Οικονομικό Πανεπιστήμιο Αθηνών
Τμήμα Πληροφορικής
ΠΜΣ στα Πληροφοριακά Συστήματα

Κρυπτογραφία και Εφαρμογές
Διαλέξεις Ακ. Έτους 2013-2014

Μαριάς Ιωάννης
marias@aueb.gr

Μαρκάκης Ευάγγελος
markakis@gmail.com

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 Cipher

Περιεχόμενα Μαθήματος – Θεματικές Ενότητες

- Θ.Ε.4: Συμμετρική κρυπτογραφία τμημάτων
  - ✓ Shannon's principles
  - ✓ Permutation Networks
  - ✓ DES/3DES
  - ✓ AES
- Θ.Ε.5: Αλγόριθμοι για primality testing και factoring
  - ✓ Πιθανοτικοί Αλγόριθμοι (Miller-Rabin, Solovay-Strassen)
  - ✓ Ντετερμινιστικοί αλγόριθμοι (Agrawal - Kayal - Saxena)
  - ✓ Pollard's rho heuristic
- Θ.Ε.6: Κρυπτογραφία Δημοσίου Κλειδιού (Public Key Cryptosystems)
  - ✓ RSA
  - ✓ El Gamal
  - ✓ Elliptic Curves

Περιεχόμενα Μαθήματος – Θεματικές Ενότητες

- Θ.Ε.7: Ψηφιακές Υπογραφές
  - ✓ ElGamal Signature Scheme
  - ✓ Digital Signature Standard - πρότυπο ψηφιακών υπογραφών ISO/IEC 9796–2
  - ✓ One-time, Undeniable, Fail-stop Signatures
- Θ.Ε.8: Hash Functions
  - ✓ Collision Resistant Hash Functions
  - ✓ Secure Hash Algorithm (SHA)
  - ✓ H-MAC
  - ✓ The Birthday Attack
- Θ.Ε.9: Διανομή και εγκαθίδρυση κλειδιών
  - ✓ Blom’s Scheme
  - ✓ Diffie-Hellman

Περιεχόμενα Μαθήματος – Θεματικές Ενότητες

- Θ.Ε.10: Ειδικά Θέματα (if time permits)
  - ✓ Διαμοιρασμός μυστικών (secret sharing) και τεμαχισμός κλειδιών, Shamir (*m*,*n*) threshold schemes
  - ✓ Πρωτόκολλα δέσμευσης bit (bit commitment protocols)
  - ✓ Πρωτόκολλα αυθεντικοποίησης μηδενικής γνώσης (Fiat-Shamir, Guillou-Quisquarter, και Schnorr)

- Συνολικά 10 θεματικές ενότητες για 12-13 διαλέξεις

Διαφάνειες

- 1-2 μέρες πριν από κάθε διάλεξη στο eclass
  - ✓ http://eclass.aueb.gr/
  - ✓ Γραφτείτε στο «Κρυπτογραφία και Εφαρμογές 2013-2014»
- Οι τελικές διαφάνειες θα μπαίνουν μετά το μάθημα και μετά από διορθώσεις – παρατηρήσεις

Διαδικαστικά

- Ώρες γραφείου
  - ✓ Δεριγνύ 12, 6ος όροφος
  - ✓ Τρίτη 13:00 – 14:00 και Πέμπτη 13:00 – 15:00
  - ✓ Καθώς και συναντήσεις μετά από αίτημά σας (by email)
- Βαθμολόγηση
  - ✓ Τελικό διαγώνισμα: 9
  - ✓ 2 σειρές ασκήσεων: 2 μονάδες σύνολο
    - 1η σειρά: υλοποίηση και κρυπτανάλυση κάποιου βασικού κρυπτοσυστήματος
    - 2η σειρά: ασκήσεις/ερωτήσεις πάνω σε θεωρία αριθμών, συμμετρική κρυπτογραφία, κρυπτογραφία δημοσίου κλειδιού

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
  - ✓ 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 (the part on algorithms for number theory)

Σταθμοί στην ιστορία της Κρυπτογραφίας

Αρχ.Ελλάδα Μέθοδος Σκυτάλης

15ος-16ος αιών. **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

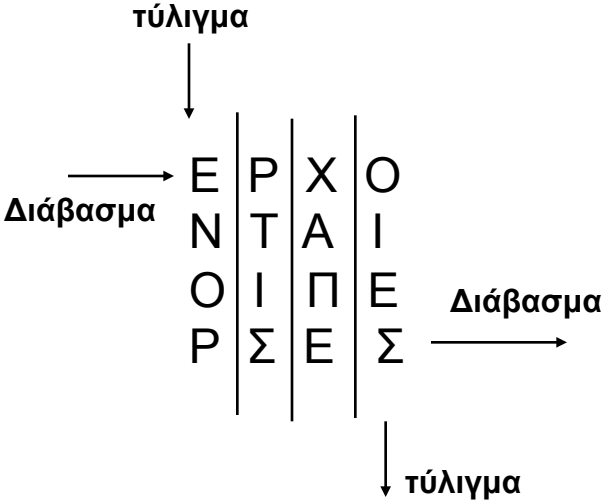
2001 Advanced Encryption Standard (**AES**) adopted as US Standard

