Βασικές αρχές κρυπτογραφίας

Νικόλαος Ε. Κολοκοτρώνης
Επίκουρος Καθηγητής

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Πελοποννήσου
Email: nkolok@uop.gr
Web: http://www.uop.gr/~nkolok/

ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ

Περιεχόμενα

- Βασικοί ορισμοί
- Απαιτήσεις κι επιθέσεις
- Κλάσεις κρυπτοσυστημάτων
- Ρυθμοί λειτουργίας
- Συναρτήσεις σύνοψης

Στόχοι κρυπτογραφίας

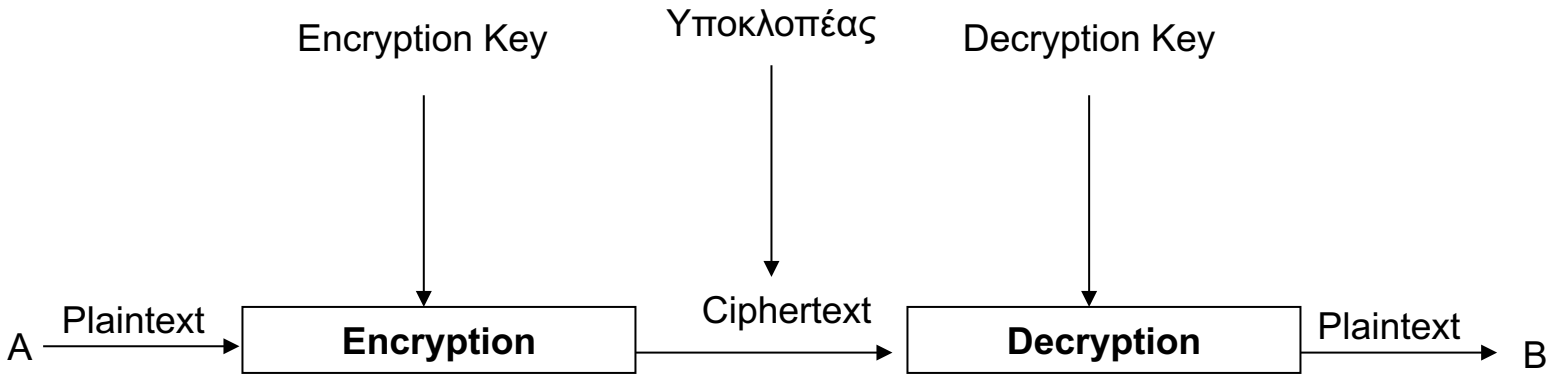
- Εμπιστευτικότητα
  Η προστασία από μη-εξουσιοδοτημένη αποκάλυψη της πληροφορίας
- Ακεραιότητα
  Η προστασία από μη-εξουσιοδοτημένη τροποποίηση της πληροφορίας
- Αυθεντικοποίηση
  Η επαλήθευση της ταυτότητας ενός χρήστη, μηχανής ή άλλης οντότητας

Βασική ορολογία

- Απλό κείμενο
  - The original message
- Κρυπτοκείμενο
  - The coded message
- Κρυπτογράφηση
  - Process of converting from plaintext to ciphertext
- Αποκρυπτογράφηση
  - Restoring the plaintext from the ciphertext
- Κρυπτοσύστημα
  - Schemes used for encryption
- Κρυπτανάλυση
  - Methods for deciphering with no knowledge of enciphering
- Κρυπτογραφία
  - Study of encryption
- Κρυπτολογία
  - Cryptography + cryptanalysis

Αλγόριθμοι και κλειδιά

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

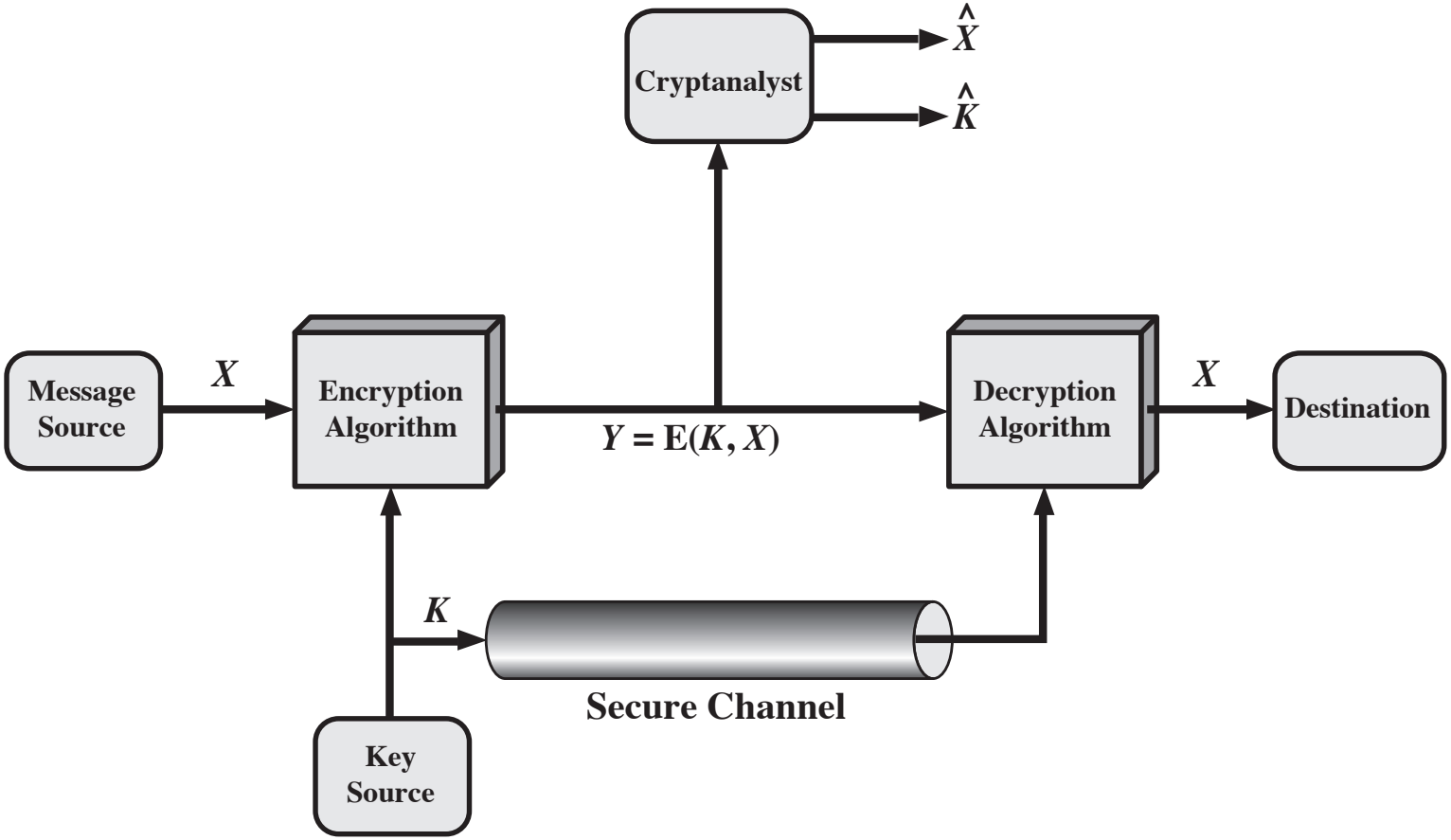


- Η ασφάλεια έγκειται στο ότι δεν είναι γνωστό το κλειδί
  οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης μπορούν να είναι ευρέως γνωστοί

Φορμαλιστικός ορισμός

- Αν Enc και Dec είναι οι συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης αντίστοιχα, τότε:
  - $\text{Enc}_{K1}(m) = c$
  - $\text{Dec}_{K2}(c) = m$
- όπου m και c υποδηλώνουν το αρχικό και το κρυπτογραφημένο μήνυμα αντίστοιχα.
- Οι δείκτες K_i υποδηλώνουν την εξάρτηση των συναρτήσεων από το κλειδί.
- Οι συναρτήσεις έχουν την ιδιότητα $\text{Dec}_{K2}(\text{Enc}_{K1}(m)) = m$

Ασφάλεια κρυπταλγορίθμων



Ασφάλεια κρυπταλγορίθμων

Cryptanalysis

- Attack relies on the nature of the algorithm + knowledge of general characteristics of the plaintext
- Attack exploits the characteristics of the algorithm to deduce (a) a specific plaintext or (b) the key being used

Brute-force attack

- Attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained
- On average, half of all possible keys must be tried to achieve success

Ασφάλεια κρυπταλγορίθμων

Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Brute-force attack

Involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained

On average, half of all possible keys must be tried to achieve success

To supplement the brute-force approach, some degree of knowledge about the expected plaintext is needed, and some means of automatically distinguishing plaintext from garble is also needed

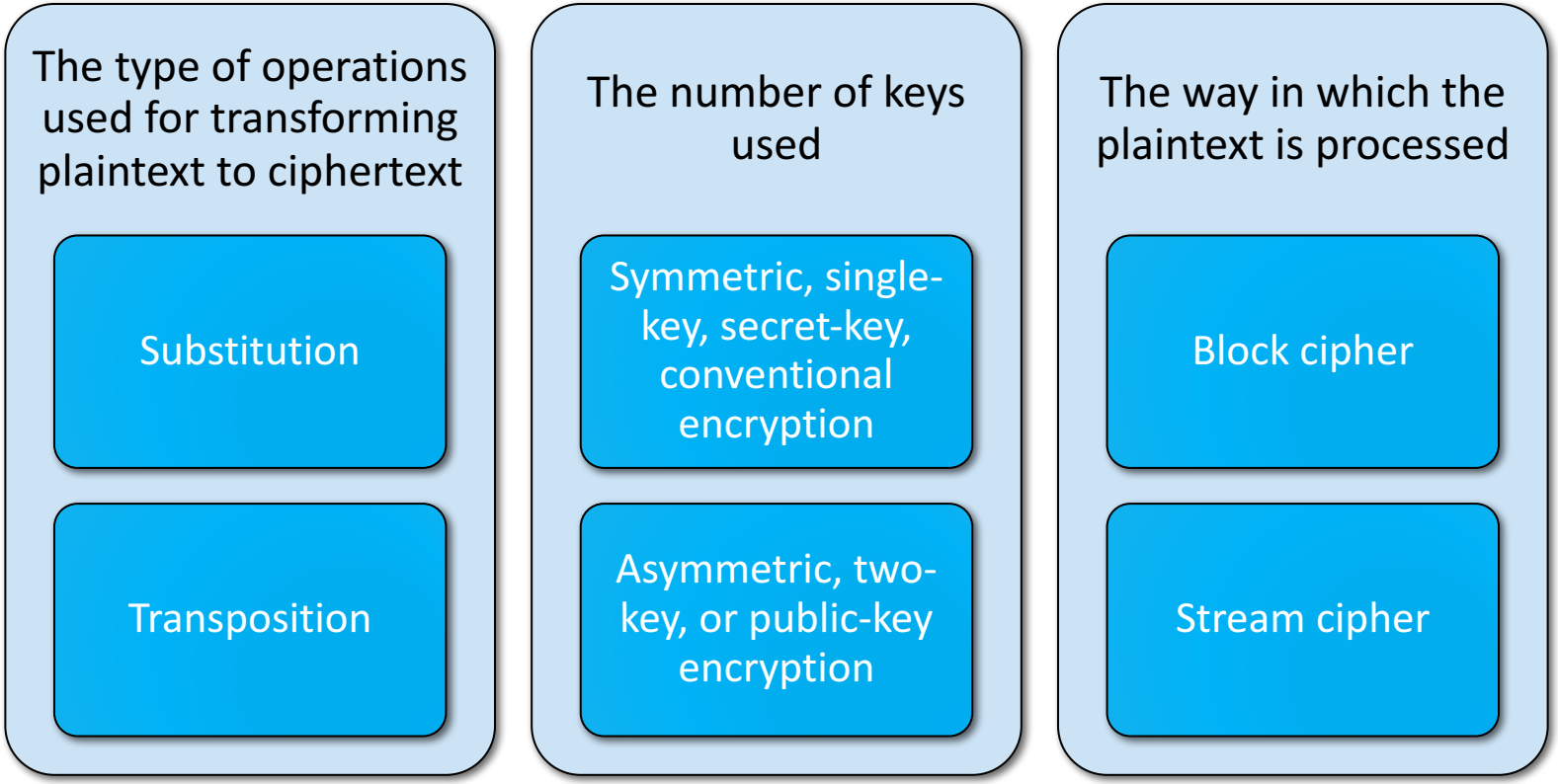
Brute-force attack

Key size (bits)	Number (N) of alternative keys	Time required at 1 encryption/µs	Time required at 10^6 encryptions/µs
32	$2^{32} = 4.3 \times 10^{09}$	35.8 minutes	2.15 ms
56	$2^{56} = 7.2 \times 10^{16}$	1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{36} years	5.9×10^{30} years
26 chars (permut)	$26! = 4.0 \times 10^{26}$	6.4×10^{12} years	6.4×10^{06} years

