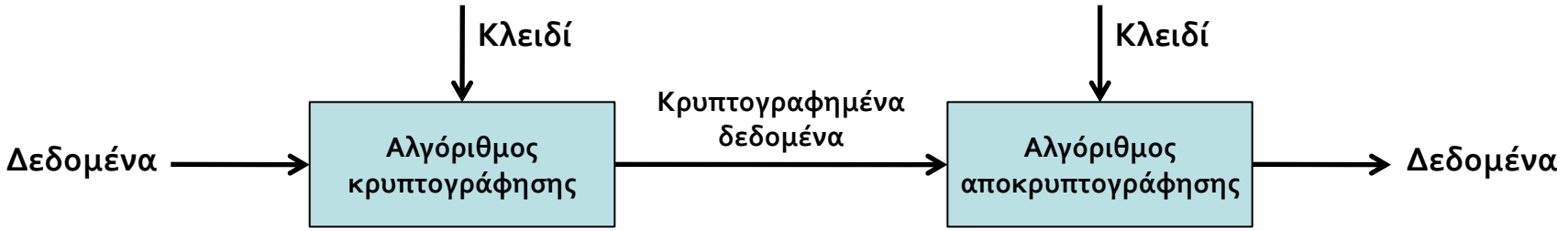
Πανεπιστήμιο Πελοποννήσου
Τμήμα Επιστήμης και Τεχνολογίας Τηλεπικοινωνιών

Διαχείριση και Ασφάλεια Δικτύων

Κρυπτογραφία

Κρυπτογραφία

- *Κρυπτόν + Γράφειν*
- Η εφαρμογή μαθηματικών (κυρίως) μηχανισμών προκειμένου να "αλλοιωθούν" κάποια δεδομένα, παραμένοντας όμως ανακτήσιμα
- Στόχος: η αποτροπή ή/και ανίχνευση κακόβουλων πράξεων που σχετίζονται με τα δεδομένα
  - Εμπιστευτικότητα πληροφοριών
  - Εξασφάλιση ακεραιότητας
  - Πιστοποίηση αυθεντικότητας δεδομένων και των πηγών τους
  - … … …



Βασικές έννοιες

- Αρχικό απλό κείμενο (plaintext)
- Κρυπτογραφημένο μήνυμα ή κρυπτογράφημα (ciphertext)
- Κρυπτογράφηση (encryption, enciphering)
- Αποκρυπτογράφηση (decryprion, deciphering)
- Αλγόριθμος κρυπτογράφησης (encryption algorithm)
- Αλγόριθμος αποκρυπτογράφησης (decryption algorithm)
- Κλειδί (key)
- Κρυπτογραφία (cryptography)
- Κρυπτανάλυση (cryptanalysis)
- Κρυπτολογία (cryptology)

Εφαρμογές κρυπτογραφίας

- Εμπιστευτικότητα ή ιδιωτικότητα δεδομένων (confidentiality)
- Ακεραιότητα δεδομένων (data integrity)
- Αυθεντικοποίηση οντοτήτων (authentication)
- Αυθεντικότητα προέλευσης δεδομένων (data origin authentication)
- Ψηφιακή υπογραφή (digital signature)
- Μη-αποποίηση (non-repudiation)
- Εξουσιοδότηση (authorization)
- Έλεγχος πρόσβασης (access control)
- Πιστοποίηση (certification)
- Χρονοσήμανση (timestamping)
- Ανωνυμία (anonymity)
- Διαχείριση ψηφιακών δικαιωμάτων (digital rights management)
- Ψηφιακή υδατογράφηση (digital watermarking)

Πρώτες μορφές κρυπτογραφίας

- Μέθοδος σκυτάλης στην αρχαία Ελλάδα
- Το μήνυμα γραφόταν σε δερμάτινη λωρίδα η οποία ήταν τυλιγμένη ελικοειδώς σε ξύλινη σκυτάλη
- Ο παραλήπτης έπρεπε να τυλίξει τη λωρίδα σε σκυτάλη ίδιας διαμέτρου προκειμένου να διαβάσει το μήνυμα
- Δηλαδή, διάμετρος σκυτάλης → κρυπτογραφικό κλειδί

Αρχικό μήνυμα: **KILL KING TOMORROW MIDNIGHT**

"Τυλιγμένο" μήνυμα:

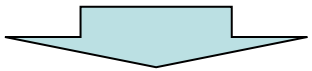
K	I	L	L	K	I	N	G
T	O	M	O	R	R	O	W
M	I	D	N	I	G	H	T

Κρυπτογραφημένο μήνυμα: **KTMIOILMDLONKRIIRGNOHGWT**

Πρώτες μορφές κρυπτογραφίας

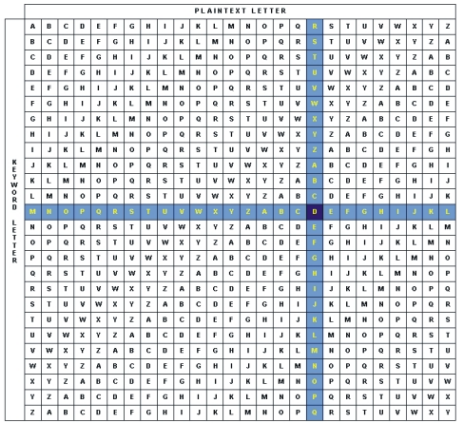
- Αλγόριθμος του Καίσαρα (Caesar cipher)
- Απλή ολίσθηση γραμμάτων κατά *X* θέσεις
- π.χ., εάν *X* = 3:

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



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

- ...εξαιρετικά εύκολη η κρυπτανάλυση!
- Παραλλαγή: Vigenère Cipher
  - Ο κάθε χαρακτήρας ολισθαίνει διαφορετικό αριθμό θέσεων, με βάση κάποιο κλειδί