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

Σταθμοί

Αρχαία Ελλάδα – Σκυτάλη

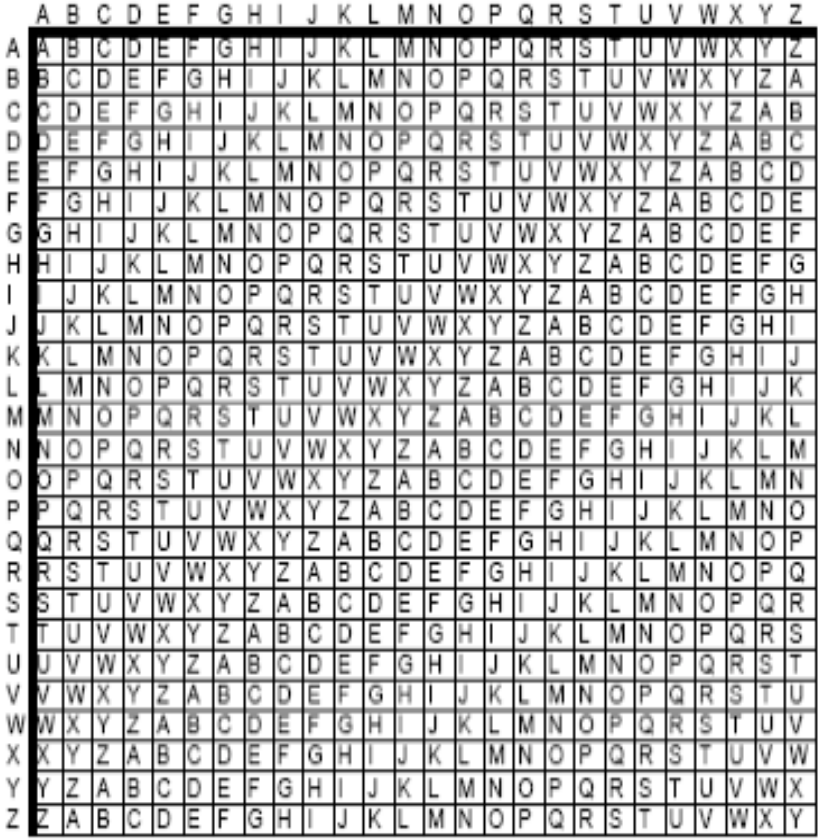
Εικόνα από wikipedia



- 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. Διαβάζει την μια πλευρά μετά την άλλη και 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

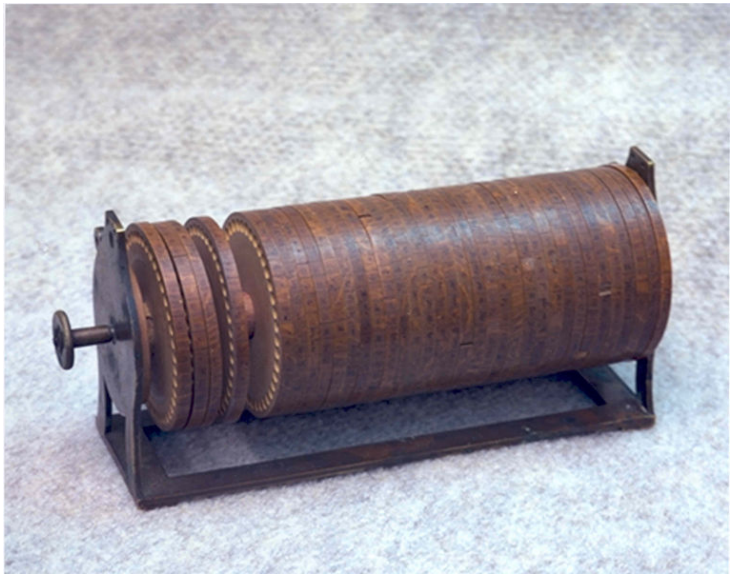
tabula recta, Johannes Trithemius

Η ιστορία είναι άδικη απέναντι στον G. B. Bellaso που 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



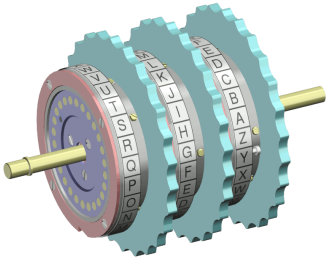
Εικόνα από wikipedia

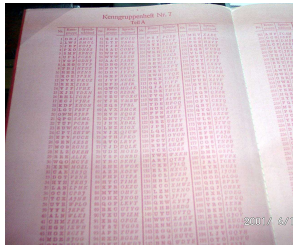
- Περιστρεφόμενοι κύλινδροι
- Κάθε ένας: 26 γράμματα (τυχαία τοποθετημένα)
- Κύλινδροι στοιβαγμένοι με την ίδια σειρά σε αποστολέα και παραλήπτη
  - Μυστικό **(ή κλειδί)** : η διάταξη της στοίβας
- Για να κρυπτογραφηθεί ένα ΜΗΝΥΜΑ ο αποστολέας περιστρέφει τους κυλίνδρους μέχρι να σχηματιστεί η λέξη σε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





