ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Οικονομικό Πανεπιστήμιο Αθηνών
Τμήμα Πληροφορικής
ΠΜΣ στα Πληροφοριακά Συστήματα

Κρυπτογραφία και Εφαρμογές
Διαλέξεις Ακ. Έτους 2018-2019

Περιεχόμενα Μαθήματος – Θεματικές Ενότητες

- Θ.Ε.1: Εισαγωγικές Έννοιες
  - ✓ Ορισμοί
  - ✓ Εννοιολογική Θεμελίωση
- Θ.Ε.2: Θεωρία Αριθμών και Θεωρία Ομάδων
  - ✓ Διαιρεσιμότητα, Πρώτοι αριθμοί / ΜΚΔ, Αλγόριθμοι Ευκλείδη
  - ✓ Αριθμητική υπολοίπων, Κινέζικο θεώρημα υπολοίπων
  - ✓ Ομάδες, Δακτύλιοι, Πεδία, Πεδία Galois
- Θ.Ε.3: Ιστορική αναδρομή – κλασσική κρυπτογραφία
  - ✓ Substitution / Permutation Ciphers
  - ✓ Shift, Affine, Vigenere Ciphers
  - ✓ Stream Ciphers

Περιεχόμενα Μαθήματος – Θεματικές Ενότητες

- Θ.Ε.4: Συμμετρική κρυπτογραφία τμημάτων
  - ✓ Shannon's principles
  - ✓ Permutation Networks
  - ✓ DES/3DES, AES
- Θ.Ε.5: Κρυπτογραφία Δημοσίου Κλειδιού (Public Key Cryptosystems)
  - ✓ RSA
  - ✓ El Gamal
- Θ.Ε.6: Συναρτήσεις Κατακερματισμού και Ψηφιακές Υπογραφές
  - ✓ Collision resistant hash functions
  - ✓ Secure Hash Algorithm (SHA)
  - ✓ ElGamal Signature Scheme
  - ✓ Digital Signature Standard - πρότυπο ψηφιακών υπογραφών ISO/IEC 9796–2

Περιεχόμενα Μαθήματος – Θεματικές Ενότητες

- Θ.Ε.7: Key Management - PKI
  - ✓ Diffie-Hellman key distribution
  - ✓ Public Key Infrastructures
  - ✓ Certification Authorities
- Θ.Ε.8: Openssl - Keytool Lab
  - ✓ Δημιουργία Αρχής Πιστοποίησης
  - ✓ Παραγωγή Κλειδιών
  - ✓ Δημιουργία Ψηφιακών Υπογραφών
- Θ.Ε.9: Cryptool – PGP Lab
  - ✓ Παρουσίαση λειτουργίας των βασικών αλγορίθμων
  - ✓ Εισαγωγή στο PGP
  - ✓ Δημιουργία και χρήση PGP κλειδιών

Περιεχόμενα Μαθήματος – Θεματικές Ενότητες

- Θ.Ε.10: Εφαρμογές Κρυπτογραφίας
  - ✓ Cryptography on the Internet (SSL Protocol, SSH)
  - ✓ Cryptography in Wireless networks (WPA, WEP)
  - ✓ Cryptography for Secure payment card transactions

- Συνολικά 10 θεματικές ενότητες για 10-11 διαλέξεις

Διαφάνειες

- Διαθέσιμες 1-2 μέρες πριν από κάθε διάλεξη στο eclass
  - ✓ http://eclass.aueb.gr/
  - ✓ Γραφτείτε στο «Κρυπτογραφία και Εφαρμογές - Μερικούς φοίτησης - 2019»
- Οι τελικές διαφάνειες θα αναρτώνται ξανά μετά το μάθημα και μετά από τυχόν διορθώσεις – παρατηρήσεις

Διαδικαστικά

- Ώρες γραφείου
  - ✓ 4ος όροφος Αντωνιάδου
  - ✓ Δευτέρα 12:00 – 13:00 και Τρίτη 13:00 – 15:00
  - ✓ Καθώς και συναντήσεις μετά από αίτημά σας (by email)
- Βαθμολόγηση
  - ✓ Τελικό διαγώνισμα: 9 μονάδες
  - ✓ 2 σειρές ασκήσεων: 1.5 - 2 μονάδες σύνολο
    - 1η σειρά: ασκήσεις/ερωτήσεις πάνω σε θεωρία αριθμών, συμμετρική κρυπτογραφία, κρυπτογραφία δημοσίου κλειδιού
    - 2η σειρά: ασκήσεις πάνω στα εργαστηριακά παραδείγματα (Openssl, keytool, κλπ)