Κρυπτανάλυση

- Η διαδικασία της προσπάθειας ανακάλυψης των αρχικών δεδομένων ή του κλειδιού κρυπτογράφησης
- Διάφοροι τύποι κρυπταναλυτικών επιθέσεων, ανάλογα με τη γνώση που έχει ο επιτιθέμενος
- Πλέον προφανής: brute-force attack, όπου δοκιμάζονται όλοι οι συνδυασμοί κλειδιών

Μέσος απαιτούμενος χρόνος για εξαντλητική αναζήτηση κλειδιού

Μέγεθος κλειδιού (bits)	**Αριθμός εναλλακτικών κλειδιών**	**Απαιτούμενος χρόνος με 10^6 κρυπτογραφήσεις/μs**
32	$2^{32} = 4.3 \times 10^9$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	10 ώρες
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18}
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} χρόνια

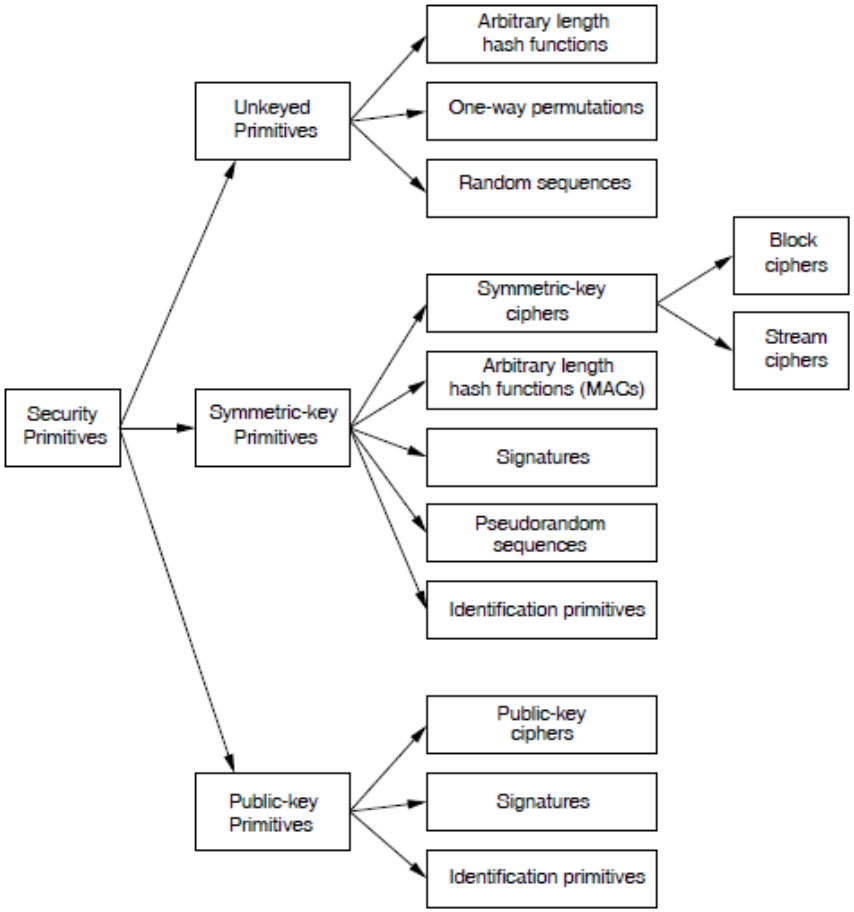
Κρυπταναλυτικές επιθέσεις

Ciphertext only	•Encryption algorithm •Ciphertext to be decoded
Known plaintext	•Encryption algorithm •Ciphertext to be decoded •One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	•Encryption algorithm •Ciphertext to be decoded •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Alan Turing

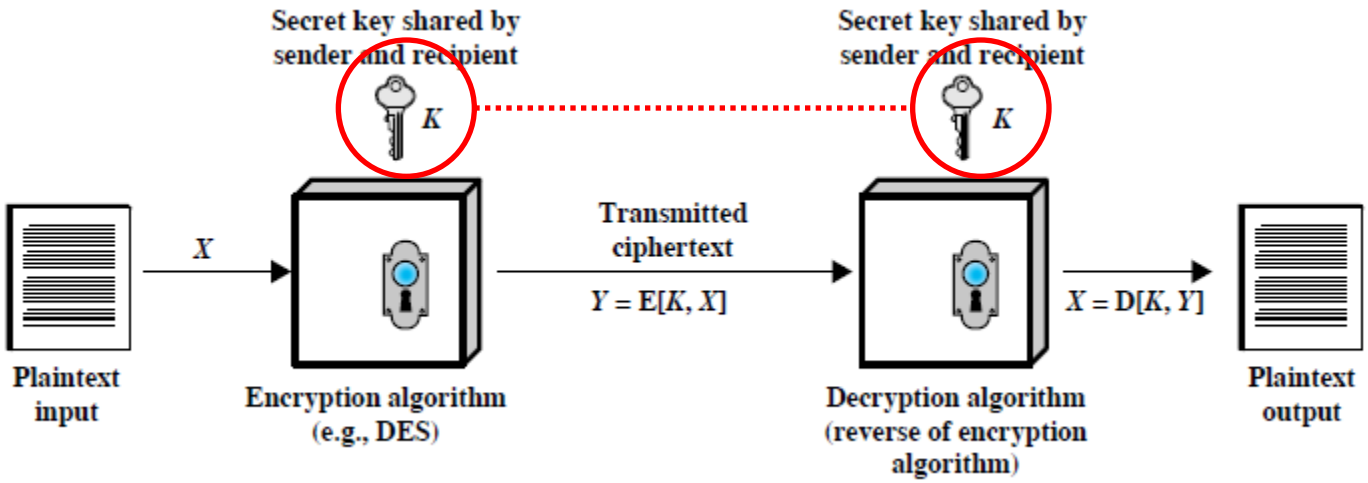
Ταξινόμηση κρυπτογραφικών τεχνικών

- Λειτουργίες
  - Αντικατάσταση
  - Μετάθεση
- Κλειδιά
  - Συμμετρικό κλειδί
  - Δημόσιο κλειδί
- Τρόπος επεξεργασίας
  - Κωδικοποίηση τμημάτων (block cipher)
  - Κωδικοποίηση ροής (stream cipher)