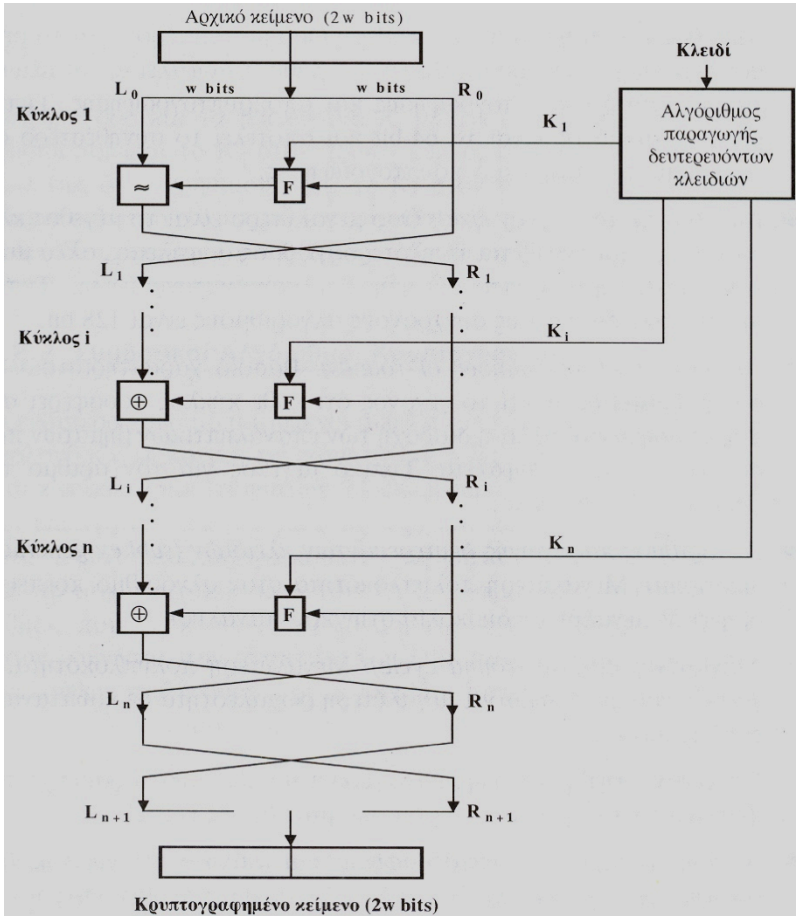
Το βιβλίο κωδικών (wikipedia)

- 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*"

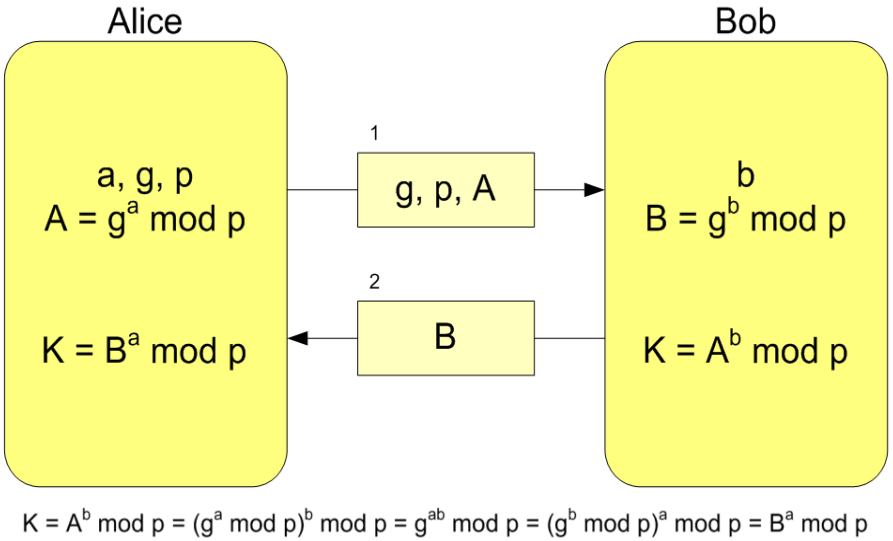
  Feistel, H. 1973. Cryptography and Computer Privacy. Scientific American
  - Ανεπαίσθητη αλλαγή στο input: Παράγει πολλαπλές αλλαγές στον 1ο κύκλο, περισσότερες στο 2ο, κοκ
  - Τελικά το μισό block αλλάζει κατά μέσο όρο
- Blowfish, CAST-128, DES, FEAL, Lucifer, MARS, RC5, Triple DES, Twofish, GOST