Βιβλιογραφία

- Βασικά βιβλία
  - ✓ Douglas Stinson, “Cryptography: Theory and Practice” 2nd or 3rd edition, Chapman & Hall/CRC Press
  - ✓ Β. Κάτος, Γ. Στεφανίδης, «Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης», Εκδόσεις Ζυγός, 2003
  - ✓ J. Menezes, P. C. van Oorschot, and S. A. Vanstone, “Handbook of Applied Cryptography”, CRC Press, October 1996
- Συμπληρωματικά
  - ✓ N. Ferguson and B. Schneier, “Practical Cryptography”, John Wiley & Sons, 1st edition, 2003
  - ✓ Keith M. Martin, “Everyday Cryptography: Fundamental Principles and Applications”
  - ✓ W. Stallings, “Network Security Essentials: Applications and Standards”, Prentice Hall, 3rd Edition, 2006
  - ✓ T. Cormen, C. Leiserson, R. Rivest and C. Stein, “Introduction to Algorithms”, 3rd Edition, The MIT Press, 2009 (για θεωρία αριθμών και κρυπτογραφία δημοσίου κλειδιού)

Σταθμοί στην ιστορία της Κρυπτογραφίας

Αρχ. Ελλάδα Μέθοδος Σκυτάλης

Μέχρι 15ο αιων. Μονοαλφαβητικοί κώδικες

15ος-16ος αιών. **Vigenere** cipher – οι πρώτοι πολυαλφαβητικοί ciphers

1790 **Jefferson** cylinder – ο πρώτος πολυαλφαβητικός και μηχανικός

1883 **Kerckhoff** desiderata – 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 Cycles (IBM), Symmetric and Block Cryptography , **DES** becomes U.S. Federal Information Processing Standard (FIPS)

1976 **Diffie, Hellman**: *New Directions in Cryptography*. Κρυπτογραφία δημοσίου κλειδιού

1978 Rivest, Shamir, Adleman (**RSA**) πρακτικό κρυπτοσύστημα δημοσίου κλειδιού + signature scheme

1994 U.S. Digital Signature Standard (**DSS**), based on the ElGamal scheme

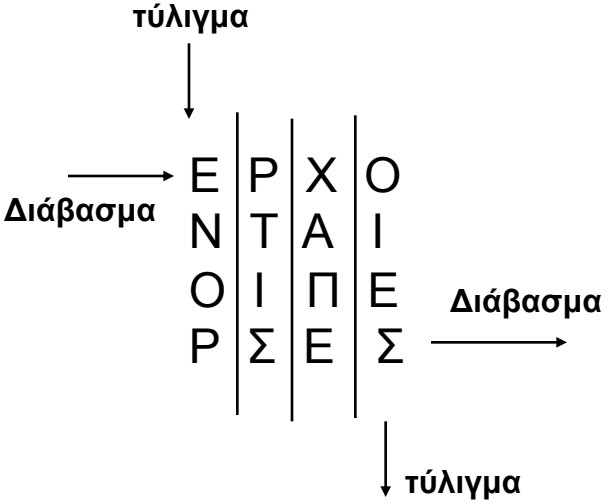
2001 Advanced Encryption Standard (**AES**) adopted as US Standard

Στις μέρες μας: συνδυασμοί ιδεών από symmetric + public-key crypto, ανάπτυξη νέων πρωτοκόλλων, rational cryptography,…

Σταθμοί

Αρχαία Ελλάδα – Σκυτάλη

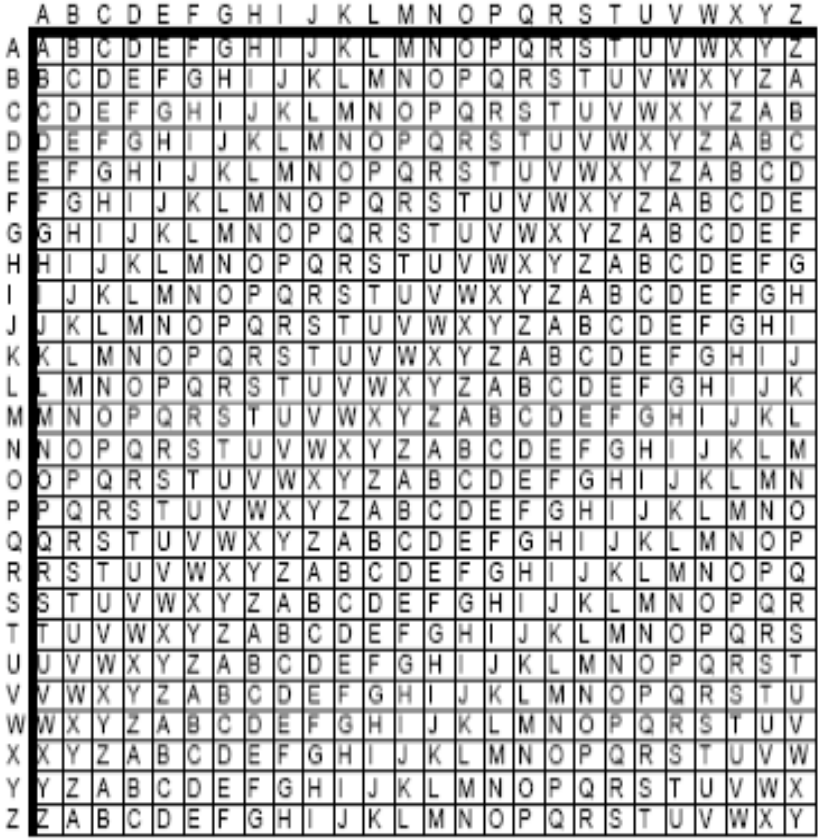
Εικόνα από wikipedia



- 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 του. Διαβάζει την μια πλευρά μετά την άλλη και έτσι αποκρυπτογραφεί