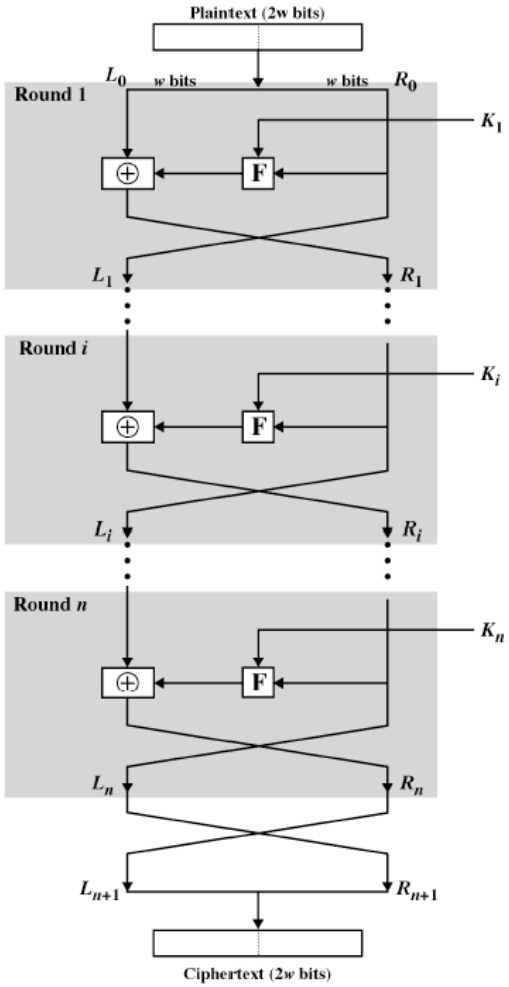
Συμμετρική κρυπτογραφία

- Χρήση του ίδιου κλειδιού για κρυπτογράφηση και αποκρυπτογράφηση
  (...ή αλλιώς, από αποστολέα και παραλήπτη)



Δομή κρυπτογραφίας Feistel

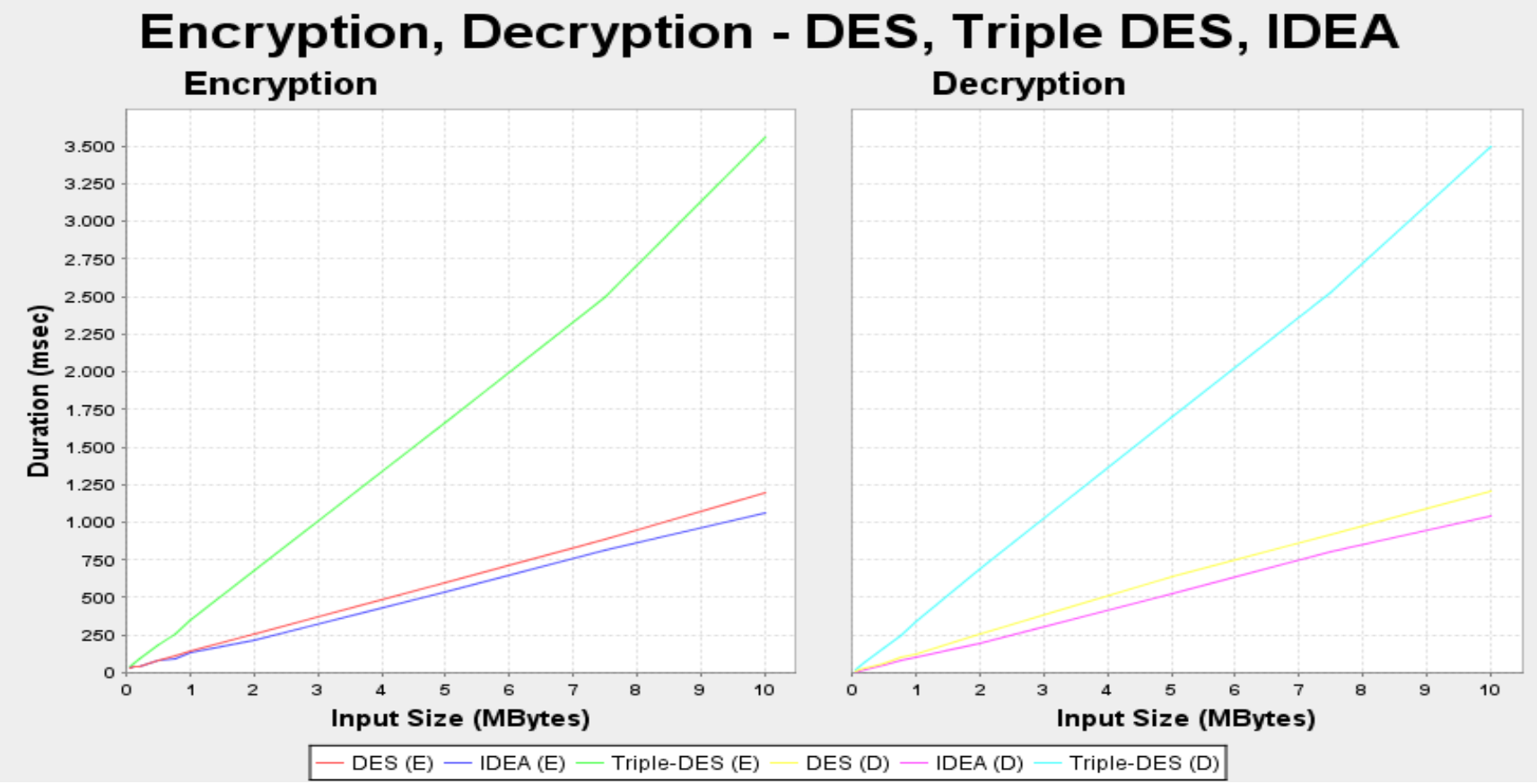
- Αφαιρετική δομή, Horst Feistel, IBM, 1973
- Είσοδος
  - Μήνυμα μήκους *2w* bits (block), χωρισμένο σε L_0 & R_0
  - Κλειδί *K*
- Επεξεργασία
  - *n* γύροι, όπου σε κάθε γύρο i, λαμβάνει χώρα μετασχηματισμός $(L_{i-1}, R_{i-1}) \longrightarrow (L_i, R_i)$, με $L_i = R_{i-1}$ και $R_i = L_{i-1} \oplus \boldsymbol{F}(R_{i-1}, K_i)$
- Έξοδος
  - Κρυπτογραφημένο μήνυμα, μήκους *2w* bits
- Θέματα:
  - Μέγεθος τμημάτων
  - Μέγεθος κλειδιού
  - Αριθμός γύρων
  - Αλγόριθμος παραγωγής υποκλειδιών K_i
  - Συνάρτηση γύρου $\boldsymbol{F}$
  - Ταχύτητα
  - Ευκολία ανάλυσης