Σταθμοί

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

Κρυπτογραφία Δημοσίου Κλειδιού

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



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

- 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

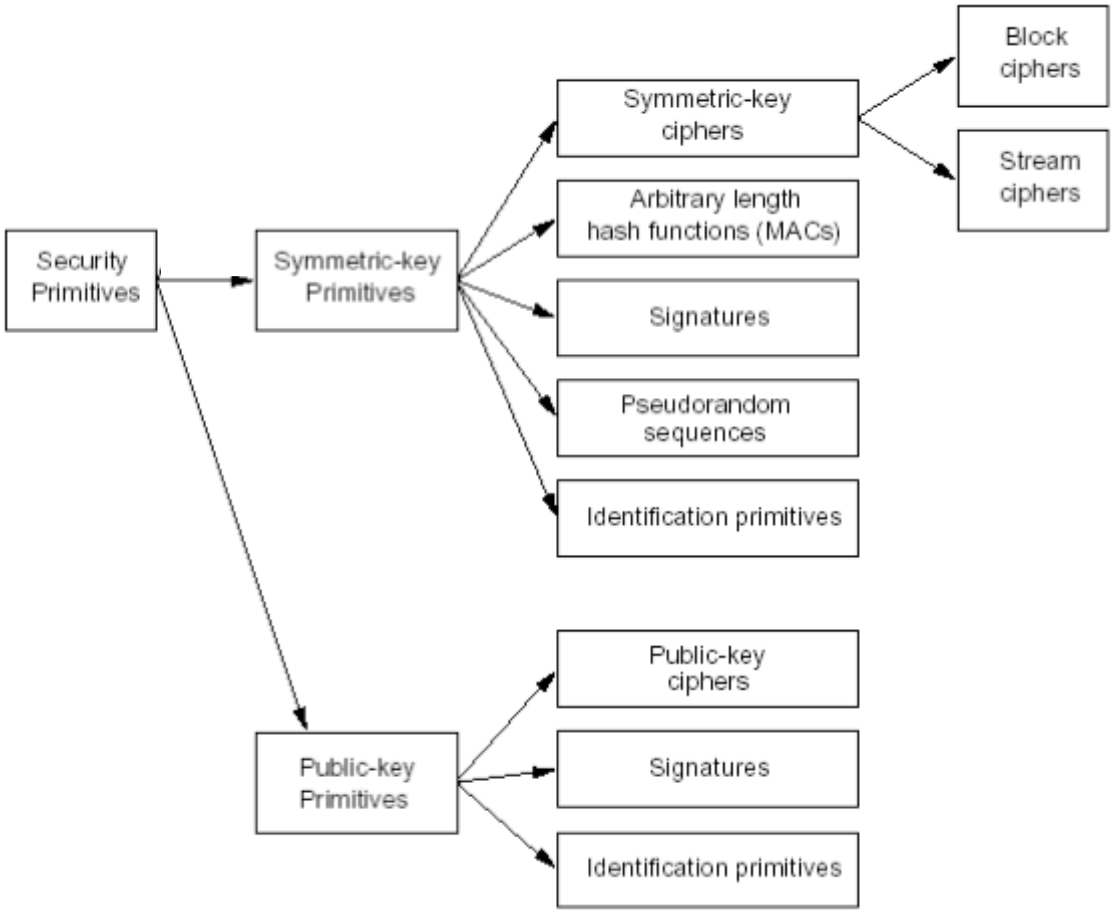
Η Κρυπογραφία ασχολείται με: τη μελέτη μαθηματικών τεχνικών που σχετίζονται με θέματα ασφάλειας πληροφοριών

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 (**non-repudiation**) ενεργειών
- ✓ 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

Ταξινόμηση Κρυπτογραφικών Τεχνικών



Κρυπτοσυστήματα και Κρυπτολογία

- ✓ Κρυπτοσύστημα (cryptosystem)
  - Ένα σύνολο από κρυπτογραφικές τεχνικές που χρησιμοποιείται για να παρέχει υπηρεσίες ασφάλειας
  - Αναφέρεται κυρίως για confidentiality, δηλαδή encryption
- ✓ 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

Ένα κρυπτοσύστημα καθορίζεται από μία πλειάδα (*A*, *P*, *C*, *K*, *E*, *D*), όπου:

A: Αλφάβητο ορισμού (alphabet of definition)

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 στο K καλείται κλειδί (*key)*

Κρυπτοσυστήματα

Ένα κρυπτοσύστημα καθορίζεται από μία πλειάδα (A, P, C, K, E, D), όπου:

E: Συναρτήσεις κρυπτογράφησης (encryption functions)

Για κάθε κλειδί $k \in K$ υπάρχει μία συνάρτηση κρυπτογράφησης $e_k \in E$ από το P στο C

D: Συναρτήσεις αποκρυπτογράφησης (decryption functions)

Για κάθε κλειδί $k \in K$ και συνάρτηση $e_k \in E$ υπάρχει μία αντίστοιχη συνάρτηση αποκρυπτογράφησης $d_k \in D$ από το C στο P, έτσι ώστε $d_k(e_k(x)) = x$ για κάθε $x \in P$

Το ζεύγος (E, D) αναφέρεται ως encryption scheme ή cipher

Για κάθε κλειδί $k \in K$, οι συναρτήσεις e_k και d_k αναφέρονται και ως ***key pair***

Κρυπτοσυστήματα

Η διαδικασία εφαρμογής του μετασχηματισμού e_k σε ένα μήνυμα $m \in P$ αναφέρεται ως κρυπτογράφηση του m

Η διαδικασία εφαρμογής του μετασχηματισμού d_k στο κρυπτογράφημα $c \in C$ αναφέρεται ως αποκρυπτογράφηση του c

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 μπορούμε να ξέρουμε αν το αρχικό μήνυμα ήταν x_1 ή x_2

Συμμετρική κρυπτογραφία και κρυπτογραφία δημοσίου κλειδιού

Έστω ένα σχήμα κρυπτογραφίας που αποτελείται από τα σύνολα $\{E: e_K, k \in K\}$ και $\{D : d_k, k \in K\}$, όπου K ο χώρος κλειδιών

Το σχήμα αναφέρεται ως **symmetric-key encryption scheme** αν για κάθε ζεύγος κλειδιών (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*, *συμβατική*, *single-key*, *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 τα σύνολα $\{E: e_K, k \in K\}$ και $\{D : d_k, k \in K\}$, 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