Σταθμοί

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

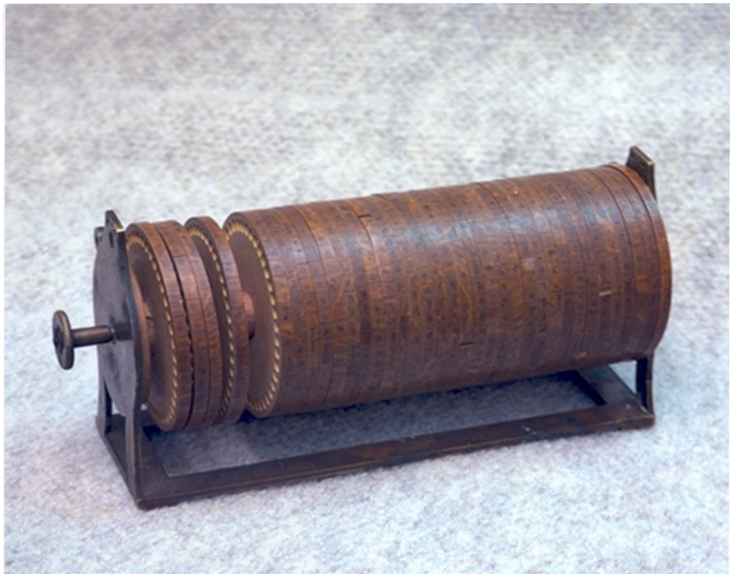
tabula recta, Johannes Trithemius

Η ιστορία είναι άδικη απέναντι στον G. B. Bellaso που μάλλον ανακάλυψε πρώτος τη μέθοδο

- Ένας πίνακας αντικατάστασης λατινικών χαρακτήρων
  - Διαστάσεις 26x26
  - Κάθε γραμμή / στήλη ξεκινά απαρίθμηση γραμμάτων από το γράμμα που τις 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 KEY οπότε ακολουθία η KEYKEYKEYKEYKEYK
  - 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

Σταθμοί

1790 – Κύλινδρος (ρότορας) Jefferson



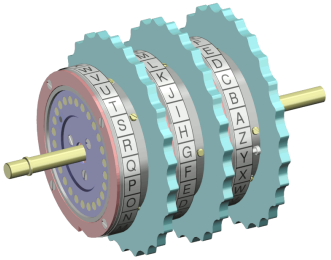
Εικόνα από wikipedia

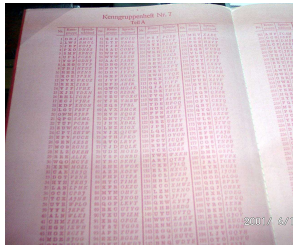
- Περιστρεφόμενοι κύλινδροι
- Κάθε ένας: 26 γράμματα (τυχαία τοποθετημένα)
- Κύλινδροι στοιβαγμένοι με την ίδια σειρά σε αποστολέα και παραλήπτη
  - Μυστικό **(ή κλειδί)** : η διάταξη της στοίβας
- Για να κρυπτογραφηθεί ένα ΜΗΝΥΜΑ ο αποστολέας περιστρέφει τους κυλίνδρους μέχρι να σχηματιστεί η λέξη σε 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