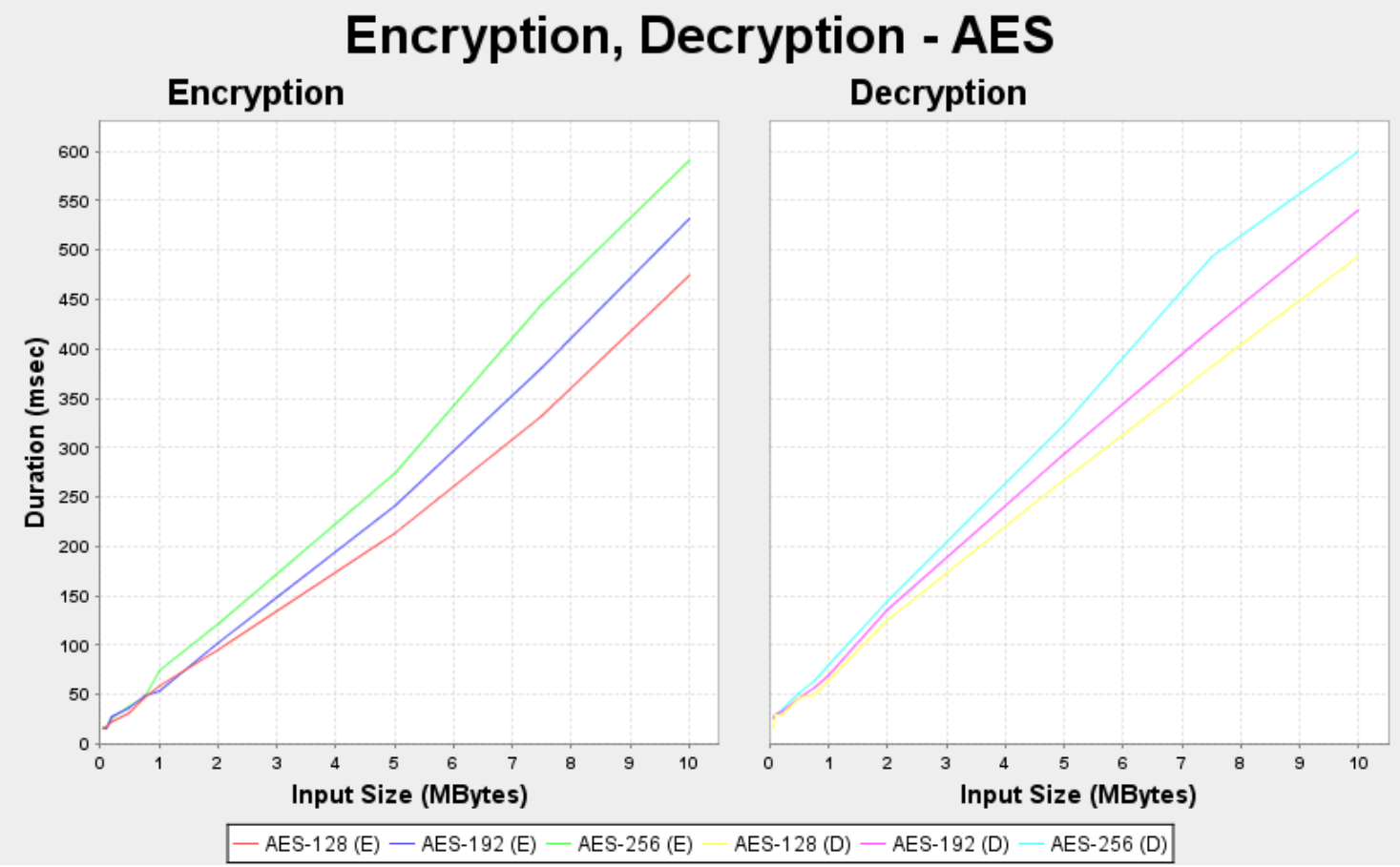
Αλγόριθμοι συμμετρικής κρυπτογραφίας

- Data Encryption Standard (DES)
  - Υιοθετήθηκε το 1977 από το NIST, FIPS PUB 46
  - Κλειδί μήκους 56 bits
  - Ακολουθεί το δίκτυο Feistel, με 16 γύρους επεξεργασίας
  - Το Electronic Frontier Foundation (EFF) κατάφερε να τον σπάσει το 1998, χρησιμοποιώντας συσκευή κόστους $250.000
- Triple DES (3DES)
  - Τρεις εφαρμογές του DES στη σειρά: $C = E(K_3, D(K_2, E(K_1, P)))$
  - Ασφαλέστερος αλλά εξαιρετικά αργός
- Advanced Encryption Standard (AES)
  - Υιοθετήθηκε το 2001 από το NIST, FIPS PUB 197
  - Κλειδιά μήκους 128, 192, 256 bits
  - Εξαιρετικά γρήγορος και ασφαλής

