεις κτλ)
  - Δεν υπάρχει διάδοση σφάλματος (αφού το κάθε bit μηνύματος επηρεάζει μόνο ένα bit του κρυπτογράμματος)
  - Λιγότερη μνήμη