Σταθμοί

1930-40 – Μηχανές Enigma

Οι συνεχόμενοι 3 ρότορες Εικόνα από wikipedia



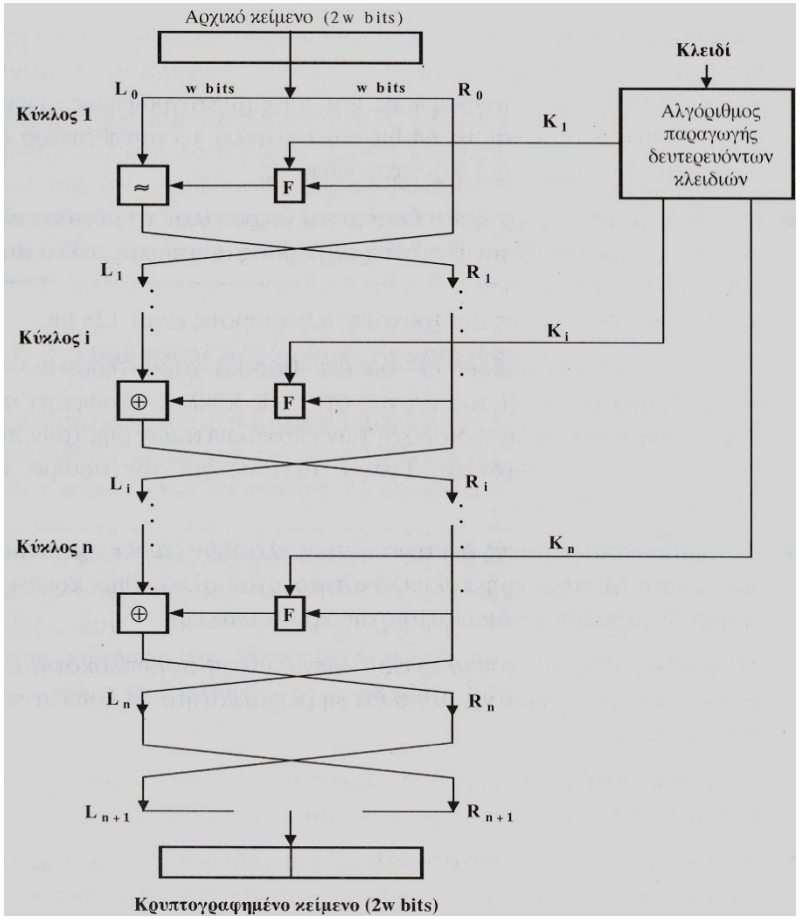


Το βιβλίο κωδικών (wikipedia)

- Ηλεκτρο-μηχανικές συσκευές με βιβλίο κωδικών
- Αντικαθίσταται ένα γράμμα κάθε φορά με άλλο ανάλογα με τη τρέχουσα διαμόρφωση της διάταξης
  - πολυ-αλφαβητική αντικατάσταση
- Μηχανικό μέρος:
  - Πληκτρολόγιο
  - Συνεχόμενοι (3 - 8) περιστρεφόμενοι κύλινδροι σε άξονα
  - Κάθε ένας: L=26 γράμματα (με τη σειρά)
- Ηλεκτρολογικό μέρος:
  - κυκλώματα που κλείνουν ανάλογα με τη θέση των κυλίνδρων
  - λαμπτήρες που δείχνουν το κρυπτόγραμμα που επιλέγεται
- Μυστικό (ή κλειδί) : αλλάζει από το codebook
  - (π.χ., κάθε μέρα) και αφορά τη θέση των κυλίνδρων

Σταθμοί

1970-80 – Feistel Network



- Δίκτυο N επιπέδων
  - Σε κάθε επίπεδο ισοδύναμες λειτουργίες αντικατάστασης, μετάθεσης, διάσπασης, επέκτασης και ανάμιξης (XOR) του κειμένου με το κλειδί
  - ξεχωριστό κλειδί σε κάθε κύκλο
- Δομή χιονοστιβάδας (**Avalanche**)

  "*As the input moves through successive layers the pattern of 1's generated is amplified and results in an unpredictable avalanche. In the end the output will have, on average, half 0's and half 1's*"

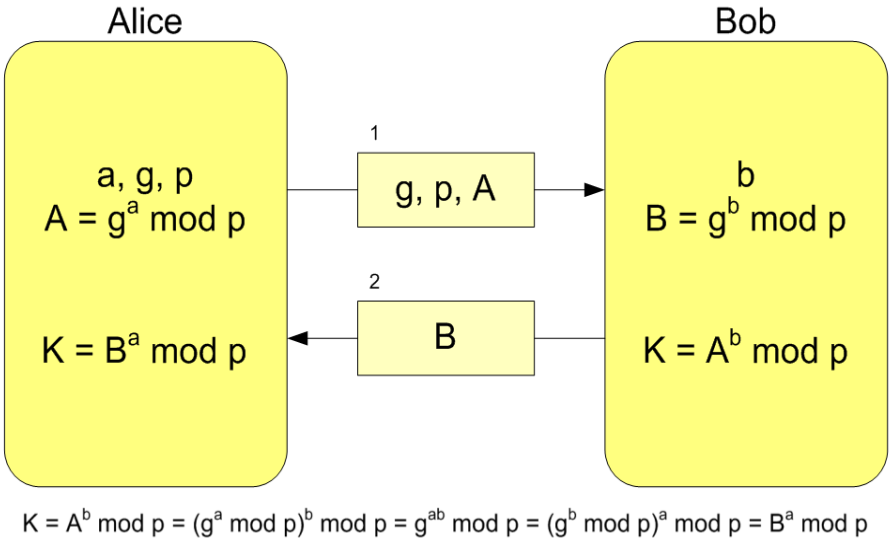
  Feistel, H. 1973. Cryptography and Computer Privacy. Scientific American
  - Ανεπαίσθητη αλλαγή στο input: Παράγει πολλαπλές αλλαγές στον 1ο κύκλο, περισσότερες στο 2ο, κοκ
  - Τελικά το μισό block αλλάζει κατά μέσο όρο
- Blowfish, CAST-128, DES, FEAL, Lucifer, MARS, RC5, Triple DES, Twofish, GOST