$T = 0.5 \times N$ µs

Κατηγορίες αλγορίθμων

- Characterized along three independent dimensions:



Κατηγοριοποίηση: πράξεις

- Is one in which the letters of plaintext are replaced by other letters or by numbers or symbols
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns
- Examples include
  - Caesar's cipher
  - Monoalphabetic ciphers
  - Vernam's cipher

Κατηγοριοποίηση: κλειδιά

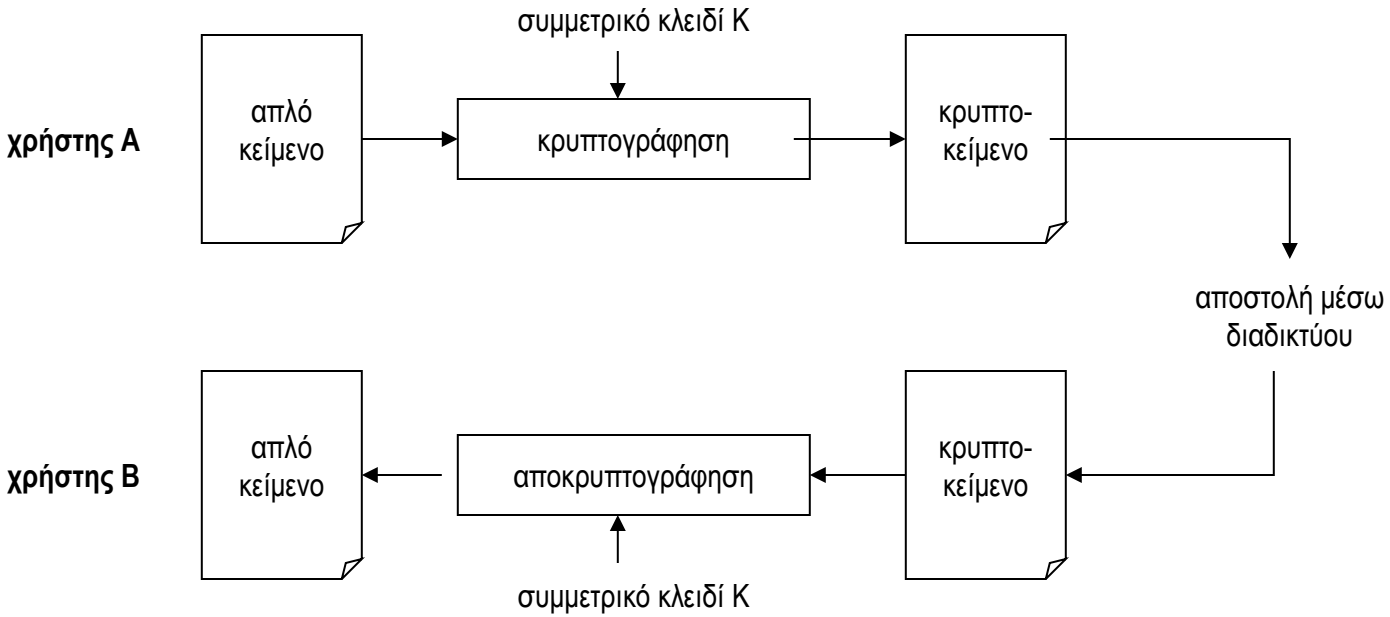
- Αλγόριθμοι συμμετρικού (ή κρυφού) κλειδιού (symmetric key algorithms)
  - Χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση
- Αλγόριθμοι ασύμμετρου (ή δημοσίου) κλειδιού (asymmetric - or public key - algorithms)
  - Χρησιμοποιούνται διαφορετικά κλειδιά για την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

Παραδείγματα αλγορίθμων

- Συμμετρική κρυπτογραφία
  - AES, DES, IDEA, RC2, RC4, RC5, E0, A5/1
  - ταχύτεροι και πιο ασφαλείς
- Ασύμμετρη κρυπτογραφία
  - RSA, DSA, ECC, Knapsack, ElGamal
- Το μέγεθος του κλειδιού εξαρτάται από:
  - τη μεθοδολογία της κρυπτογραφίας
  - την φύση των δεδομένων προς κρυπτογράφηση
  - την αξία των δεδομένων προς κρυπτογράφηση

Συμμετρική κρυπτογραφία

- Εμπιστευτικότητα



Συμμετρική κρυπτογραφία

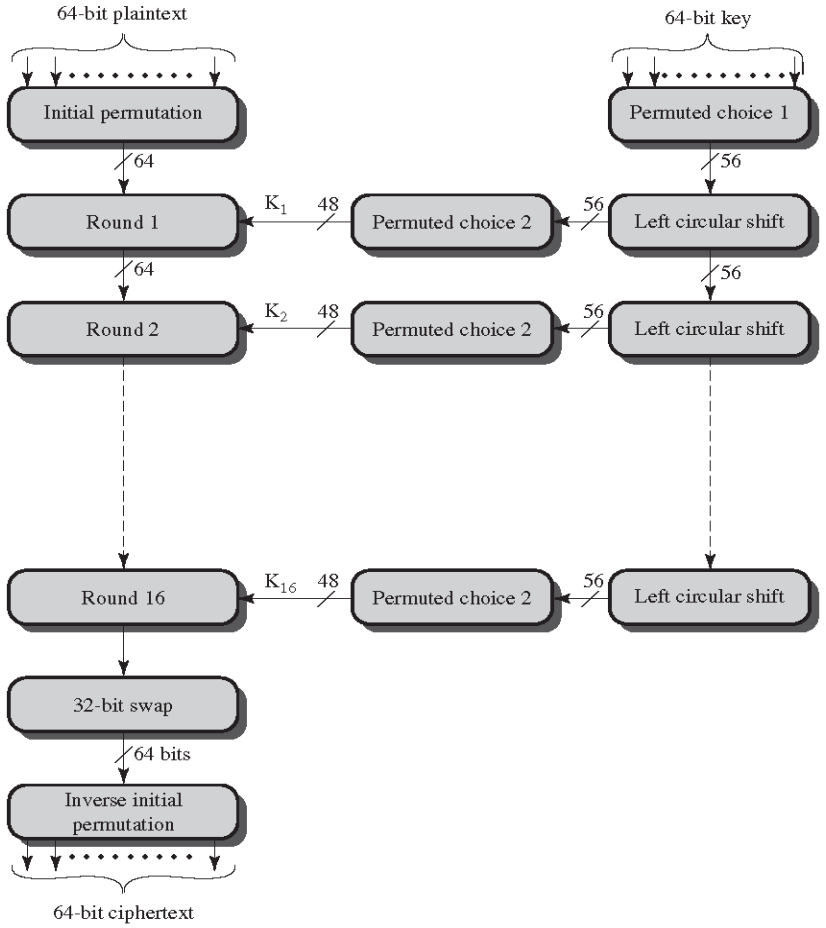
- Το ίδιο κλειδί χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων
- Τα προβλήματα που αντιμετωπίζει είναι:
  - η διανομή των συμμετρικών κλειδιών σε ανοικτά δίκτυα (γνωστό ως “πρόβλημα του τετραγώνου”)
  - για *n* χρήστες χρειαζόμαστε $\binom{n}{2} = \frac{n(n-1)}{2}$ κλειδιά
  - η χρήση τέτοιων μηχανισμών σε ευρεία κλίμακα
  - η αποθήκευση και διαχείριση κλειδιών
- Τα κλειδιά έχουν πεπερασμένη περίοδο ζωής

DES: Data Encryption Standard

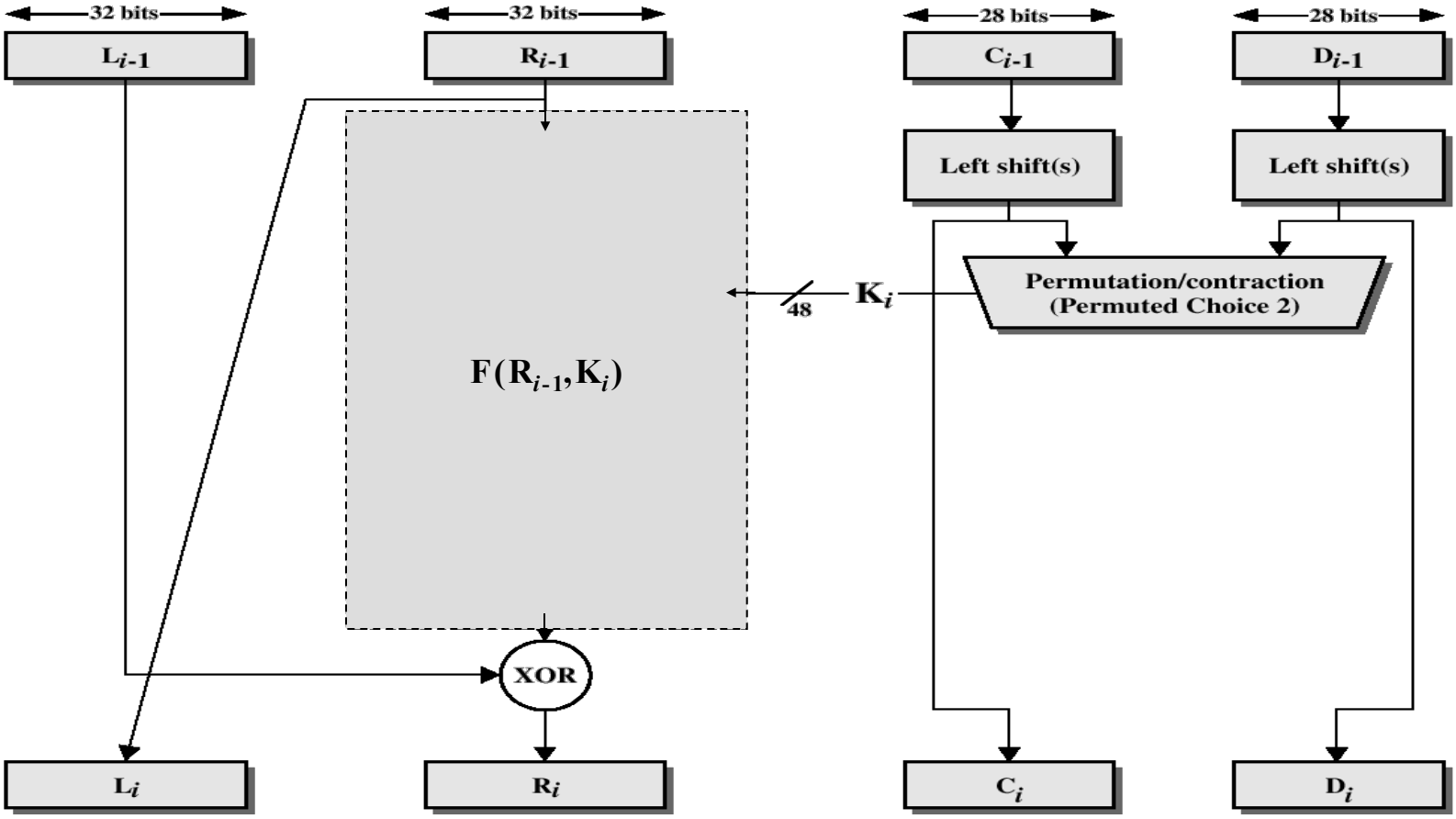
- Το 1973 ο NIST έθεσε μία δημόσια πρόσκληση για προσφορές κρυπταλγορίθμων με τα χαρακτηριστικά
  - Παροχή υψηλού επιπέδου προστασίας
  - Η ασφάλεια να έγκειται στην ύπαρξη κλειδιού
  - Προσαρμοστικότητα σε ποικίλες εφαρμογές
  - Οικονομική hardware υλοποίηση
  - Αποδοτικό στη χρήση και αξιόπιστο
  - Δυνατότητα φορητότητας (exportable)

DES: Δομή αλγορίθμου

- Βασικά χαρακτηριστικά
  - 64-bit blocks
  - 56-bit κλειδί (+ 8 bits ισοτιμίας)
  - 16 γύροι
- Στην αρχή και τέλος πραγματοποιείται μετάθεση των bits
- Το κλειδί ολισθαίνει κυκλικά σε κάθε γύρο