Επιδόσεις

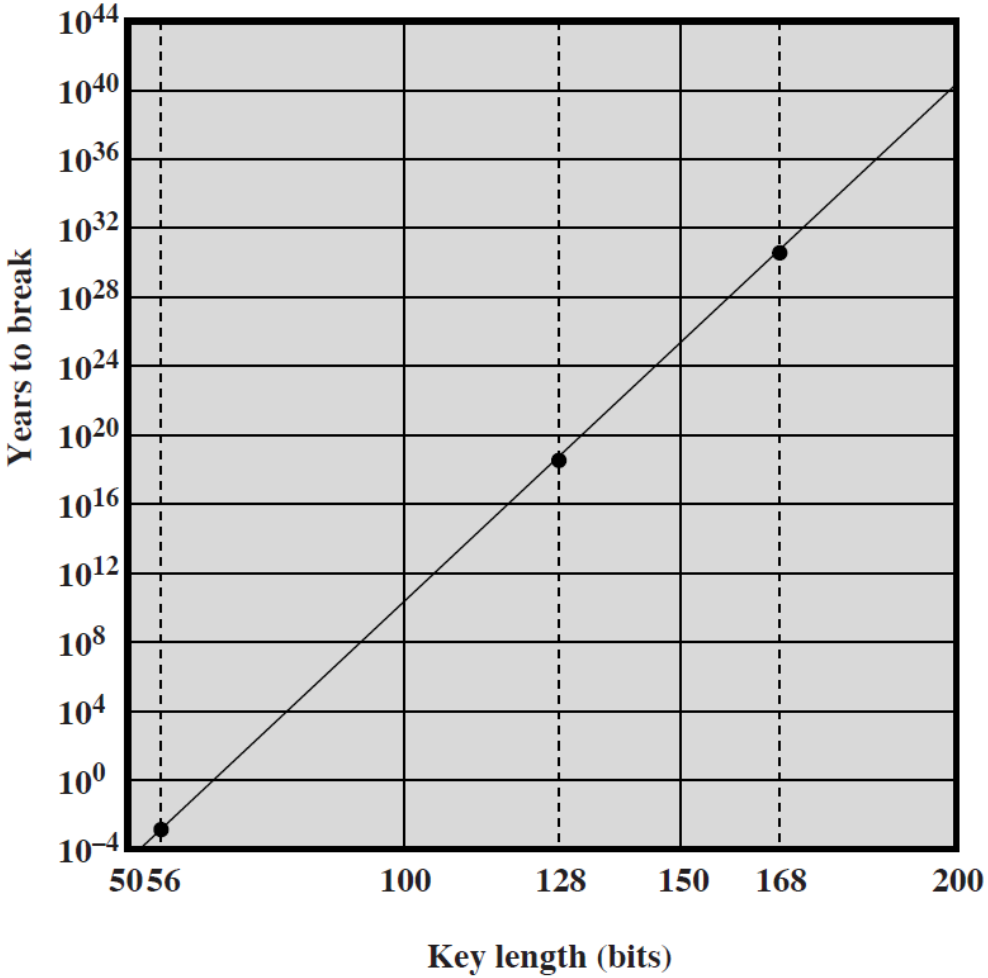

Encryption, Decryption - DES, Triple DES, IDEA
Encryption
Decryption
Duration (msec)
3.500
3.250
3.000
2.750
2.500
2.250
2.000
1.750
1.500
1.250
1.000
750
500
250
0
0 1 2 3 4 5 6 7 8 9 10
Input Size (MBytes)
Input Size (MBytes)
DES (E)
IDEA (E)
Triple-DES (E)
DES (D)
IDEA (D)
Triple-DES (D)

Επιδόσεις


Encryption, Decryption - AES
Encryption
Decryption
Duration (msec)
0
50
100
150
200
250
300
350
400
450
500
550
600
0
1
2
3
4
5
6
7
8
9
10
Input Size (MBytes)
Input Size (MBytes)
AES-128 (E)
AES-192 (E)
AES-256 (E)
AES-128 (D)
AES-192 (D)
AES-256 (D)