Σταθμοί

1970-80: [Diffie, Hellman] + [Rivest, Shamir, Adleman]

Κρυπτογραφία Δημοσίου Κλειδιού

Οι χρήστες μπορούν να δημοσιοποιούν πληροφορία σχετική με την παραγωγή του ιδιωτικού κλειδιού



- Παράδειγμα: Πρωτόκολλο για το πρόβλημα διανομής κλειδιού
- Ένας απο τους δύο (Alice) απομακρυσμένους χρήστες ανακοινώνει έναν πρώτο αριθμό p, και μία βάση g, καθώς και ένα **δημόσιο κλειδί A**
  - κρατά μυστικό το κλειδί **a**
- Ο δεύτερος (Bob) λαμβάνει τους αριθμούς αυτούς και υπολογίζει το δικό του **δημόσιο κλειδί B**
  - κρατά μυστικό το κλειδί **b**
- Με βάση τα **A** και **B** υπολογίζεται και από τους δύο το κοινό κλειδί **K**
- Κανείς άλλος δεν μπορεί να υπολογίσει το ίδιο **K** γιατί δεν γνωρίζει τα **a** και **b**

Ορισμός Κρυπτογραφίας

Η Κρυπογραφία ασχολείται με: τη μελέτη μαθηματικών τεχνικών που σχετίζονται με θέματα ασφάλειας πληροφοριών

Στόχος: Η αποτροπή ή ανίχνευση απάτης, υποκλοπής, ή άλλης κακόβουλης πράξης που σχετίζεται με τα δεδομένα και τις πληροφορίες

Εφαρμογές Κρυπτογραφίας

- ✓ εμπιστευτικότητα ή ιδιωτικότητα δεδομένων (**confidentiality**)
- ✓ ακεραιότητα δεδομένων (**data integrity**)
- ✓ αυθεντικοποίηση οντοτήτων (**entity authentication**)
- ✓ αυθεντικότητα πηγής προέλευσης δεδομένων (**data origin authentication**)
- ✓ υπογραφή (**signature**) – σχετίζει πληροφορία με χρήστη
- ✓ μη-αποποίηση ενεργειών (**non-repudiation**)
- ✓ εξουσιοδότηση (**authorization**) – έγκριση σε κάποια οντότητα ότι είναι ή μπορεί να κάνει κάτι
- ✓ έλεγχος πρόσβασης (**access control**) – περιορισμός χρήσης πόρων μόνο σε κατέχοντες προνόμια
- ✓ πιστοποίηση (**certification**) – επιβεβαίωση πληροφορίας από έμπιστη οντότητα
- ✓ χρονοσήμανση (**timestamping**) – διαβεβαίωση χρόνου συναλλαγής ή ενέργειας
- ✓ Ανωνυμία (**anonymity**) – απόκρυψη της οντότητας που συμμετέχει σε μια διαδικασία

Κρυπτοσυστήματα και Κρυπτολογία

- ✓ Κρυπτοσύστημα (Cryptosystem)
  - Ένα σύνολο από κρυπτογραφικές τεχνικές που χρησιμοποιείται για να παρέχει υπηρεσίες ασφάλειας
  - Αναφέρεται κυρίως σε τεχνικές κρυπτογράφησης
- ✓ Κρυπτανάλυση (Cryptanalysis)
  - Μελέτη μαθηματικών τεχνικών για τη ματαίωση / ακύρωση των υπηρεσιών ασφάλειας (ουσιαστικά η προσπάθεια για την εύρεση του μυστικού κλειδιού)
- ✓ Κρυπτολογία (Cryptology)
  - Είναι η μελέτη της κρυπτογραφίας και της κρυπτανάλυσης

Κρυπτοσυστήματα

Σε ένα κρυπτοσύστημα πρέπει να ορίσουμε πρώτα τα εξής:

A: Αλφάβητο ορισμού

π.χ. A = {0,1}, ή A = {0,1,...,9} ή A = {A, B, ..., Z}

P: Χώρος μηνύματος (plaintext ή message space)

Αποτελείται από ακολουθίες συμβόλων από το A. Ένα στοιχείο του P καλείται plaintext. Π.χ. binary strings, Ελληνικό κείμενο, κ.ο.κ.