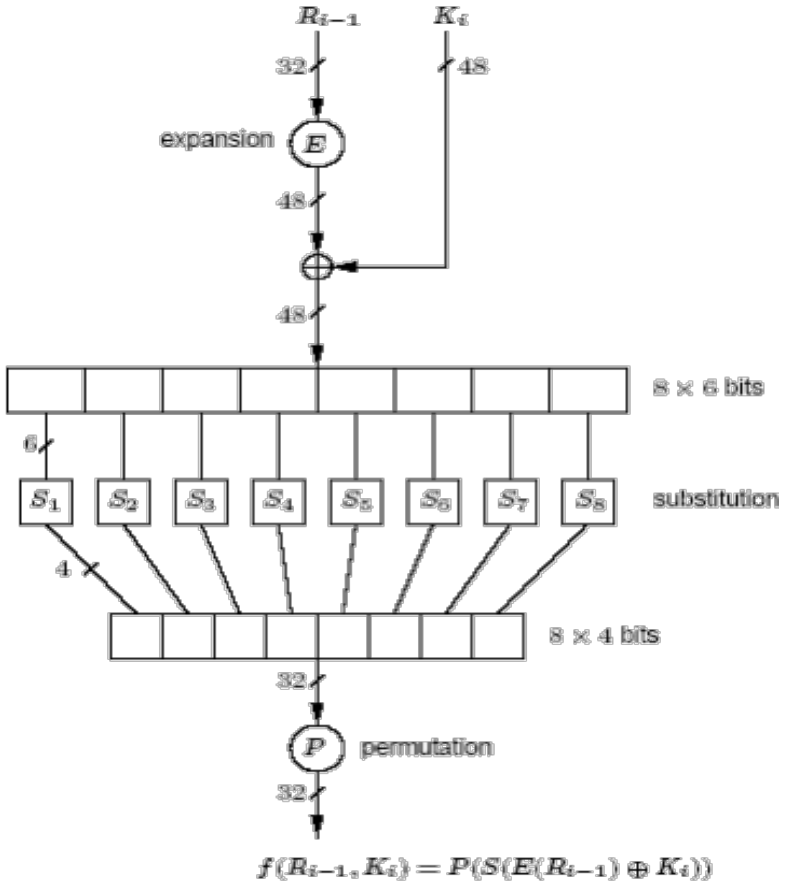


DES: Συνάρτηση γύρου



DES: Συνάρτηση γύρου

- Υπολογισμός F(R_{i-1}, K_i)
  - Χρήση του E για τη μετατροπή του 32-bit R_{i-1} σε 48-bit block
  - Το αποτέλεσμα διασπάται σε 8 blocks $\mathbf{b}_1$, …, $\mathbf{b}_8$ των 6 bits
- Υπολογισμός s-boxes:
  - Κάθε $\mathbf{b}_j$ είναι είσοδος σε ένα κουτί αντικατάστασης (s-box)
  - 4-bit block $\mathbf{c}_j = s_j(\mathbf{b}_j)$ ως έξοδος
  - Τα $\mathbf{c}_1$, …, $\mathbf{c}_8$ μετατίθενται με P



DES: Στρώμα αντικατάστασης

s-box 1															
e	4	d	1	2	f	b	8	3	a	6	c	5	9	0	7
0	f	7	4	e	2	d	1	a	6	c	b	9	5	3	8
4	1	e	8	d	6	2	b	f	c	9	7	3	a	5	0
f	c	8	2	4	9	1	7	5	b	3	e	a	0	6	d

s-box 2															
f	1	8	e	6	b	3	4	9	7	2	d	c	0	5	a
3	d	4	7	f	2	8	e	c	0	1	a	6	9	b	5
0	e	7	b	a	4	d	1	5	8	c	6	9	3	2	f
d	8	a	1	3	f	4	2	b	6	7	c	0	5	e	9

s-box 3															
a	0	9	e	6	3	f	5	1	d	c	7	b	4	2	8
d	7	0	9	3	4	6	a	2	8	5	e	e	b	f	1
d	6	4	9	8	f	3	0	b	1	2	c	5	a	e	7
1	a	d	0	6	9	8	7	4	f	e	3	b	5	2	c

s-box 4															
7	d	e	3	0	6	9	a	1	2	8	5	b	c	4	f
d	8	b	5	6	f	0	3	4	7	2	c	1	a	e	9
a	6	9	0	c	b	7	d	f	1	3	e	5	2	8	4
3	f	0	6	a	1	d	8	9	4	5	b	c	7	2	e

s-box 5															
2	c	4	1	7	a	b	6	8	5	3	f	d	0	e	9
e	b	2	c	4	7	d	1	5	0	f	a	3	9	8	6
4	2	1	b	a	d	7	8	f	9	c	5	6	3	0	e
b	8	c	7	1	e	2	d	6	f	0	9	a	4	5	3

s-box 6															
c	1	a	f	9	2	6	8	0	d	3	4	e	7	5	b
a	f	4	2	7	c	9	5	6	1	d	e	0	b	3	8
9	e	f	5	2	8	c	3	7	0	4	a	1	d	b	6
4	3	2	c	9	5	f	a	b	e	1	7	6	0	8	d

s-box 7															
4	b	2	e	f	0	8	d	3	c	9	7	5	a	6	1
d	0	b	7	4	9	1	a	e	3	5	c	2	f	8	6
1	4	b	d	c	3	7	e	a	f	6	8	0	5	9	2
6	b	d	8	1	4	a	7	9	5	0	f	e	2	3	c

s-box 8															
d	2	8	4	6	f	b	1	a	9	3	e	5	0	c	7
1	f	d	8	a	3	7	4	c	5	6	b	0	e	9	2
7	b	4	1	9	c	e	2	0	6	a	d	f	3	5	8
2	1	e	7	4	a	8	d	f	c	9	0	3	5	6	b

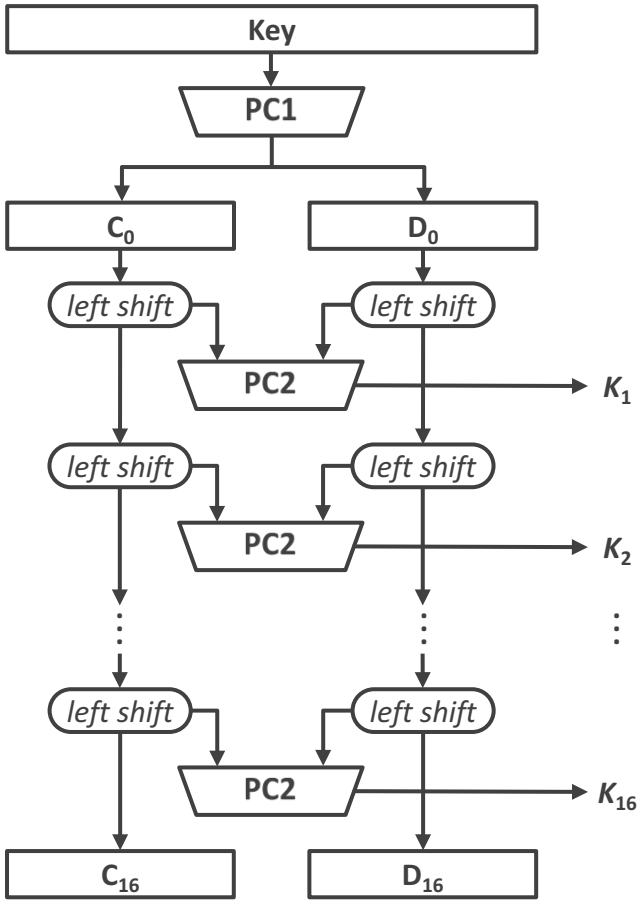
DES: Στρώμα αντιμετάθεσης

- Η 32-bit έξοδος από τα S-boxes περνά από ένα **P-box**
- Αυτό μεταθέτει τα bits με βάση τον πίνακα P
  - Το 1ο bit εξόδου θα είναι το 16ο bit της εισόδου
  - Το 2ο bit εξόδου θα είναι το 7ο bit της εισόδου
  - κ.ο.κ.

- Πίνακας P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

DES: Υπολογισμός κλειδιού



iteration no.	left shift
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

DES: Κρυπτανάλυση

- Ο DES προσέλκυσε το ενδιαφέρον κρυπταναλυτών για την εύρεση μεθόδων που θα μπορούσαν να τον «σπάσουν»
- Ενδεικτικοί αλγόριθμοι κρυπτανάλυσης
  - Διαφορική κρυπτανάλυση (differential cryptanalysis – Biham and Shamir, 1990)
  - Γραμμική κρυπτανάλυση (linear cryptanalysis – Matsui, 1993)
- Οι μέθοδοι αυτές εφαρμόζονται σε κάθε νέο αλγόριθμο που προτείνεται, για τον έλεγχο της ασφάλειάς του

DES: Ανασφαλής αλγόριθμος

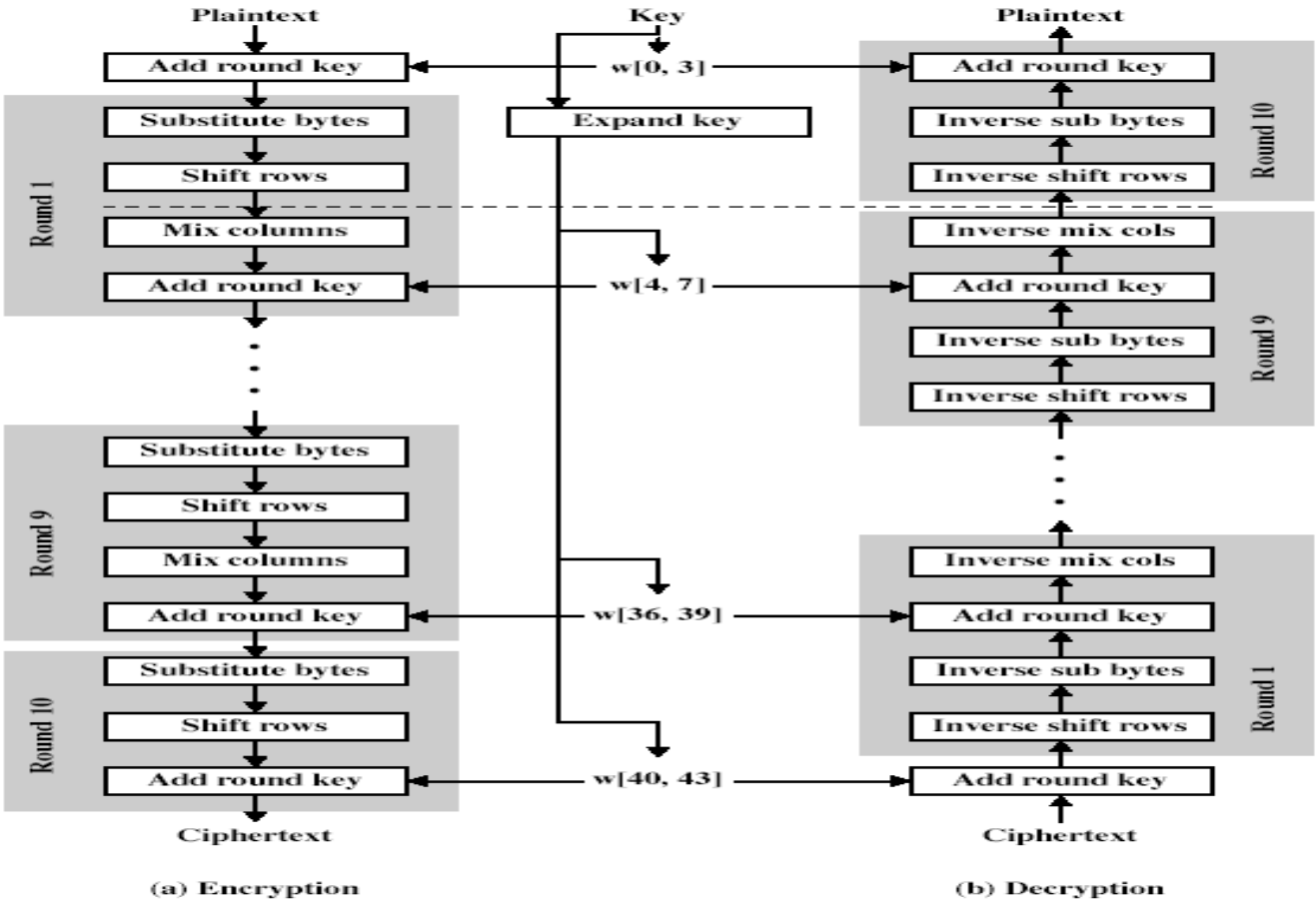
- Το 1996 άρχισε διάλογος για την ασφάλεια του DES
- Electronic Frontier Foundation DES Cracker project
  - 8-byte known plaintext attack σε λιγότερο από μία εβδομάδα
  - 16-byte known ciphertext στον ίδιο χρόνο
  - … τα παραπάνω σε 40 MHz chips …
- Το 1998, στοχευμένο h/w $250K τον έσπασε σε 56 ώρες
  - Το 1999 ο χρόνος αυτός μειώθηκε σε 22 ώρες
  - Έλεγχος 90 δισεκατομμυρίων κλειδιών το δευτερόλεπτο

AES: Advanced Encryption Std.