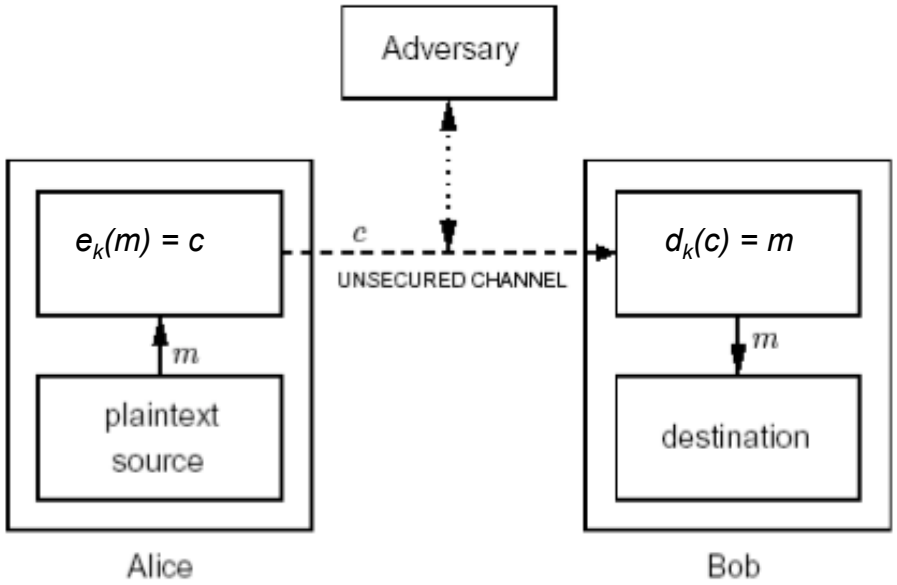
- ✓ Οντότητες επικοινωνίας
  - Κάποιος ή κάτι το οποίο στέλνει, λαμβάνει ή επεξεργάζεται πληροφορίες.
    - Πρόσωπο, υπολογιστής, πρόγραμμα, κοκ
  - two-party communication
    - Alice: Αποστολέας (Sender): γνήσιος (νόμιμος) μεταδότης της πληροφορίας
    - Bob: Παραλήπτης (Receiver): ο επιδιωκόμενος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

Κρυπτογραφία και εμπιστευτικότητα

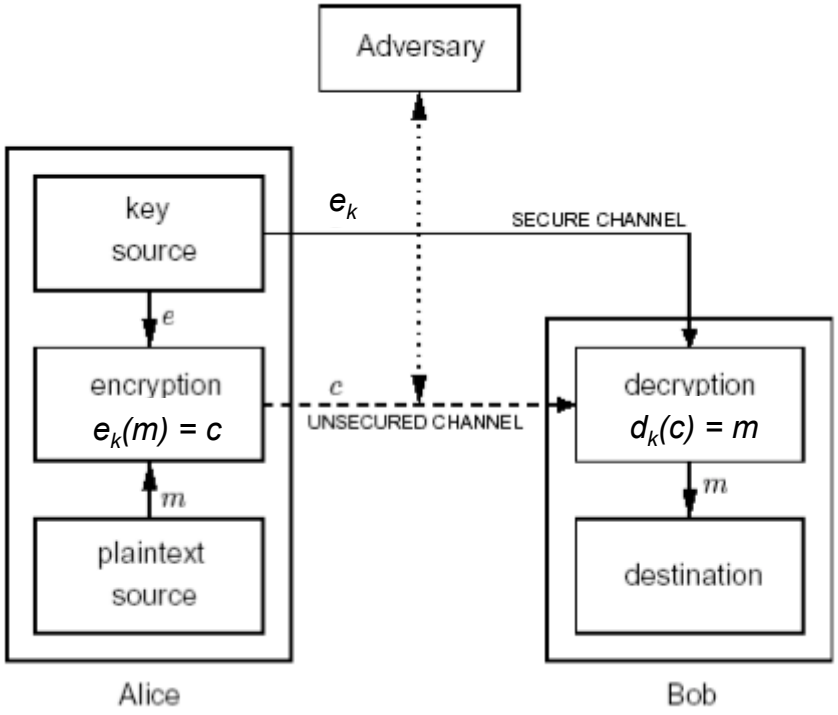
- ✓ Κανάλι επικοινωνίας
  - Μεταφέρει πληροφορία ή δεδομένα μεταξύ οντοτήτων
  - Φυσικά ασφαλές ή ασφαλές κανάλι:
    - Αυτό που δεν είναι προσβάσιμο από adversary
  - Ανασφαλές κανάλι
    - Αυτό στο οποίο τρίτες οντότητες, εκτός από αυτές που αφορά ή προορίζεται η πληροφορία, μπορούν να την διαβάσουν, 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

Κρυπτογραφία και εμπιστευτικότητα

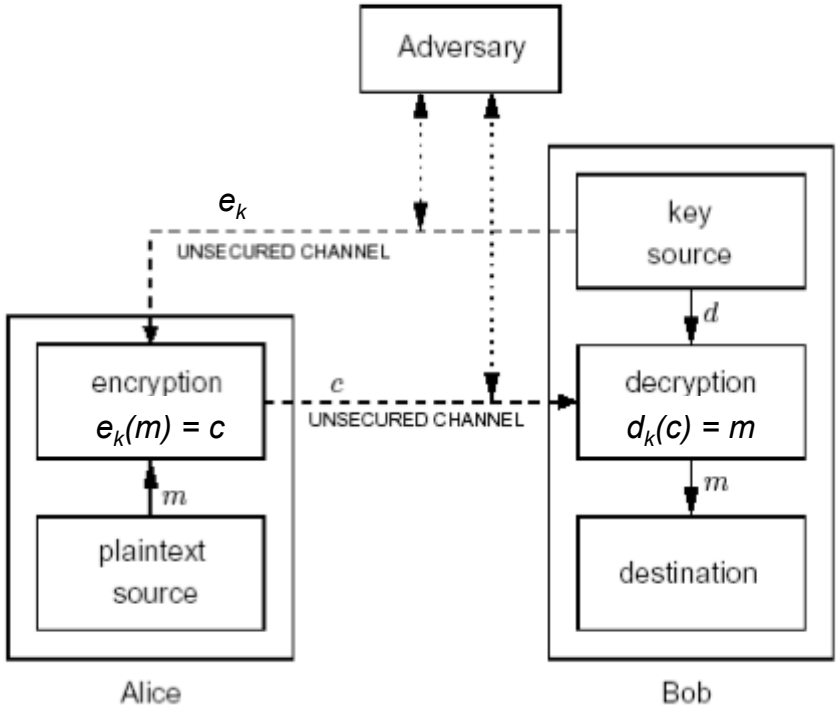
- Η Alice και ο Bob θέλουν να επικοινωνήσουν με μυστικότητα
- Πρώτα ανταλλάσσουν μυστικά το ζεύγος κλειδιών (e_k, d_k) (στη συμμετρική κρυπτογραφία) ή η Alice βλέπει το δημοσιευμένο e_k (στην κρυπτογραφία δημοσίου κλειδιού).
- Η Alice θέλει να στείλει ένα μήνυμα $m \in P$ στον Bob
- Υπολογίζει $c = e_k(m)$ και στέλνει το c στον Bob.
- Όταν ο Bob λάβει το c, υπολογίζει $d_k(c) = m$, και ανακτά το αρχικό κείμενο m