C: Χώρος κρυπτογραφήματος (ciphertext space)

Αποτελείται από ακολουθίες συμβόλων από το αλφάβητο που χρησιμοποιούμε για την κρυπτογράφηση (μπορεί να διαφέρει από το A). Ένα στοιχείο του C καλείται ciphertext ή code

K: Χώρος κλειδιών (key space)

Ένα στοιχείο από το K καλείται κλειδί (key), π.χ. ακολουθίες 512 bits

Κρυπτοσυστήματα

Σε κάθε κρυπτοσύστημα πρέπει επίσης να καθορίσουμε:

- Τις πιθανές συναρτήσεις κρυπτογράφησης (encryption functions)
  - Συνήθως παραμετροποιούνται με βάση το κλειδί
  - Για κάθε κλειδί $k \in K$ υπάρχει μία συνάρτηση κρυπτογράφησης
    $e_k : P \rightarrow C$
- Τις πιθανές συναρτήσεις αποκρυπτογράφησης (decryption functions)
  - Για κάθε κλειδί $k \in K$ και συνάρτηση κρυπτογράφησης e_k υπάρχει μία αντίστοιχη συνάρτηση αποκρυπτογράφησης
    $d_k : C \rightarrow P$, έτσι ώστε $d_k(e_k(x)) = x$ για κάθε $x \in P$
- Παρατήρηση: Η συνάρτηση e_k πρέπει να είναι 1-1 για να μην υπάρχει αμφιβολία στην αποκρυπτογράφηση:
  - Αν $y = e_k(x_1) = e_k(x_2)$ δεν ξέρουμε αν το μήνυμα ήταν x_1 ή x_2

Συμμετρική κρυπτογραφία και κρυπτογραφία δημοσίου κλειδιού

Έστω ένα σχήμα κρυπτογραφίας που αποτελείται από τις συναρτήσεις $\{e_K, k \in K\}$ και $\{d_k, k \in K\}$, όπου K ο χώρος κλειδιών

Το σχήμα αναφέρεται ως **symmetric-key encryption scheme** αν για κάθε ζεύγος (e_k, d_k), είναι **υπολογιστικά εφικτό** να προσδιοριστεί το d_k γνωρίζοντας μόνο το e_k, ή να προσδιοριστεί το e_k από το d_k

Σε πολλές περιπτώσεις $e_k = d_k$

Αναφέρεται ως *συμμετρική* ή *συμβατική* ή *single-key* ή *private key* κρυπτογραφία

Παραδείγματα: DES/3DES, AES, RC5/6, CAST-128/256, Lucifer, Blowfish, IDEA, FEAL, COST, MARS …

Συμμετρική κρυπτογραφία και κρυπτογραφία δημοσίου κλειδιού

Έστω ένα σχήμα κρυπτογραφίας που αποτελείται από τις συναρτήσεις $\{e_K, k \in K\}$ και $\{d_k, k \in K\}$, όπου K ο χώρος κλειδιών

Το σχήμα αναφέρεται ως **public-key encryption scheme** αν για κάθε ζεύγος κλειδιών (e_k, d_k), ο αλγόριθμος κρυπτογράφησης e_k (*public key*) είναι δημόσια διαθέσιμος, ενώ το d_k (*private key*) είναι μυστικό

Για την κρυπτογράφηση, μπορούμε πλέον να έχουμε δημόσια ένα ευρετήριο με το κλειδί του κάθε χρήστη

Για ένα τέτοιο σχήμα πρέπει να είναι **υπολογιστικά ανέφικτο** να προσδιοριστεί το d_k γνωρίζοντας το e_k !!!

Παραδείγματα: RSA, ElGamal, Elliptic Curves Cryptosystems, Merkle-Hellman Knapsack, McEliece, …