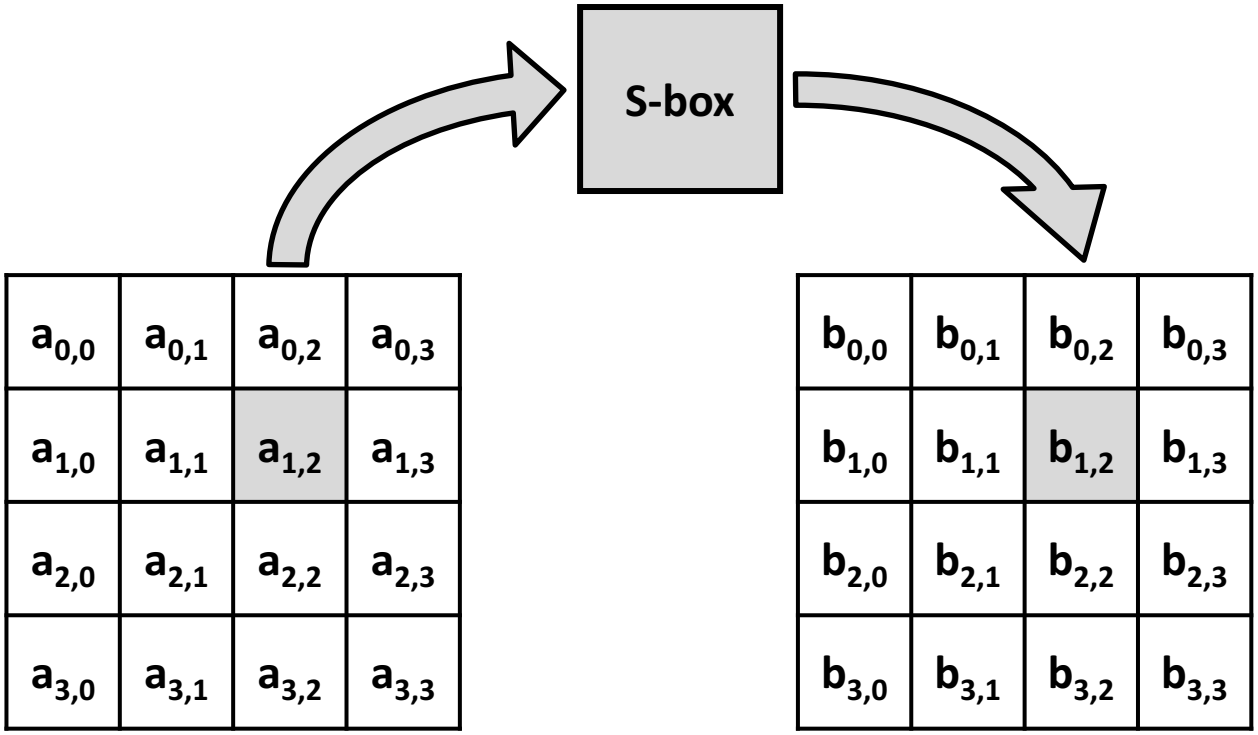
- Φιλοσοφία σχεδιασμού (128, 192, 256 bits κλειδί)
  - Απλότητα σχεδιασμού
  - Κατάλληλο για χρήση σε Smart cards (γενικά σε συσκευές με χαμηλή υπολογιστική ισχύ)
  - Ευέλικτη υλοποίηση σε εξειδικευμένο υλικό
- Αριθμός γύρων N_r αναλόγως του μεγέθους του κλειδιού

Key	128	192	256
N_r	10	12	14

AES: Δομή αλγορίθμου



AES: Στρώμα αντικατάστασης

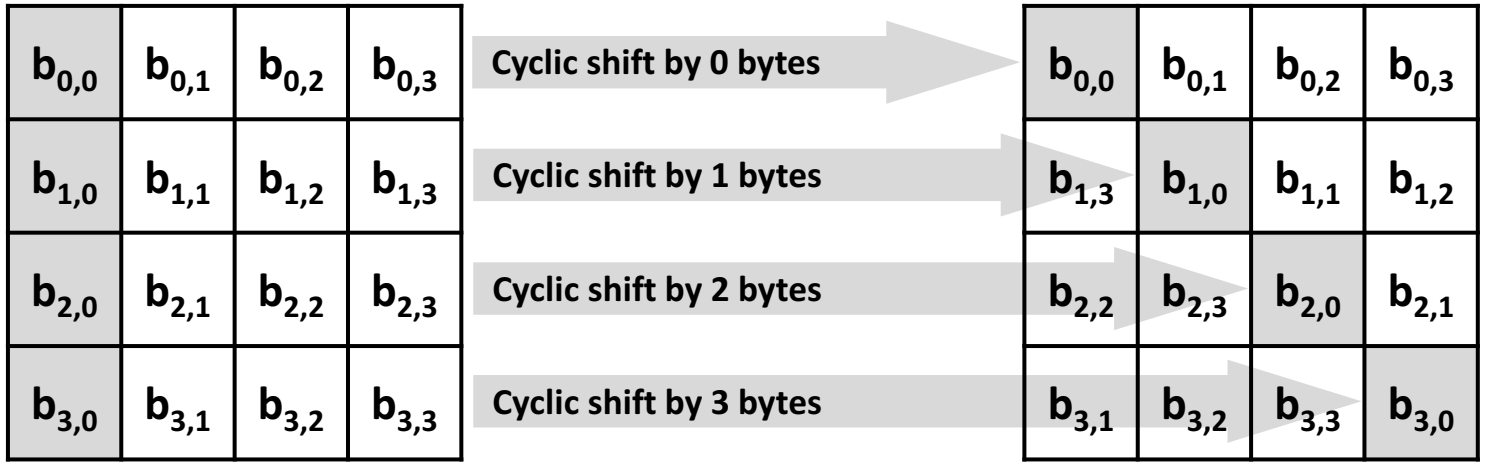


AES: Στρώμα αντικατάστασης

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	31	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

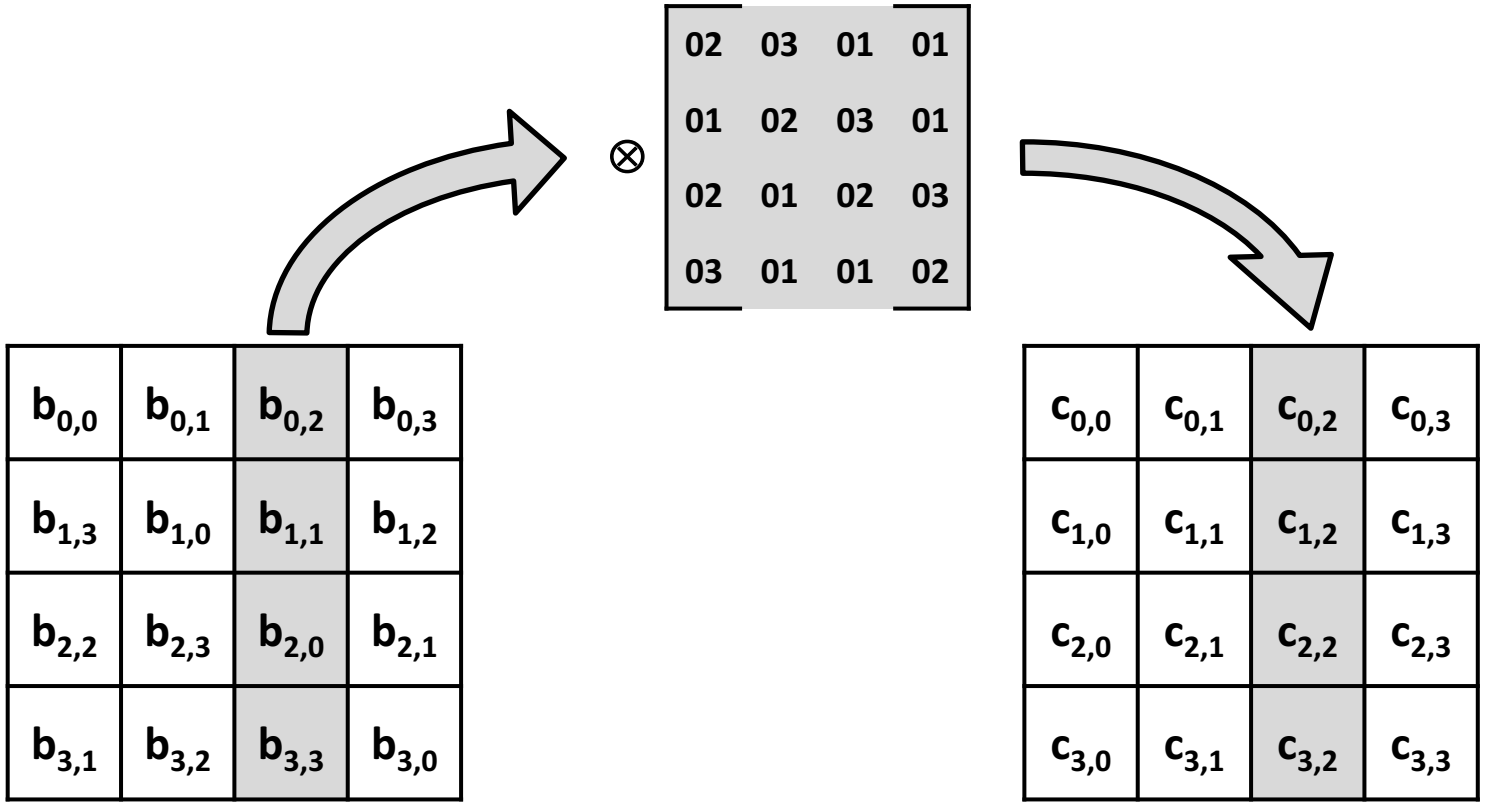
AES: Στρώμα αντιμετάθεσης

- Διάχυση ανά γραμμή



AES: Στρώμα αντιμετάθεσης

- Διάχυση ανά στήλη



AES: Προσθήκη κλειδιού

- Προσθέτουμε το κλειδί κάθε γύρου

$c_{0,0}$	$c_{0,1}$	$c_{0,2}$	$c_{0,3}$
$c_{1,0}$	$c_{1,1}$	$c_{1,2}$	$c_{1,3}$
$c_{2,0}$	$c_{2,1}$	$c_{2,2}$	$c_{2,3}$
$c_{3,0}$	$c_{3,1}$	$c_{3,2}$	$c_{3,3}$

$\oplus$

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

=

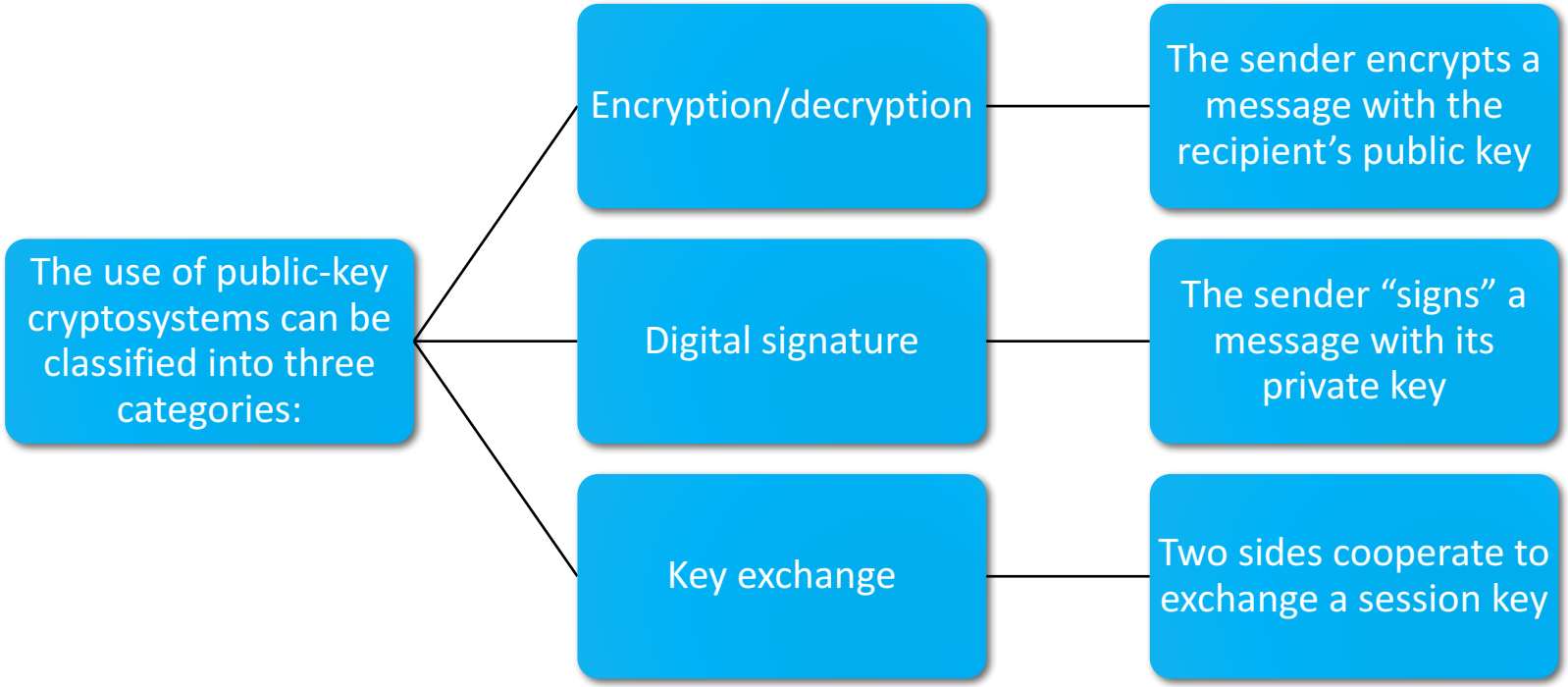
$d_{0,0}$	$d_{0,1}$	$d_{0,2}$	$d_{0,3}$
$d_{1,0}$	$d_{1,1}$	$d_{1,2}$	$d_{1,3}$
$d_{2,0}$	$d_{2,1}$	$d_{2,2}$	$d_{2,3}$
$d_{3,0}$	$d_{3,1}$	$d_{3,2}$	$d_{3,3}$