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 !
- Kerckhoffs' 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

Ασφάλεια και κρυπτολογία

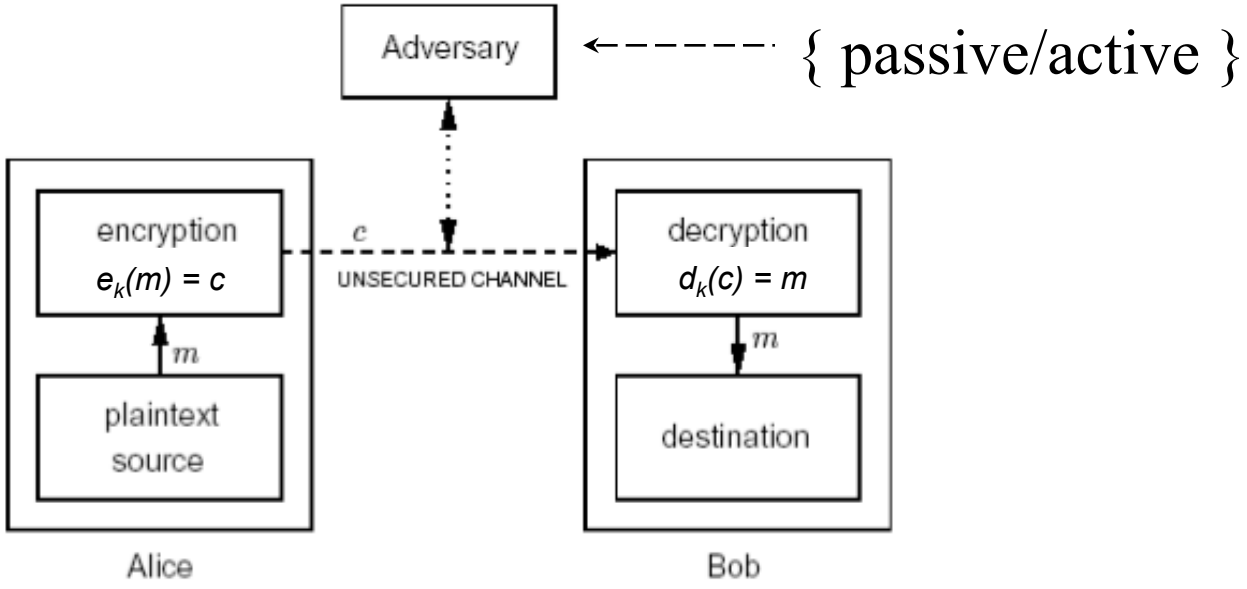
- ✓ Θεμελιώδης απαίτηση στην κρυπτογραφία:
  - τα σύνολα C, K, E, D, να είναι δημόσια
  - όταν δύο οντότητες επικοινωνούν με ασφάλεια πρέπει να διατηρούν μυστικό
    - το ζεύγος (e, d) – συμμετρική
    - το d – ασύμμετρη
- ✓ Ένα encryption scheme είναι εύθραυστο (breakable) αν
  - τρίτο μέρος χωρίς πρότερη γνώση για το κλειδί μπορεί συστηματικά να ανακτά plaintexts από αντίστοιχα ciphertexts
  - σε εύλογο χρονικό διάστημα!!!

- ✓ Κάθε σχήμα μπορεί να σπάσει με χρήση όλων των πιθανών κλειδιών
  - ✓ Υπό υπόθεση ότι το σχήμα είναι δημόσια γνωστό
  - ✓ brute force search του χώρου κλειδιών
  - ✓ Συμπέρασμα: Ο αριθμός των πιθανών κλειδιών (key space size) πρέπει να είναι **πολύ** μεγάλος

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

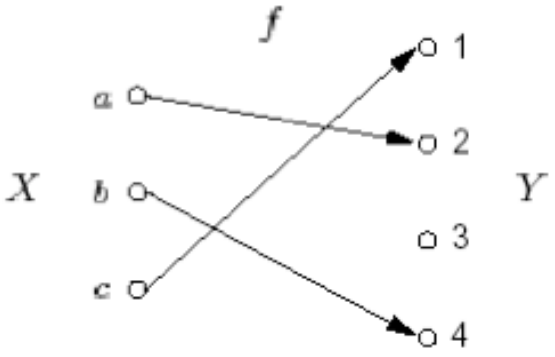
  - Γνώση για μέρος του plaintext πάντα βοηθά (π.χ. postscript files' headers)

Κατηγορίες Επιθέσεων

Αν ο εχθρός ανακτά 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

Συναρτήσεις



Έστω σύνολα X={a, b, c} και Y={1,2,3,4},

και συνάρτηση f από το X στο Y που ορίζεται ως:

f(a)=2, f(b)=4, f(c)=1

X: πεδίο ορισμού (domain)

Y: πεδίο τιμών (range)

Η εικόνα της f (***Im(f)***) είναι το {1,2,4} υποσύνολο του Y

Παράδειγμα.