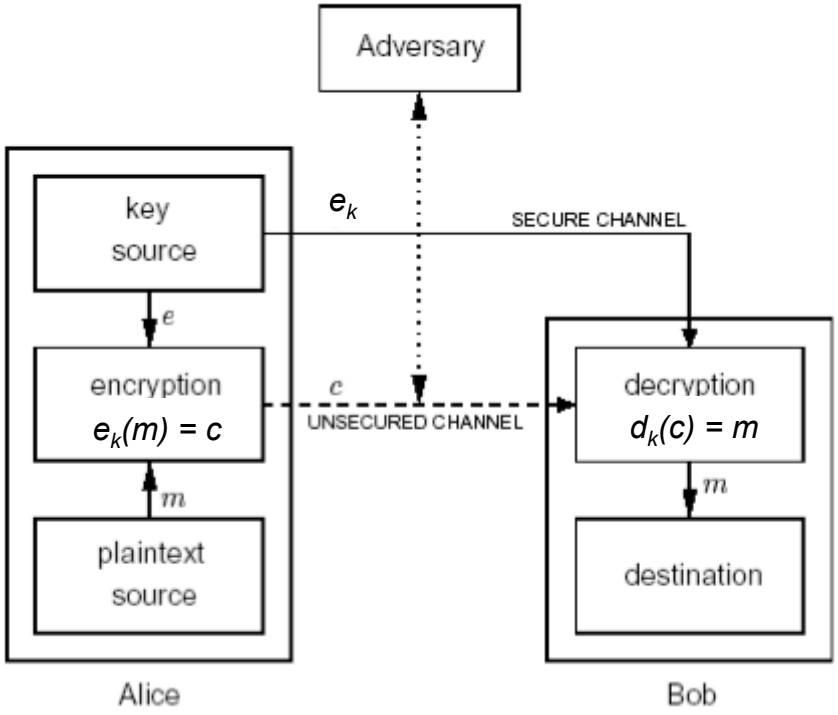
Κρυπτογραφία και εμπιστευτικότητα

- ✓ Οντότητες επικοινωνίας
  - Κάποιος ή κάτι το οποίο στέλνει, λαμβάνει ή επεξεργάζεται πληροφορίες.
    - Πρόσωπο, υπολογιστής, πρόγραμμα, κοκ
  - two-party communication
    - Alice: Αποστολέας (Sender): γνήσιος (νόμιμος) μεταδότης της πληροφορίας
    - Bob: Παραλήπτης (Receiver): ο επιδιωκόμενος παραλήπτης
    - Oscar: Αντίπαλος (Adversary): προσπαθεί να ακυρώσει την ασφάλεια που παρέχεται μεταξύ αποστολέα και παραλήπτη.
      - Εχθρός, υποκλοπέας, ωτακουστής, παρείσακτος, αντίπαλος, …

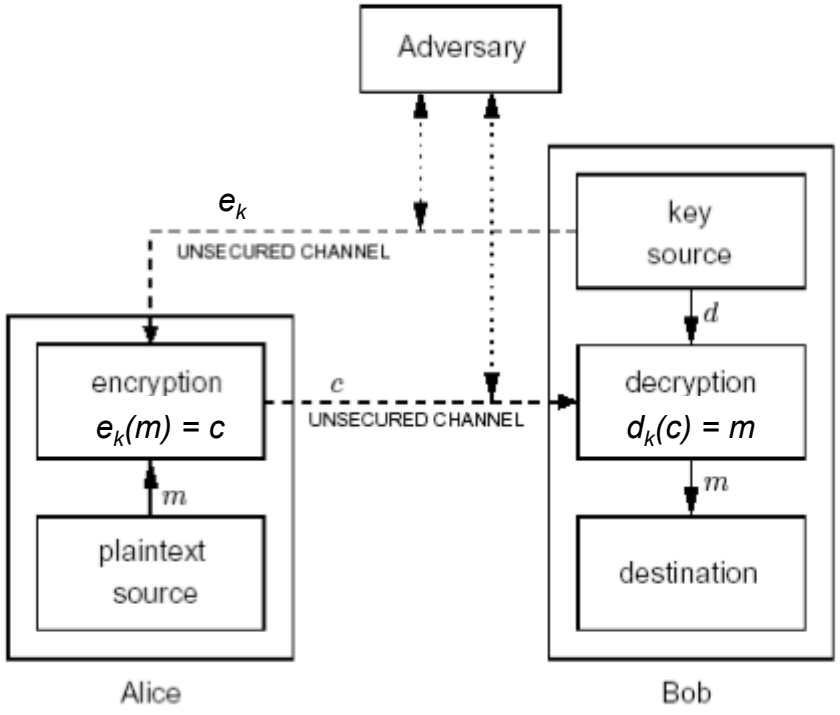
Κρυπτογραφία και εμπιστευτικότητα

- ✓ Κανάλι επικοινωνίας
  - Μεταφέρει πληροφορία ή δεδομένα μεταξύ οντοτήτων
  - Φυσικά ασφαλές ή ασφαλές κανάλι:
    - Αυτό που δεν είναι προσβάσιμο από adversary
  - Ανασφαλές κανάλι
    - Αυτό στο οποίο τρίτες οντότητες, εκτός από αυτές που αφορά ή προορίζεται η πληροφορία, μπορούν να την διαβάσουν, τροποποιήσουν, αλλοιώσουν, αναπαράγουν, διαγράψουν, ή να εισαγάγουν άλλη
  - Κρυπτογραφικά ασφαλές κανάλι
    - Μπορεί να είναι προσβάσιμο από adversary
    - Αλλά δεν μπορεί να ακυρώσει τις υπηρεσίες ασφάλειας