AES: Επισκόπηση

AES: Θέματα υλοποίησης

- Can efficiently be implemented on 32-bit CPU
  - Redefine steps to use 32-bit words
  - Can precompute 4 tables of 256-words
  - Then each column in each round can be computed using 4 table lookups + 4 XORs
  - At a cost of 16Kb to store tables
- Designers believe this very efficient implementation was a key factor in its selection as the AES cipher

Ασύμμετρη κρυπτογραφία



Ασύμμετρη κρυπτογραφία

- Factoring: Για δοθέν ακέραιο *n*, εύρεση της παραγοντοποίησής του σε πρώτους παράγοντες
- Discrete logarithm: Δοθέντος ενός ακεραίου *q*, ενός στοιχείου-γεννήτορα *g* μιας ομάδας *G* και στοιχείου g^x, εύρεση του *x* mod *q* της ομάδας Z_q^*

Ασύμμετρη κρυπτογραφία

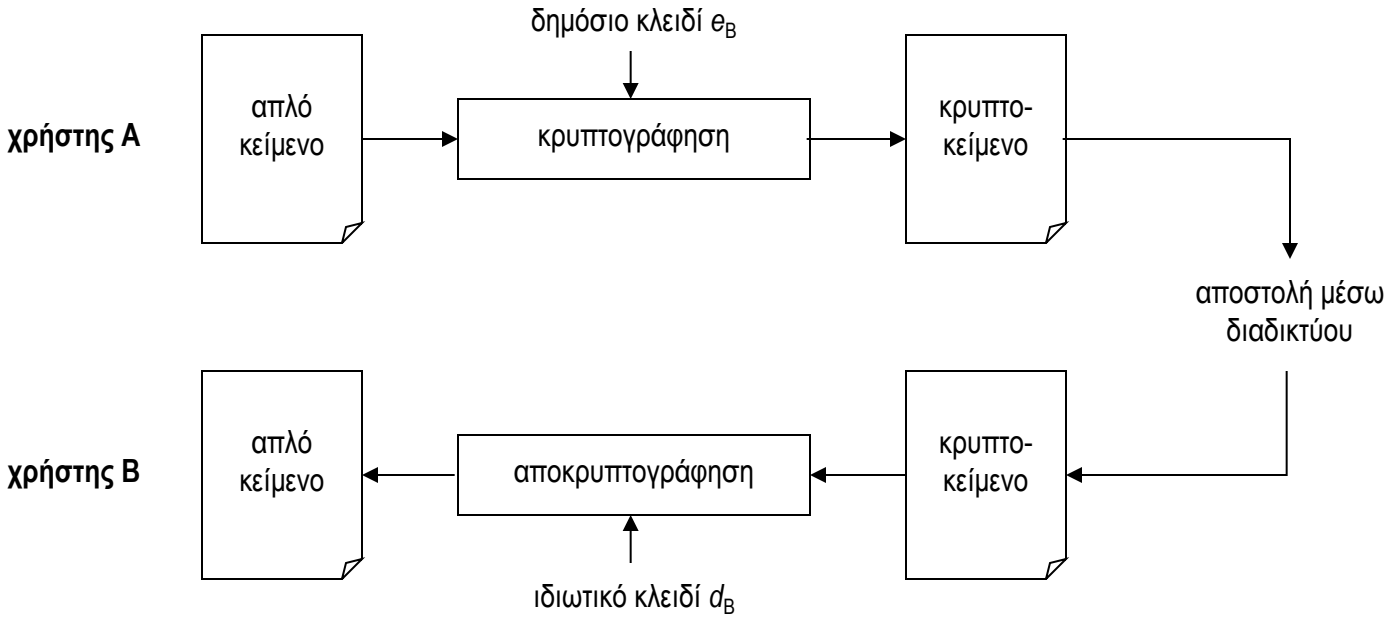
Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No
Elliptic Curve	Yes	Yes	Yes

Ασύμμετρη κρυπτογραφία

- Κάθε συμμετέχων στο σύστημα έχει ένα ζευγάρι κλειδιών *e* και *d*, αντίστροφα μεταξύ τους: $\mathrm{Dec}_d(\ \mathrm{Enc}_e(m)\ ) = m$
- Διαφορετικές συναρτήσεις χρησιμοποιούνται για κρυπτογράφηση και αποκρυπτογράφηση
- Ένα από τα κλειδιά μπορεί να είναι γνωστό, εφ' όσον η γνώση αυτή δε διευκολύνει την ανάκτηση του άλλου κλειδιού
- Το *e* μπορεί να είναι δημόσιο (γνωστό) αλλά το *d* κρατείται μυστικό
- Η ανταλλαγή κλειδιών μεταξύ αποστολέα και παραλήπτη αντικαθίσταται από την ύπαρξη ενός διαφανούς καταλόγου
  - Όλοι έχουν πρόσβαση και περιέχει τα κλειδιά *e* όλων των συμμετεχόντων

Ασύμμετρη κρυπτογραφία

- Εμπιστευτικότητα

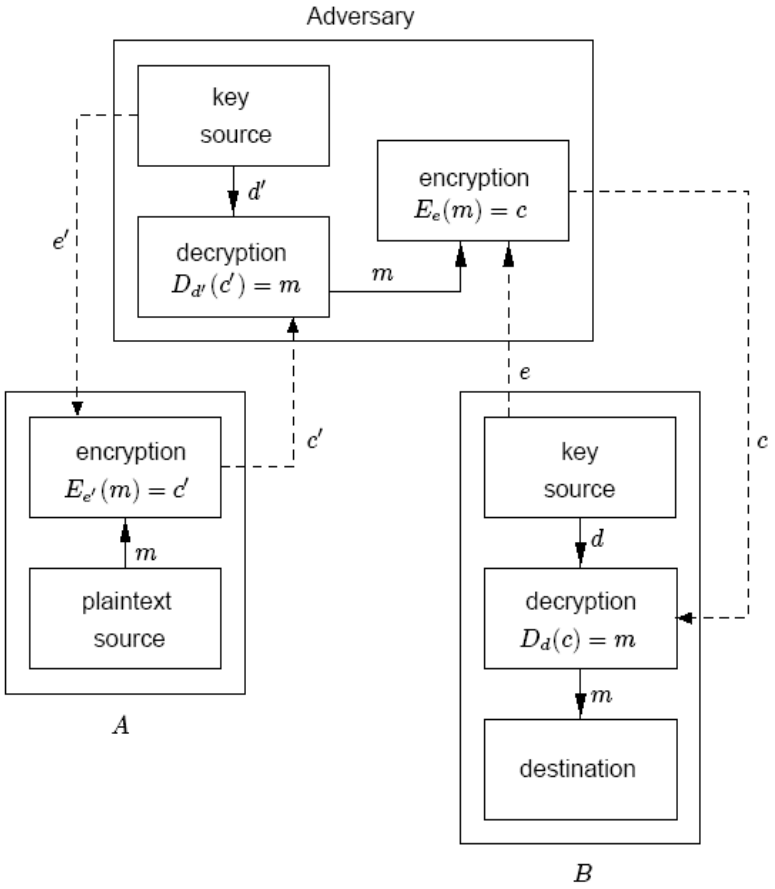


Ασύμμετρη κρυπτογραφία

- Ο οποιοσδήποτε μπορεί να προσποιηθεί ότι είναι κάποιος άλλος χρήστης!!
- Βήματα:
  - ο επιτιθέμενος «σταματάει» το μήνυμα που στέλνει ο Α στον Β
  - γράφει ένα δικό του και το στείλει στον Β (κρυπτογραφημένο με το δημόσιο κλειδί του Β)
  - τότε ο Β δεν θα γνωρίζει τον πραγματικό αποστολέα του μηνύματος που λαμβάνει
- Ανάγκη πιστοποίησης της ταυτότητας κάθε χρήστη

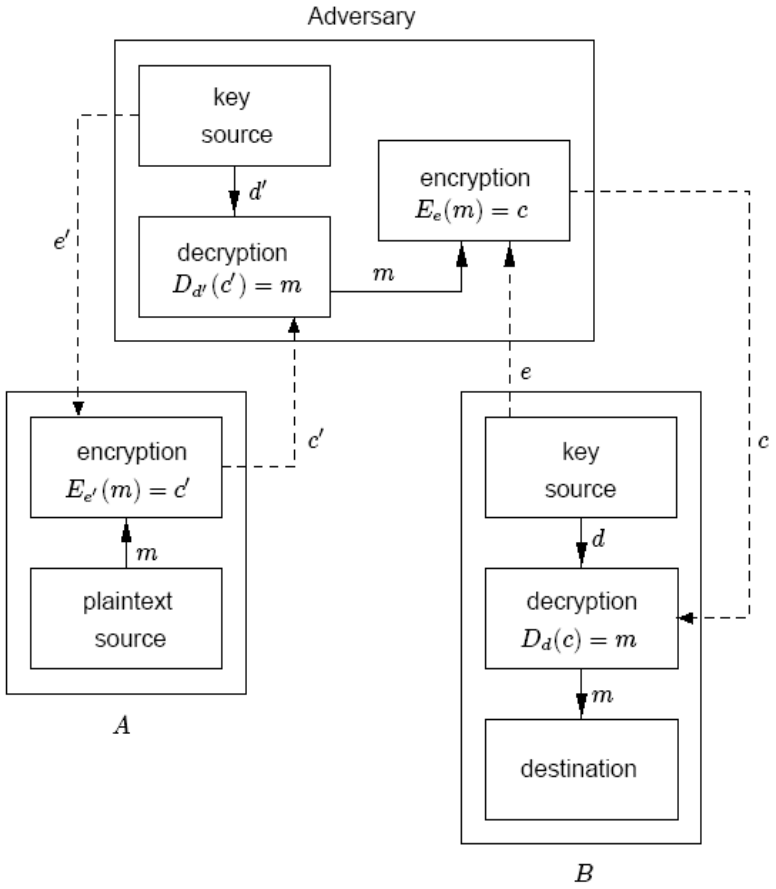
Ασύμμετρη κρυπτογραφία

- Ο επιτιθέμενος ξεγελά τον Α ότι είναι ο Β, στέλνοντας το δικό του δημόσιο κλειδί *e'*
- Ο Α κρυπτογραφεί τα μηνύματα με το *e'* κι άρα ο επιτιθέμενος μπορεί να διαβάζει τα μηνύματα από τον Α στον Β



Ασύμμετρη κρυπτογραφία

- Ο Β δεν μπορεί να αντιληφθεί την παρουσία του επιτιθέμενου, καθώς λαμβάνει κανονικά τα μηνύματα
- Ο Β, λαμβάνοντας ένα μήνυμα, δε μπορεί να ξέρει με βεβαιότητα ποιος το έστειλε