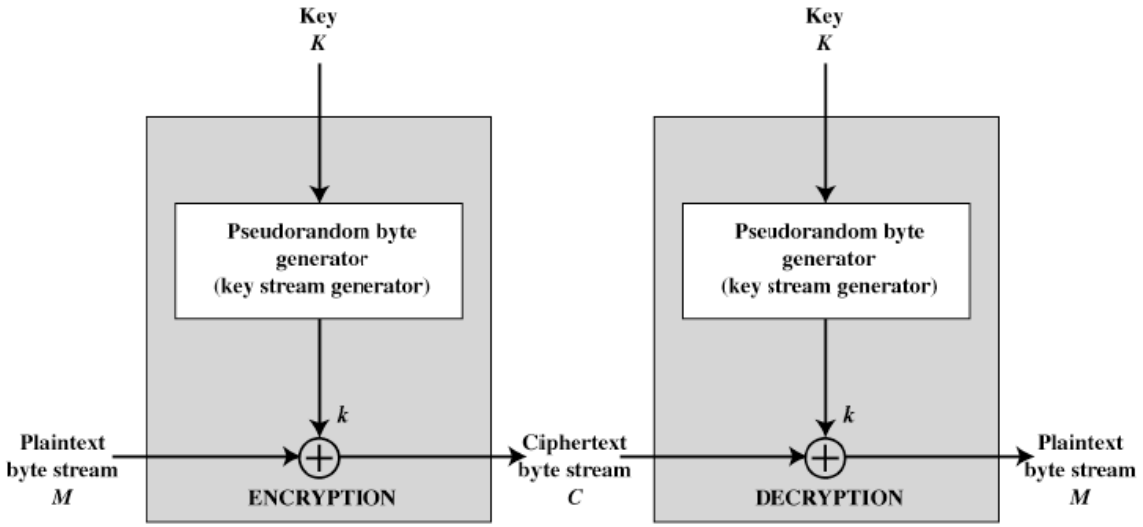
Κρυπτανάλυση DES

- Με το σύστημα του EFF:
  - ~ 3 μέρες για κλειδί μήκους 56 bits
  - ~10^{18} χρόνια για κλειδί μήκους 128 bits



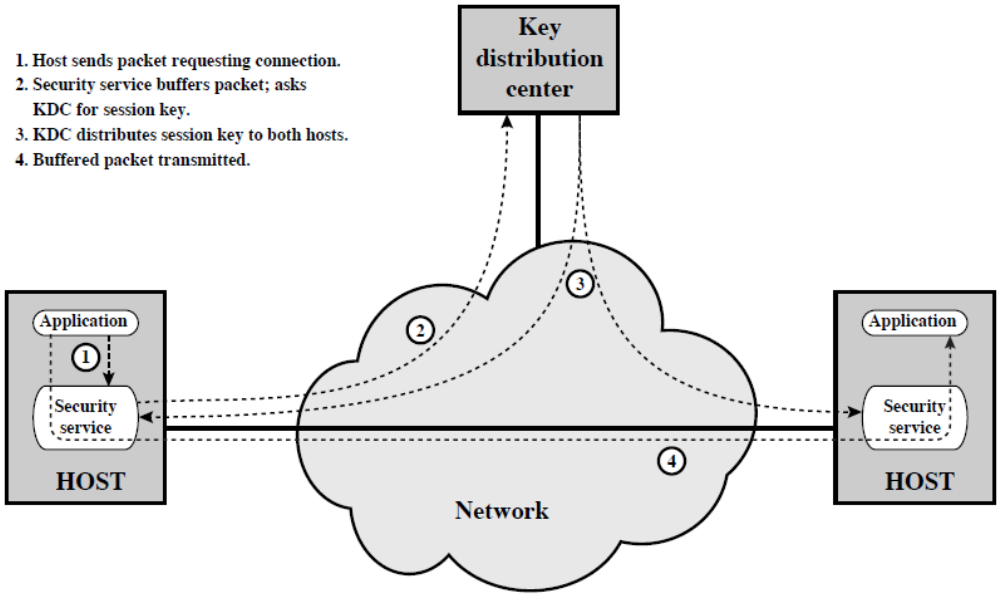
Κωδικοποιητές ροής

- Stream ciphers
- Δεν επεξεργάζονται τμήματα (blocks), αλλά ροές δεδομένων
- Κατάλληλοι για κατηγορίες εφαρμογών, όπως δικτυακές συνδέσεις
- Αντιπροσωπευτικό παράδειγμα: RC4 (Ron Rivest, 1987)
- Ο RC4 είναι εξαιρετικά γρήγορος και ασφαλής



Διανομή κλειδιών

- Το μεγάλο πρόβλημα της συμμετρικής κρυπτογραφίας...
- Διάφορες τεχνικές, που αφορούν
  - Τη διανομή με "φυσικό" τρόπο
  - Τη χρήση παλιού κλειδιού για τη διανομή του νέου
  - Την εκμετάλλευση κάποιας τρίτης οντότητας