Έστω X={1,2,3,...,10} και φ ο μετασχηματισμός:

∀ x∈X, φ(x)= x^2 mod 11 (= υπόλοιπο που προκύπτει από τη διαίρεση του x^2 με το 11)

Τότε:

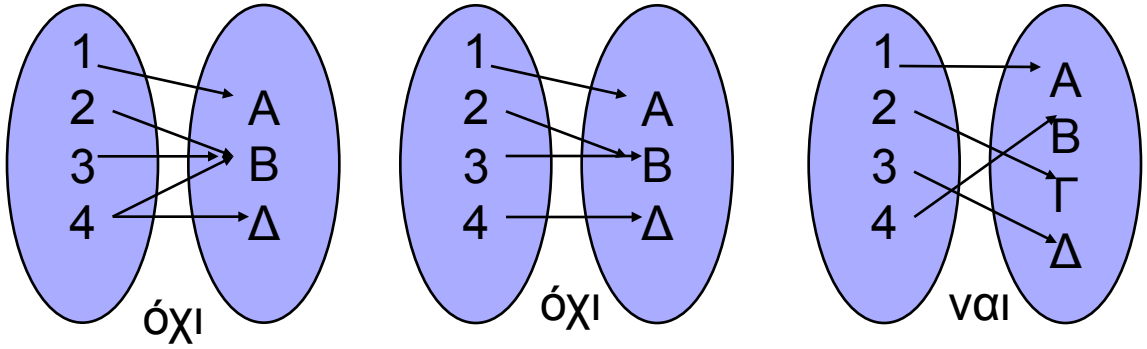
φ(1)=1, φ(2)=4, φ(3)=9, φ(4)=5, φ(5)=3,
φ(6)=3, φ(7)=5, φ(8)=9, φ(9)=4, φ(10)=1

Άρα **Im(φ)**={1,3,4,5,9}

Συναρτήσεις

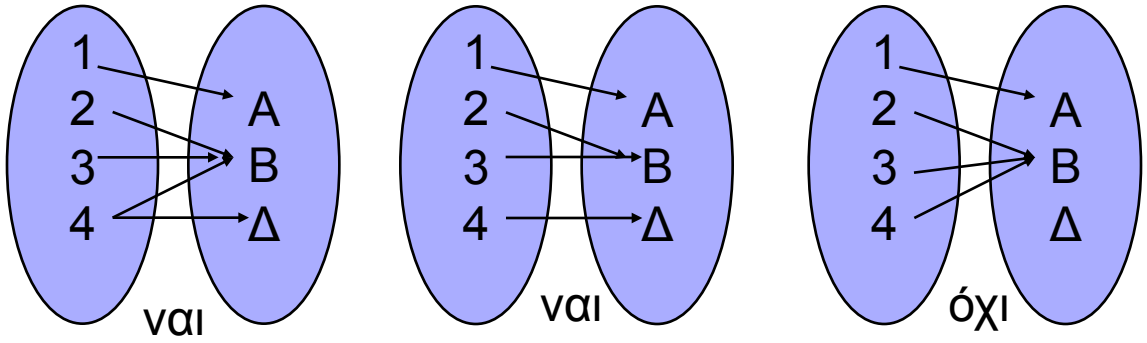
- Injection (1-1):
  - ✓ Μία συνάρτηση είναι injective (ή one-to-one) αν για κάθε x_1, x_2 του X, με $x_1 \neq x_2$ έχουμε $f(x_1) \neq f(x_2)$
  - ✓ Κάθε στοιχείο του X απεικονίζεται σε διαφορετικό στοιχείο του Y

  - Η f : R → R : f(x) = 2x + 1 είναι injective
  - Η g : R → R : g(x) = x^2 δεν είναι injective
  - Η g : R^+ → R : g(x) = x^2 είναι injective



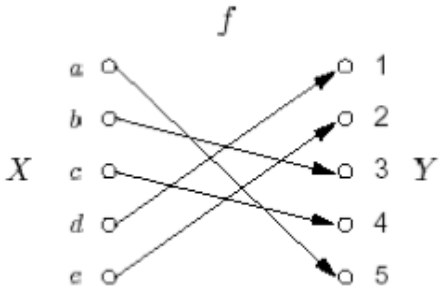
Συναρτήσεις

- Surjection (επί):
  - ✓ Μία συνάρτηση είναι surjective (επί) αν κάθε στοιχείο του Y είναι η εικόνα ενός στοιχείου του X.
  - ✓ συσχετίζει τουλάχιστον μια τιμή του πεδίου X σε κάθε τιμή του πεδίου Y
    - H f : R → R : f(x) = 2x + 1 είναι surjective
    - H g : R → R : g(x) = x^2 δεν είναι surjective
      - δεν υπάρχει πραγματικός x τέτοιος ώστε $x^2 = -1$.
    - H g : R → R^+ : g(x) = x^2 είναι surjective