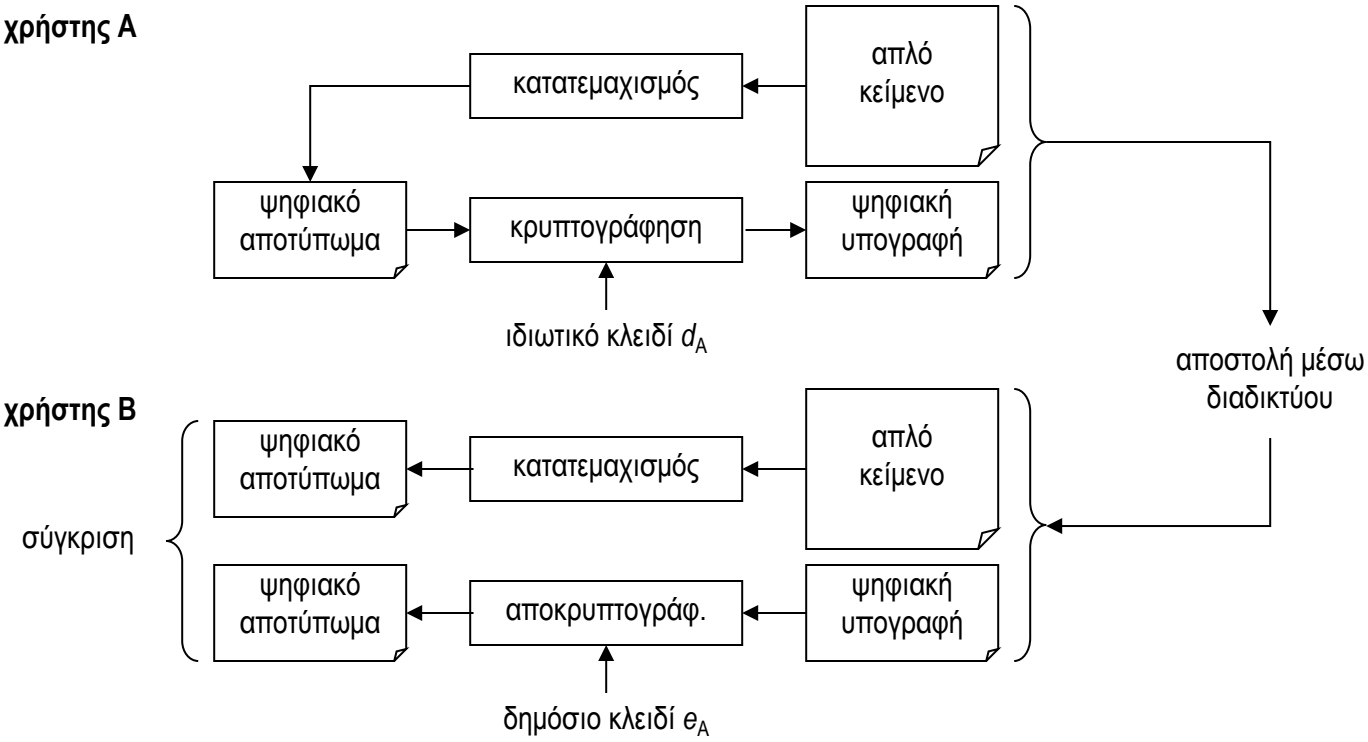


Ασύμμετρη κρυπτογραφία

- Επιθέσεις, όπως η επίθεση “ενδιαμέσου ατόμου” (man-in-the-middle), οφείλονται σε αποτυχίες πρωτοκόλλων
- Δεν αρκεί σωστή κατασκευή αλγορίθμων $\Rightarrow$ χρειάζεται σωστή υλοποίηση πρωτοκόλλων

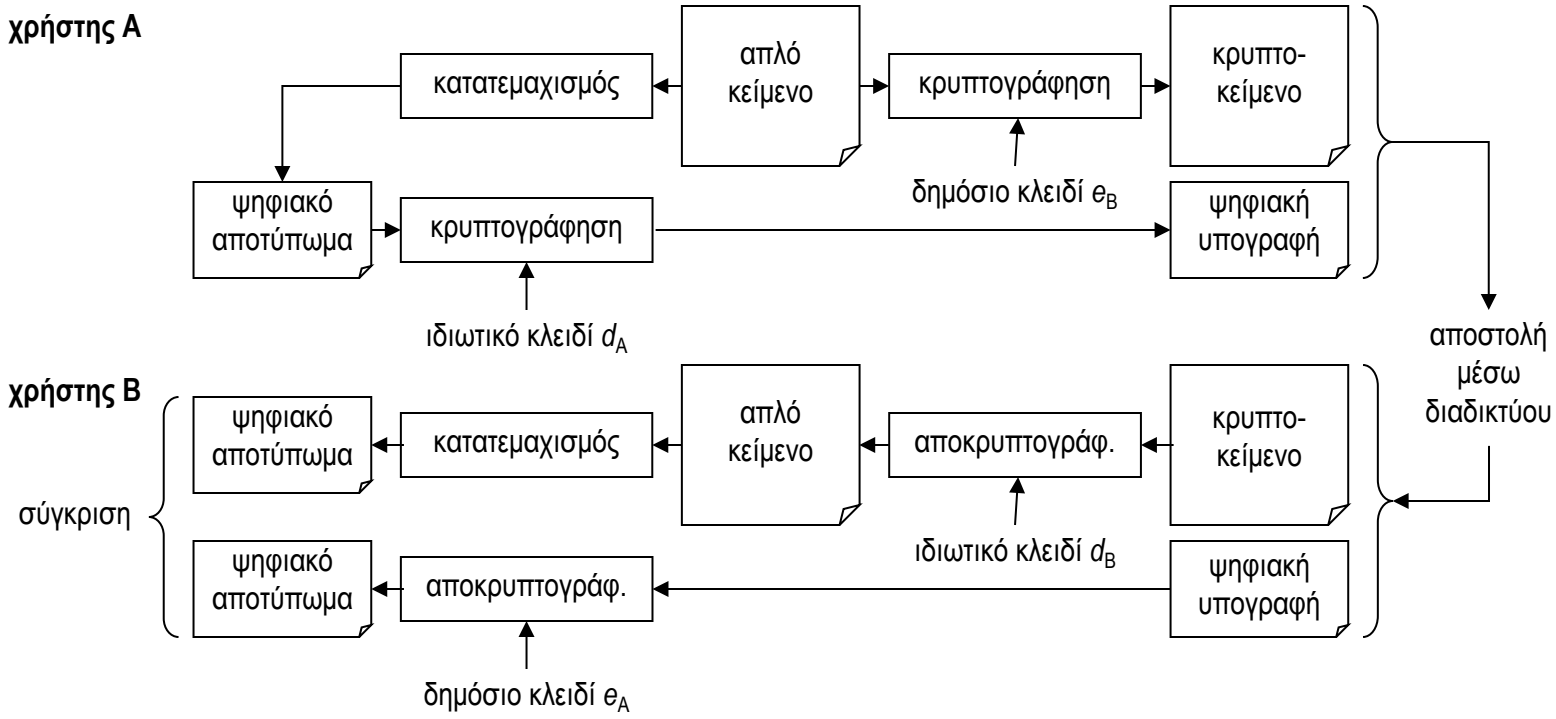
Ασύμμετρη κρυπτογραφία

- Ακεραιότητα



Ασύμμετρη κρυπτογραφία

- Ακεραιότητα, εμπιστευτικότητα

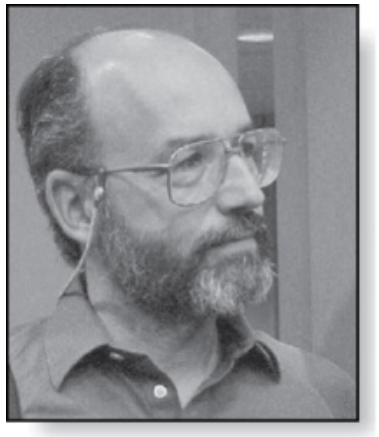


Ασύμμετρη κρυπτογραφία

- Μόνο το ιδιωτικό κλειδί πρέπει να μένει κρυφό
- Το ζεύγος δημόσιο κλειδί – ιδιωτικό κλειδί μπορεί να μένει το ίδιο για μεγάλα χρονικά διαστήματα (π.χ. για χρόνια)
- Σε ένα μεγάλο δίκτυο, ο αριθμός των κλειδιών που χρειάζονται είναι μικρότερος από ό,τι αν χρησιμοποιούνταν συμμετρική κρυπτογράφηση
- Το ζεύγος κλειδιών κρυπτογράφησης ≠ από εκείνο ψηφιακών υπογραφών

RSA: Εισαγωγή

- Πήρε το όνομά του από τους Rivest, Shamir, Adleman


- Σχεδιάστηκε το 1976? (πιο πριν... Clifford Cocks, GCHQ)
- Στηρίζεται στο δύσκολο πρόβλημα παραγοντοποίησης

RSA: Δημιουργία κλειδιού

- Επιλογή τυχαίων μεγάλων πρώτων p, q με $p \neq q$
- Υπολογισμός του $N = pq$
- Επιλογή τυχαίου e με την

  $\gcd(e, (p-1)(q-1)) = 1$

- Υπολογισμός μοναδικού d που ικανοποιεί την

  $ed = 1 \bmod (p-1)(q-1)$

- Δημόσιο κλειδί (e, N)
- Ιδιωτικό κλειδί (d, p, q)

RSA: Κρυπτογράφηση

Για την κρυπτογράφηση του μηνύματος m:

- Το m διασπάται σε μία σειρά τμημάτων $m_1, m_2, \ldots, m_p$
  - Κάθε m_i αναπαρίσταται από έναν ακέραιο μεταξύ 0 και N
- Η κρυπτογράφηση γίνεται ξεχωριστά για κάθε m_i με χρήση του δημοσίου κλειδιού (N, e)
- Παράγεται το κρυπτόγραμμα c_i ως εξής:

$$c_i = m_i^e \bmod N$$

RSA: Αποκρυπτογράφηση

- Ο Α αποκρυπτογραφεί το κρυπτόγραμμα c_i υπολογίζοντας

$$m_i = c_i^d \bmod N$$

- Η σχέση μεταξύ του d και του e εξασφαλίζει τη σωστή ανάκτηση του m_i
- Μόνο ο Α μπορεί να αποκρυπτογραφήσει το μήνυμα, αφού είναι ο μόνος που γνωρίζει το d

RSA: Security

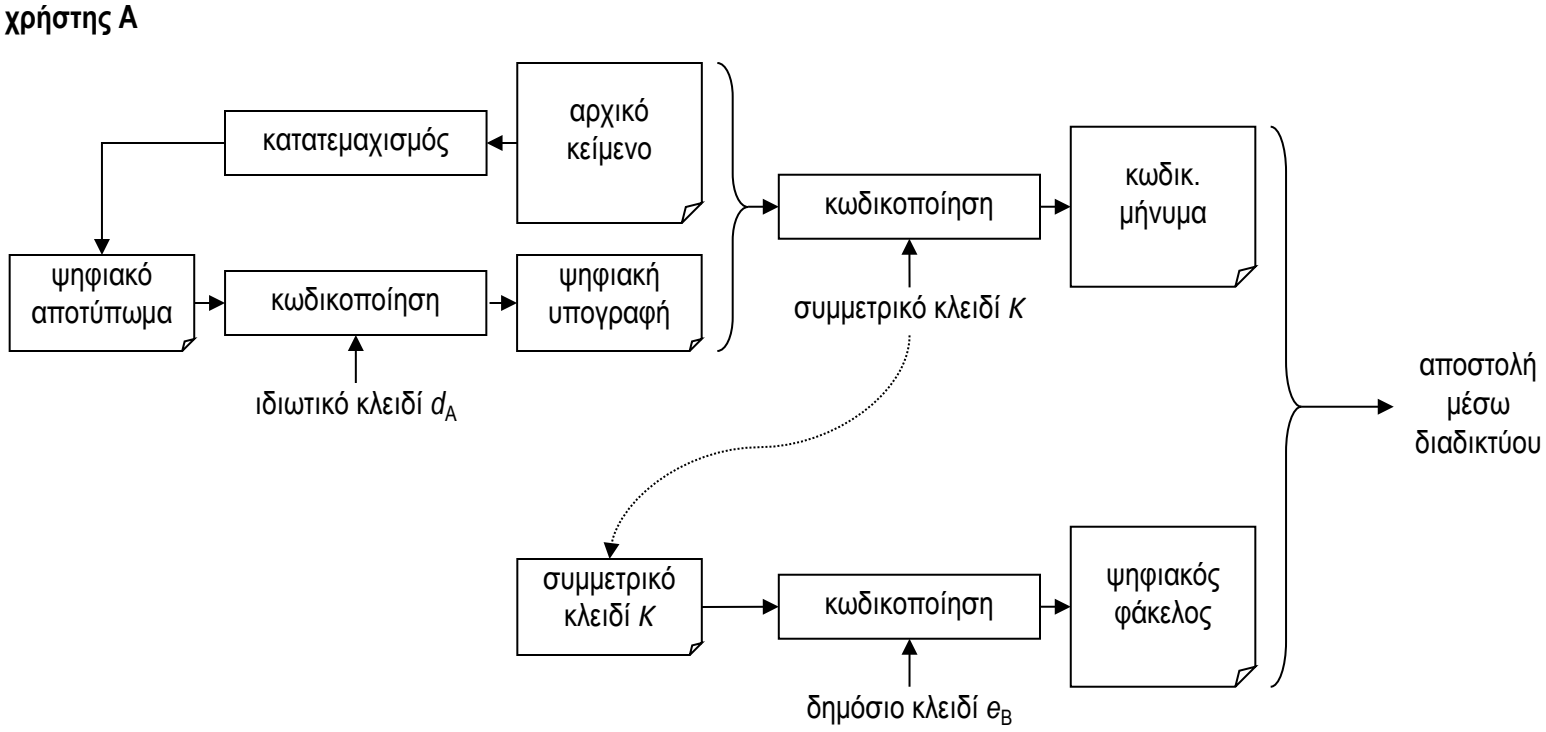
- Όσο πιο μεγάλο είναι το N, τόσο πιο μεγάλη η ασφάλεια
  - Από την άλλη, ο RSA γίνεται πιο αργός
- Τα p, q πρέπει να έχουν μεγάλη διαφορά μεταξύ τους:
  - Αν η διαφορά *p* - *q* είναι μικρή, τότε p $\approx \sqrt{N}$
  - Έτσι ο *p* (άρα και ο *q*) μπορούν να υπολογιστούν με δοκιμές
- Τρέχουσα κατάσταση:
  - Ο 512-bit RSA έσπασε μέσα σε 7 μήνες το 1999
  - Το RSA laboratory προτείνει σαν μέγεθος κλειδιού τουλάχιστον 1024 bits (ικανοποιητικό μέγεθος 2048 bits)