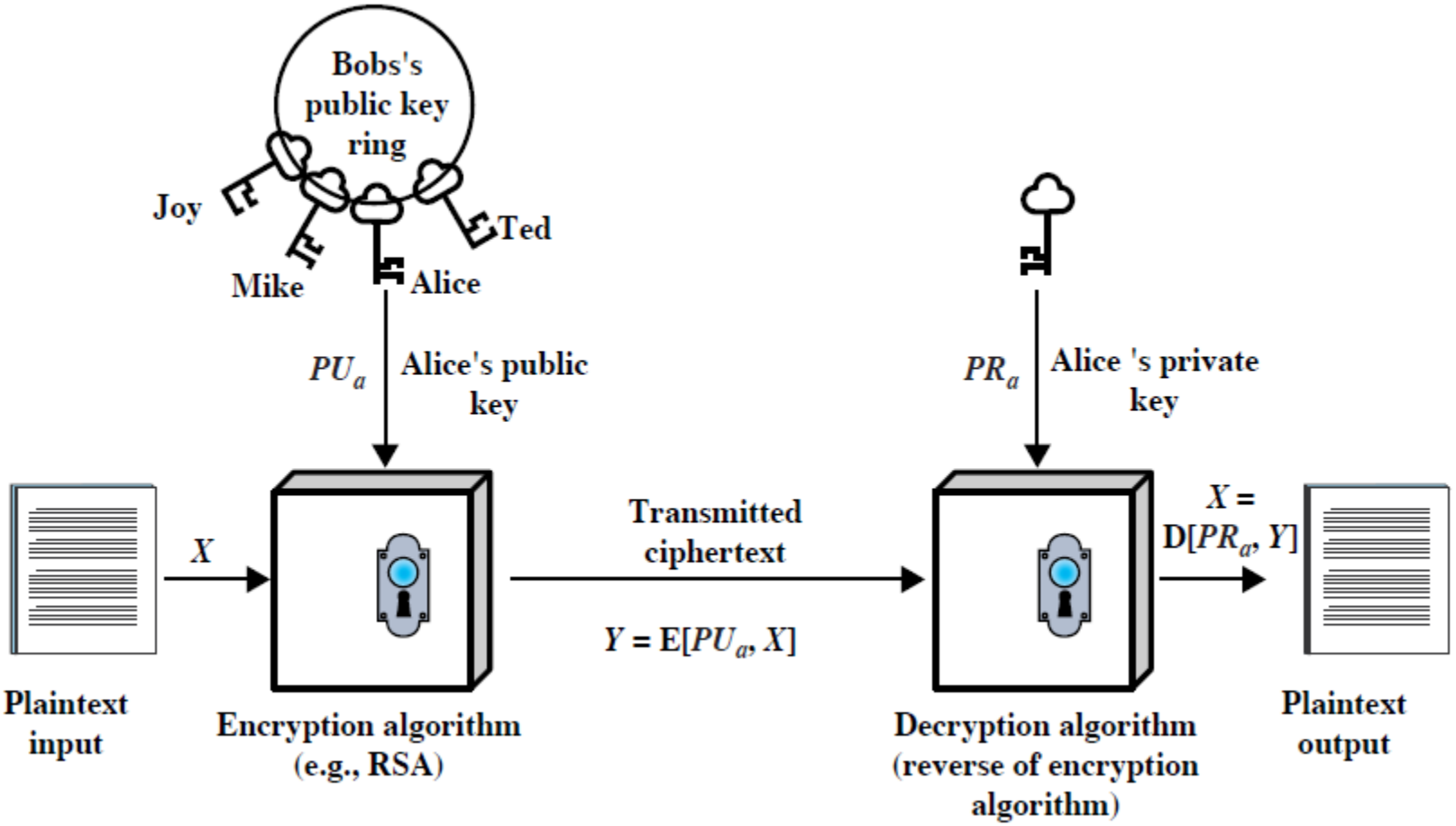


- Βιώσιμη λύση: **Κρυπτογραφία Δημοσίου Κλειδιού!**

Κρυπτογραφία δημοσίου κλειδιού

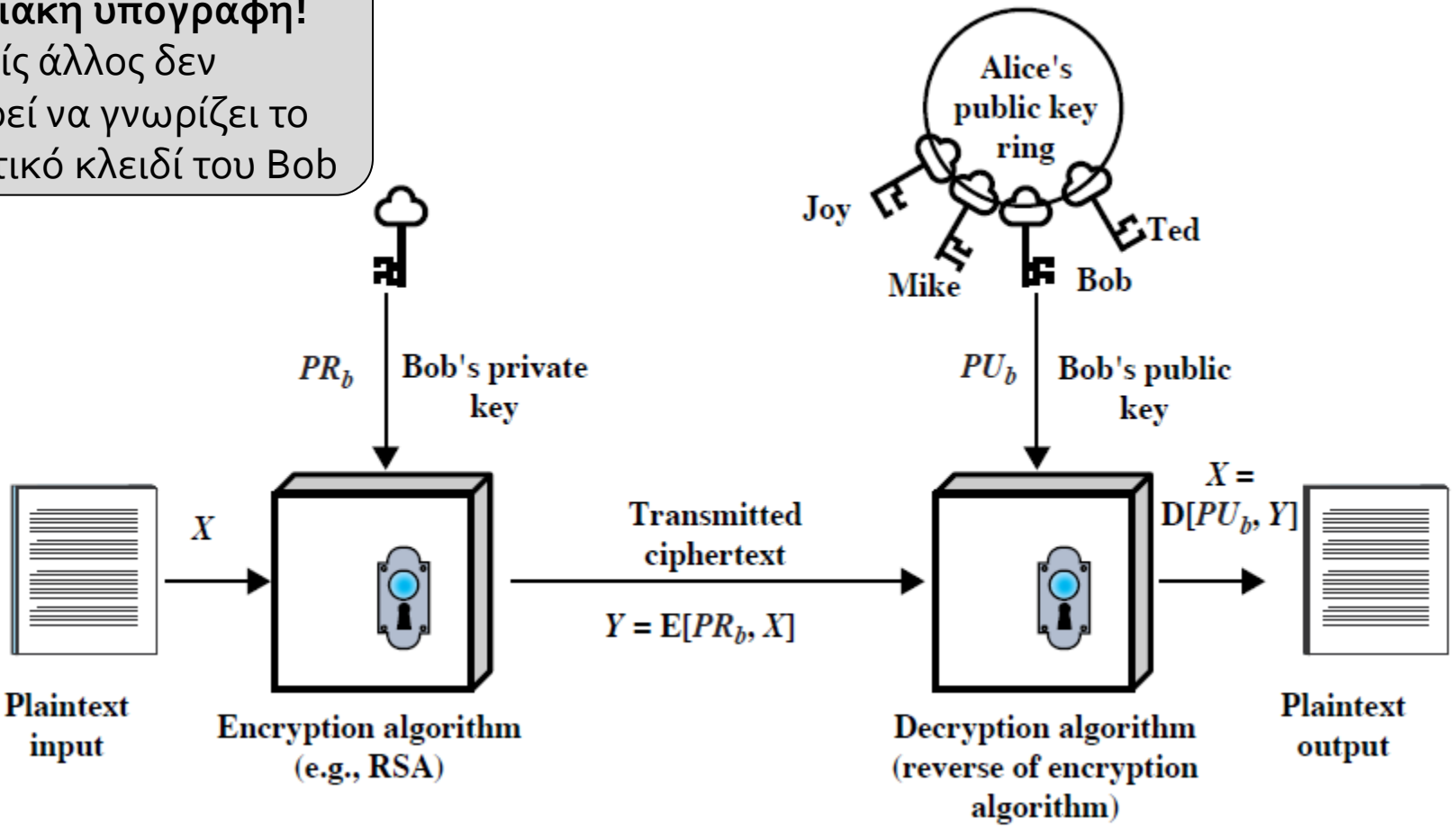
- Diffie & Hellman, 1976
- Ασύμμετρη κρυπτογραφία, με χρήση ζεύγους κλειδιών:
  - Ιδιωτικό κλειδί (private key), το οποίο παραμένει μυστικό
  - Δημόσιο κλειδί (public key), το οποίο καθίσταται γνωστό
- Βασίζεται σε μαθηματικές συναρτήσεις
- Βασική λογική: ό,τι κρυπτογραφείται με το ένα κλειδί, αποκρυπτογραφείται με το άλλο κλειδί
- Σημαντικές εφαρμογές:
  - Κρυπτογράφηση & αποκρυπτογράφηση
  - Διανομή κλειδιών
  - Ψηφιακές υπογραφές
- Αντιπροσωπευτικοί αλγόριθμοι:
  - Diffie-Hellman
  - Rivest-Shamir-Adleman (RSA)
  - Κρυπτογραφία ελλειπτικής καμπύλης (elliptic-curve cryptography)