Συναρτήσεις

- Bijection (1-1 και επί):
  - ✓ Μία συνάρτηση είναι bijective αν είναι injective και surjective (κάθε στοιχείο του Y είναι η εικόνα ενός ακριβώς στοιχείου του X).
    - H f : R → R : f(x) = 2x + 1 είναι bijective
    - H g : R → R : g(x) = x^2 δεν είναι bijective (g(1)=g(-1)=1)
    - H g : R^+ → R^+ : g(x) = x^2 είναι bijective



H f είναι bijective

Συναρτήσεις

- Αν μία συνάρτηση είναι bijective
- και το πεδίο ορισμού είναι ίδιο με το πεδίο τιμών,
- και είναι και πεπερασμένο, τότε λέγεται **αντιμετάθεση (permutation)**
- Π.χ. έστω S= {1, 2, 3, 4, 5}
- Έστω η permutation p: S → S που ορίζεται ως
  - p(1) = 3 p(2) = 5 p(3) = 4 p(4) = 2 p(5) = 1
- Αναπαράσταση:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$$

← Πεδίο ορισμού

← Εικόνα

- Θα μας χρειαστούν για το DES/AES

Παράδειγμα Συμμετρικής Κρυπτογραφίας

Έστω $P=\{m_1,m_2,m_3\}$ και $C=\{c_1,c_2,c_3\}$. Υπάρχουν $3!=6$ bijections από το P στο C

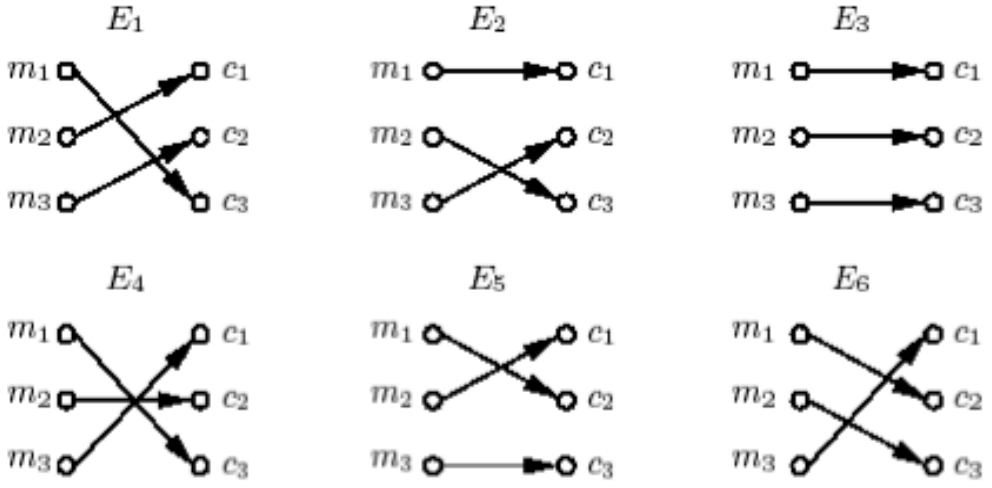
key space $K = \{1,2,3,4,5,6\}$, έξι στοιχεία, καθένα προσδιορίζει ένα bijection

Έξι δυνατές συναρτήσεις κρυπτογράφησης που δηλώνονται ως $e_i, i=1,\ldots,6$.

Έστω ότι η Alice και ο Bob συμφωνούν κρυφά για το μετασχηματισμό e_1

Για να κρυπτογραφήσει το μήνυμα m_1, η Alice υπολογίζει $e_1(m_1)=c_3$ και στέλνει c_3 στον Bob.

Ο Bob αποκρυπτογραφεί το c_3 με το να αντιστρέψει τα βέλη στο διάγραμμα του μετασχηματισμού e_1. Παρατηρεί ότι το c_3 δείχνει το m_1.



Συναρτήσεις

- Μονόδρομες Συναρτήσεις
  - ✓ One-way function
    - συνάρτηση f τέτοια ώστε για κάθε x στο πεδίο ορισμού της f, η f(x) είναι εύκολο να υπολογιστεί
    - δεδομένου ενός y στο πεδίο τιμών της f είναι υπολογιστικά ανέφικτο να προσδιοριστεί x τέτοιο ώστε y=f(x)
      - Integer factorization
      - Discrete logarithms
  - ✓ Trapdoor One-way function
    - one-way function της οποίας η αντίστροφη είναι υπολογιστικά εύκολο να προσδιοριστεί αν συγκεκριμένα χαρακτηριστικά της είναι γνωστά
  - ✓ Η κρυπτογραφία δημοσίου κλειδιού βασίζεται σε συναρτήσεις που πιστεύουμε ότι είναι trapdoor one way functions

Συναρτήσεις

- Παράδειγμα
  - Έστω πρώτοι αριθμοί p=48611 και q=53993
  - n=p*q=2624653723
  - Έστω X={1,2,..., n-1}
  - Έστω η συνάρτηση $\varphi(x) = x^3 \bmod n$
  - Ο υπολογισμός του φ(x) είναι εφικτός
    - φ(2489991)=1981394214
  - Ωστόσο η αντιστροφή είναι πολύπλοκη
    - Δηλαδή, δεδομένου του υπολοίπου να βρεθεί η τιμή του x που υψώθηκε στη δύναμη του 3
  - Αν οι παράγοντες p και q είναι άγνωστοι και μεγάλοι πρόκειται για ένα δύσκολο πρόβλημα
    - Αν ένας από τους δύο γίνει γνωστός, τότε τα πράγματα ... διευκολύνονται