Συνδυασμός μεθοδολογιών

- Όχι ανταγωνιστικά – χρησιμοποιούνται μαζί
- Το δημόσιο κλειδί διαμοιράζεται εύκολα, αλλά μπορεί να χρησιμοποιηθεί μόνο σε μικρά μηνύματα
- Το συμμετρικό κλειδί διανέμεται δύσκολα (πρόβλημα εύρεσης ασφαλούς «καναλιού» μετάδοσής του), αλλά μπορεί να χρησιμοποιηθεί και σε μεγάλα μηνύματα
- Έχουν συμπληρωματικά προτερήματα και ελαττώματα

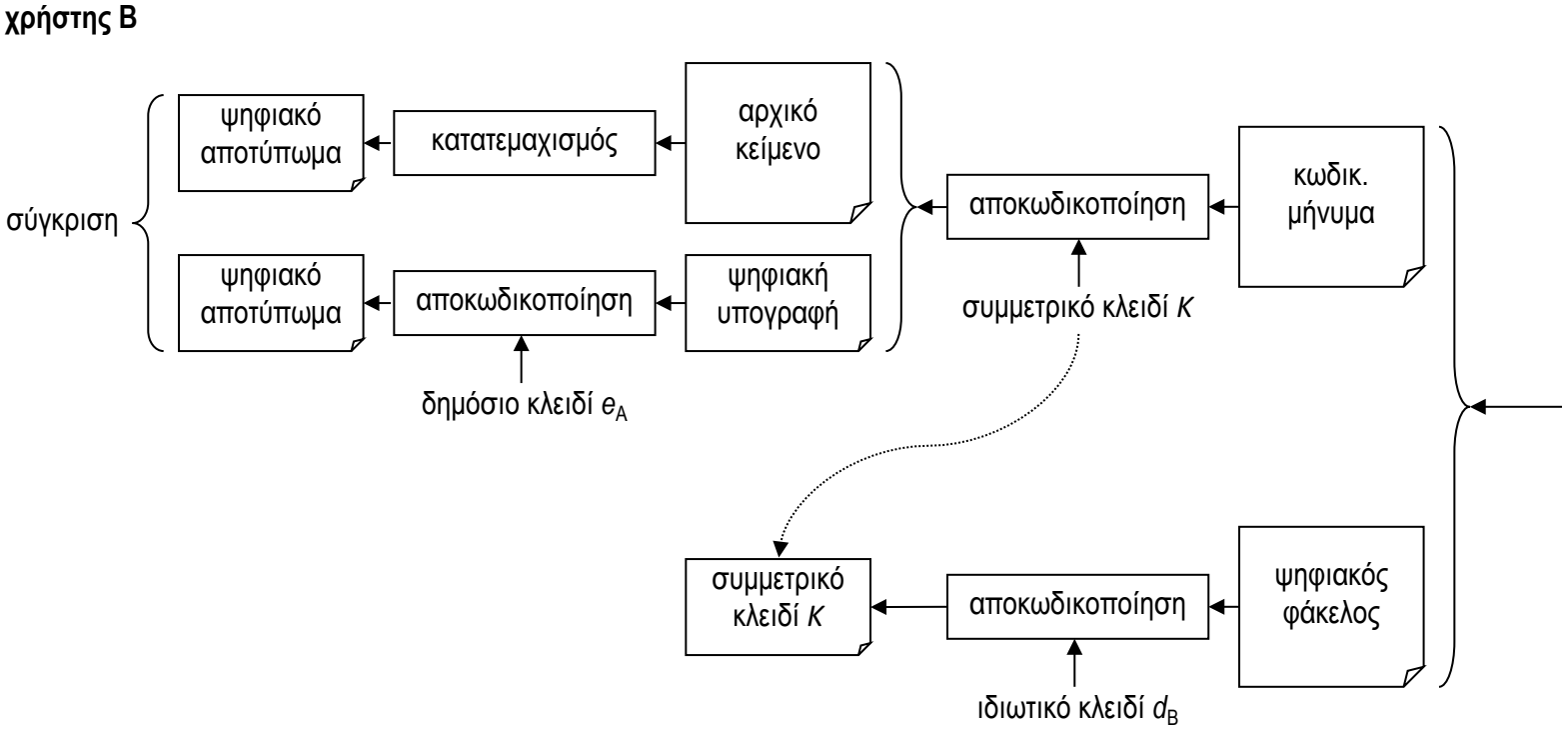
Συνδυασμός μεθοδολογιών

- Ακεραιότητα, εμπιστευτικότητα



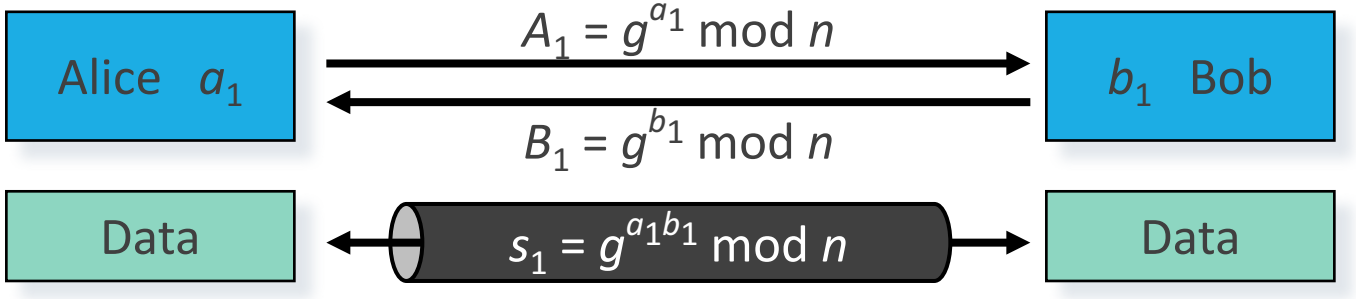
Συνδυασμός μεθοδολογιών

- Ακεραιότητα, εμπιστευτικότητα

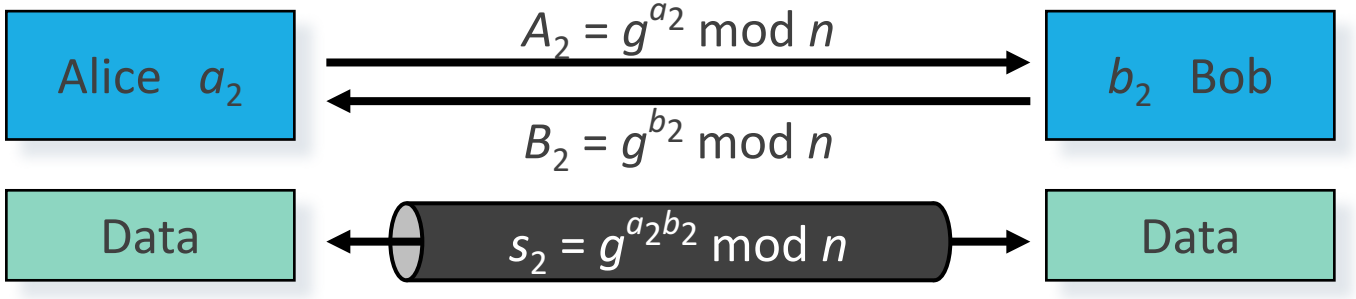


Ανταλλαγή κλειδιών με DH

Session 1:



Session 2:



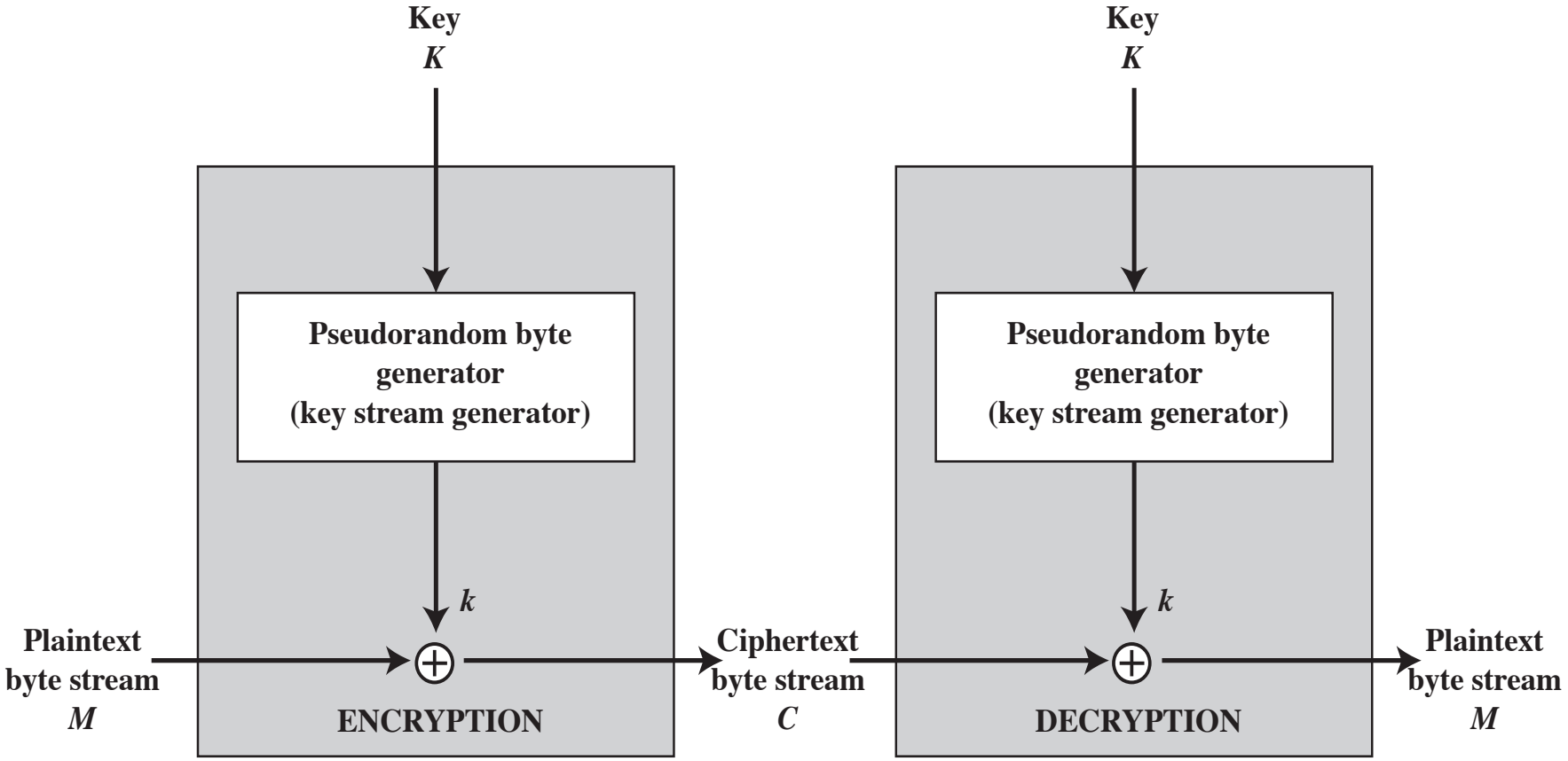
If key s_1 gets compromised, then key s_2 is still totally secure (assuming that a_1, b_1, a_2 and b_2 are truly random)

Ανταλλαγή κλειδιών με DH

Κατηγοριοποίηση: λειτουργία

- Κρυπτοσυστήματα ροής (stream ciphers)
  - Λειτουργούν σε ένα σύμβολο τη φορά
  - Κλειδοροή είναι περιοδική ακολουθία (με μεγάλη περίοδο)
  - Κλειδί = αρχή της περιόδου
  - Το ίδιο σύμβολο κωδικοποιείται διαφορετικά
- Κρυπτοσυστήματα τμήματος (block ciphers)
  - Λειτουργούν σε ένα τμήμα συμβόλων τη φορά
  - Το ίδιο τμήμα συμβόλων κωδικοποιείται όμοια