Συμμετρική και κρυπτογραφία δημοσίου κλειδιού



Συμμετρική κρυπτογραφία



Κρυπτογραφία δημοσίου κλειδιού

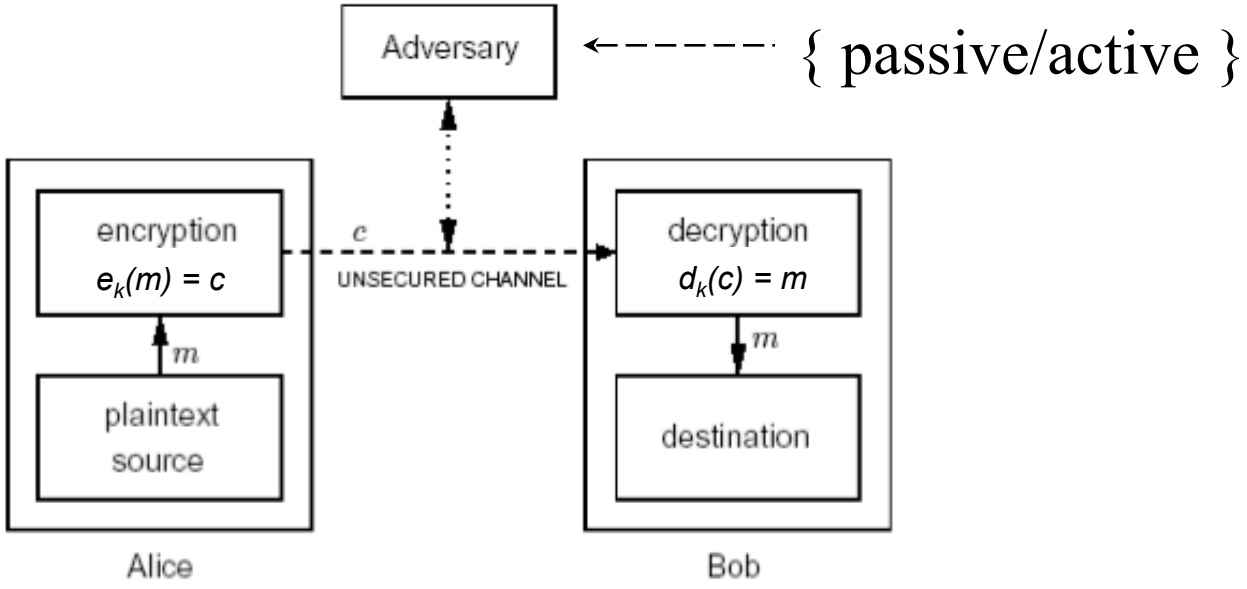
Είναι απαραίτητα τα κλειδιά; Ναι

- Η Alice και ο Bob δεν επιλέγουν κάθε φορά διαφορετικές συναρτήσεις κρυπτογράφησης (απλά αλλάζουν το κλειδί)
  - Γιατί;
- Αν σε ένα encryption scheme έχουμε όμοιους μετασχηματισμούς αλλά χαρακτηρίζονται μοναδικά από κλειδιά τότε αν το σχήμα αποκαλυφθεί δεν χρειάζεται ανασχεδιασμός, αλλά απλά αλλαγή κλειδιού
- Κοινή κρυπτογραφική τεχνική να αλλάζει συχνά το κλειδί !
- Kerckhoff's desiderata, 1883
  - Οι αλγόριθμοι πρέπει να είναι δημόσιοι
  - Τα κλειδιά πρέπει να είναι μυστικά
- Ευθέως ανάλογο με χρηματοκιβώτιο
  - Μηχανισμός γνωστός στον αγοραστή
  - Κωδικός αλλάζει συχνά

Κατηγορίες Επιθέσεων

Passive attack: Ο εχθρός (adversary) κρυφακούει – υποκλέπτει το κανάλι επικοινωνίας. Επίθεση στην εμπιστευτικότητα των δεδομένων.

Active attack: Ο εχθρός (adversary) στοχεύει να διαγράψει ή να τροποποιήσει τα υπό μετάδοση δεδομένα. Επίθεση στην ακεραιότητα, εμπιστευτικότητα και αυθεντικότητα δεδομένων, καθώς και στην αυθεντικοποίηση οντοτήτων.



Κατηγορίες Επιθέσεων

- ***Ciphertext-only attack:***

  Ο εχθρός προσπαθεί να συμπεράνει το decryption key, ή το plaintext με το να παρατηρεί (υποκλέπτει) το ciphertext.

  - Ένα σχήμα ευπαθές σε τέτοια επίθεση είναι ***τελείως ανασφαλές.***
  - Χρήση στατιστικών (English, Greek text, HTML file, …)

- ***Known plaintext attack:***

  Ο εχθρός έχει στη διάθεσή του κάποιο plaintext (ή ένα τμήμα του) και το αντίστοιχο ciphertext

  - Γνώση για μέρος του plaintext πάντα βοηθά (π.χ. postscript files' headers)

Κατηγορίες Επιθέσεων

Αν ο εχθρός αποκτά πρόσβαση στο κρυπτοσύστημα:

- ***Chosen plaintext attack***
  - Εισάγει plaintexts στο σύστημα κρυπτογράφησης και παρατηρεί τα αντίστοιχα ciphertexts.
- ***Adaptive Chosen plaintext attack***
  - Το plaintext που εισάγεται σχετίζεται με το ciphertext που λήφθηκε σε προηγούμενα πειράματα
- ***Chosen ciphertext attack***
  - Εισάγει ciphertexts στο σύστημα από-κρυπτογράφησης και παρατηρεί τα αντίστοιχα plaintexts.
- ***Adaptive Chosen ciphertext attack***
  - Το ciphertext που εισάγεται σχετίζεται με το plaintext που λήφθηκε σε προηγούμενα πειράματα