Κρυπτογράφηση με ΚΔΚ



Πιστοποίηση αυθεντικότητας με ΚΔΚ

Ψηφιακή υπογραφή!
Κανείς άλλος δεν μπορεί να γνωρίζει το ιδιωτικό κλειδί του Bob



Ο αλγόριθμος RSA

- Δημιουργία ζεύγους κλειδιού
  - Επιλογή πρώτων αριθμών p, q, με $p \neq q$
  - Υπολογισμός $n = p \times q$
  - Υπολογισμός $\phi(n) = (p - 1)(q - 1)$
  - Επιλογή ακεραίου e: ΜΚΔ$(\phi(n), e) = 1$, $1 < e < \phi(n)$
  - Υπολογισμός d: $de \bmod \phi(n) = 1$
  - Ιδιωτικό κλειδί: d
  - Δημόσιο κλειδί: (n, e)
- Κρυπτογράφηση:
  - Αρχικό κείμενο: $M < n$
  - Κρυπτογράφημα: $C = M^e \bmod n$
- Αποκρυπτογράφηση:
  - Κρυπτογράφημα: C
  - Αρχικό κείμενο: $M = C^d \bmod n$

Ο αλγόριθμος RSA – παράδειγμα

- Δημιουργία ζεύγους κλειδιού
  - Επιλογή πρώτων αριθμών 2357, 2551
  - Υπολογισμός $n = p \times q = 6012707$
  - Υπολογισμός $\phi(n) = (p - 1)(q - 1) = 6007800$
  - Επιλογή ακεραίου e: $\text{ΜΚΔ}(\phi(n), e) = 1$, $1 < e < \phi(n) \longrightarrow e = 3674911$
  - Υπολογισμός d: $de \bmod \phi(n) = 1 \longrightarrow d = 422191$
  - Ιδιωτικό κλειδί: $d = 422191$
  - Δημόσιο κλειδί: $(n, e) = (6012707, 3674911)$
- Κρυπτογράφηση:
  - Αρχικό κείμενο: $M = 5234673$
  - Κρυπτογράφημα: $C = M^e \bmod n \longrightarrow C = 3650502$
- Αποκρυπτογράφηση:
  - Κρυπτογράφημα: $C = 3650502$
  - Αρχικό κείμενο: $M = C^d \bmod n \longrightarrow M = 5234673$

Συναρτήσεις κατακερματισμού

- Hash functions
- Συναρτήσεις που παράγουν μία "σύνοψη" των δεδομένων, συνήθως σταθερού μεγέθους
- Είναι μονόδρομες (one way), δηλαδή δεν είναι δυνατό να ανακτηθεί το αρχικό μήνυμα
- Χρησιμοποιούνται στις ψηφιακές υπογραφές
  - Αντί να κρυπτογραφηθεί ολόκληρο το μήνυμα, κρυπτογραφείται μόνο το αποτέλεσμα κάποιας συνάρτησης κατακερματισμού
- Αντιπροσωπευτικές συναρτήσεις κατακερματισμού:
  - MD2 (MD: Message Digest)
  - MD5
  - SHA-1 (SHA: Secure Hash Algorithm)
  - SHA-224
  - SHA-256
  - SHA-512

Πιστοποιητικά δημοσίου κλειδιού

- Θέμα: εφόσον το δημόσιο κλειδί είναι δημόσιο, ο καθένας μπορεί να δημοσιεύσει ένα κλειδί προσποιούμενος ότι είναι κάποιος άλλος
- π.χ.: κάποια ιστοσελίδα υποκρίνεται ότι είναι το amazon.com, δημοσιεύοντας και κάποιο αντίστοιχο δημόσιο κλειδί
- Λύση: πιστοποιητικά δημοσίου κλειδιού (Public Key Certificates), τα οποία πιστοποιούν με κρυπτογραφικό τρόπο την πατρότητα ενός δημοσίου κλειδιού
- Τα πιστοποιητικά δημοσίου κλειδιού εκδίδονται (και υπογράφονται) από "έμπιστες οντότητες"
  - Κυβερνητικούς οργανισμούς (π.χ., ΣΥΖΕΥΞΙΣ)
  - Φορείς κοινής αποδοχής (π.χ., VeriSign)

Χρήση πιστοποιητικού δημοσίου κλειδιού