Κρυπτοσυστήματα ροής



Κρυπτοσυστήματα ροής

- Αποστολέας/παραλήπτης πρέπει να είναι συγχρονισμένοι
  - Αν τμήμα του κρυπτογράμματος χαθεί κατά τη μετάδοση χάνεται ο συγχρονισμός και απαιτούνται τεχνικές επανασυγχρονισμού
- Η παραποίηση ενός ψηφίου του κρυπτογράμματος κατά τη μετάδοση δεν έχει ως αποτέλεσμα περαιτέρω λανθασμένη αποκρυπτογράφηση επόμενων ψηφίων
- “Ενεργές επιθέσεις” προκαλούν σοβαρά προβλήματα (π.χ. έλλειψη συγχρονισμού)
  - Απαιτούνται τεχνικές για πιστοποίηση της γνησιότητας και της ακεραιότητας του μηνύματος

Κρυπτοσυστήματα ροής

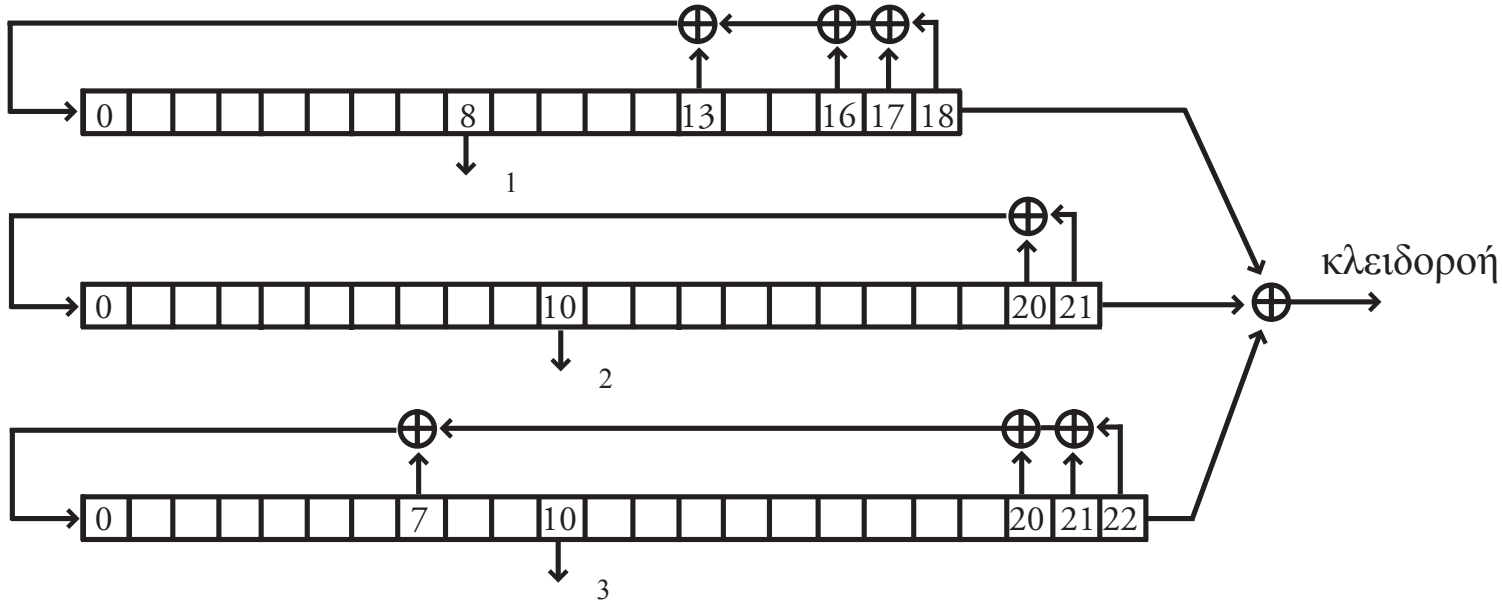
- Το throughput είναι μπορεί σημαντικά μεγαλύτερο, συγκριτικά με τους καλύτερους block ciphers.
- Το μήκος των κλειδιών είναι πιο μεγάλο, ως προς τους block ciphers
- Κανένας αλγόριθμος δεν έχει αποδειχτεί ασφαλής (αν και το ίδιο ισχύει και στους block ciphers)
  - Όλοι στηρίζονται σε γνωστά προβλήματα της θεωρίας πολυπλοκότητας & υπολογισμού

Κρυπτοσυστήματα ροής

- RC4
  - Σε προϊόντα της Oracle
- A5/1
  - Σε κινητές επικοινωνίες GSM
- E0
  - Στο πρωτόκολλο Bluetooth

Κρυπταλγόριθμοι ροής: A5/1

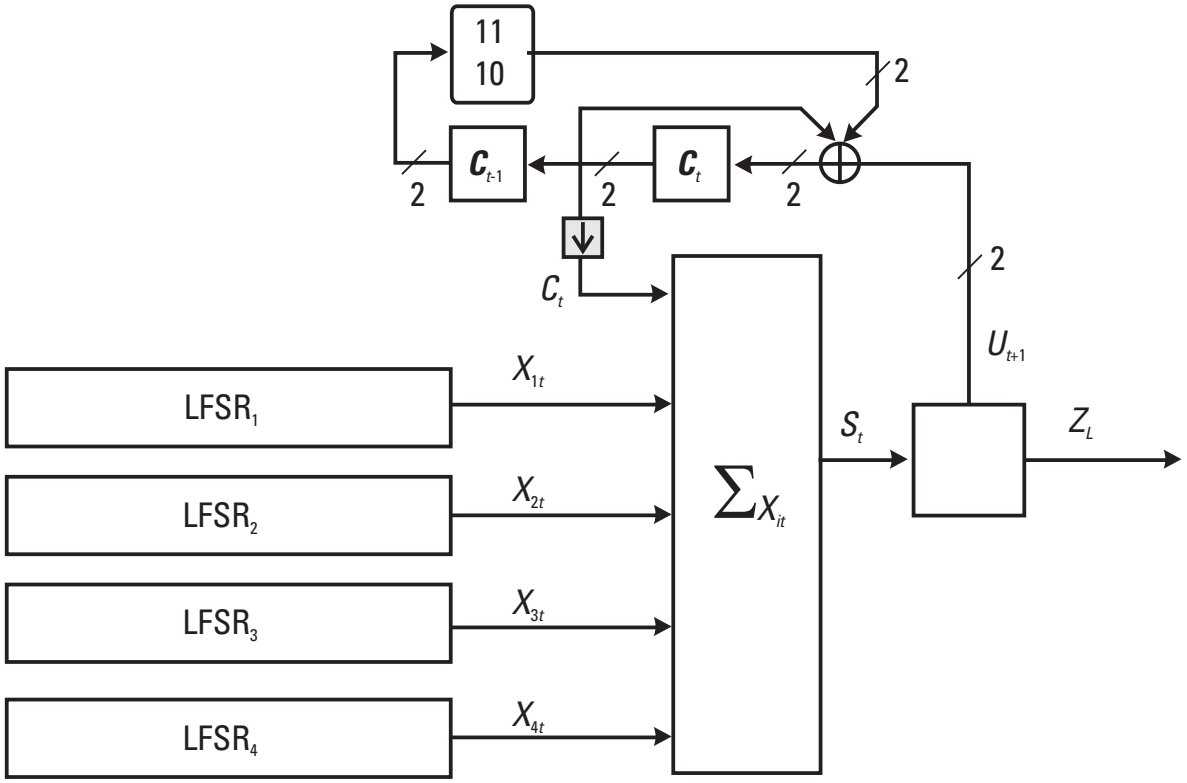
- Χρησιμοποιείται στο GSM



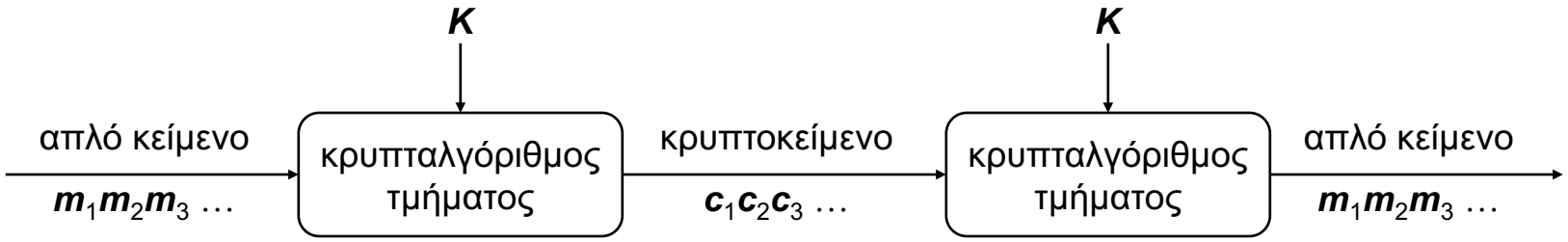
- Οι θέσεις 1,2,3 καθορίζουν τους ενεργούς καταχωρητές σε κάθε χρονική στιγμή

Κρυπταλγόριθμοι ροής: E0

- Χρησιμοποιείται στο Bluetooth

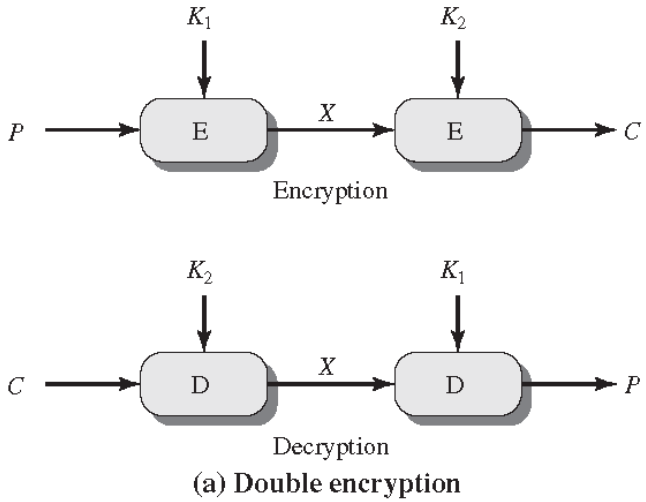


Κρυπτοσυστήματα τμήματος



Επαναλαμβανόμενη κρυπτογράφηση: π.χ. 2DES

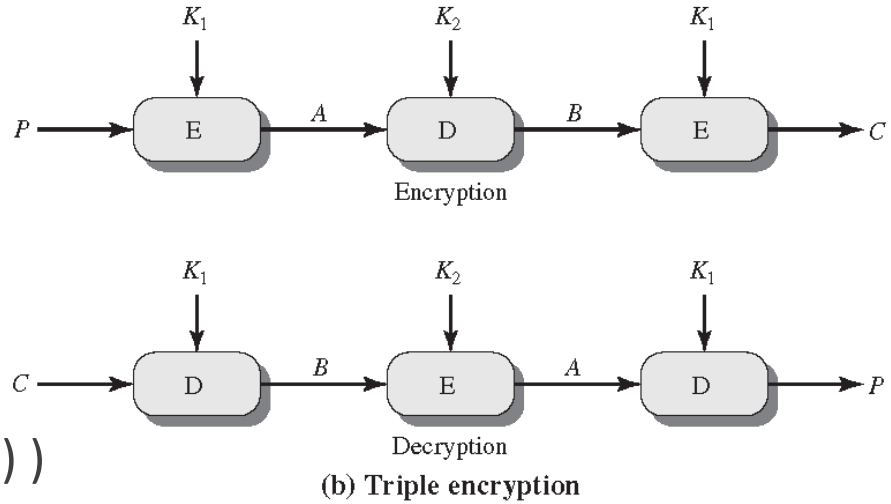
- Παραλλαγή του DES
- Παρέχει περισσότερη ασφάλεια
- Ο 2DES χρησιμοποιεί δυο 56-bit κλειδιά
  - $c = Enc_{k2}(Enc_{k1}(m))$
  - $m = Dec_{k1}(Dec_{k2}(c))$



(a) Double encryption

Επαναλαμβανόμενη κρυπτογράφηση: π.χ. 3DES

- Παραλλαγή του DES
- Παρέχει περισσότερη ασφάλεια
- Ο 3DES χρησιμοποιεί τρία 56-bit κλειδιά
  - $c = Enc_{k3}(Dec_{k2}(Enc_{k1}(m)))$
  - $m = Dec_{k1}(Enc_{k2}(Dec_{k3}(c)))$
- Εαν $K_1=K_2 \Rightarrow$ 3DES = DES



(b) Triple encryption

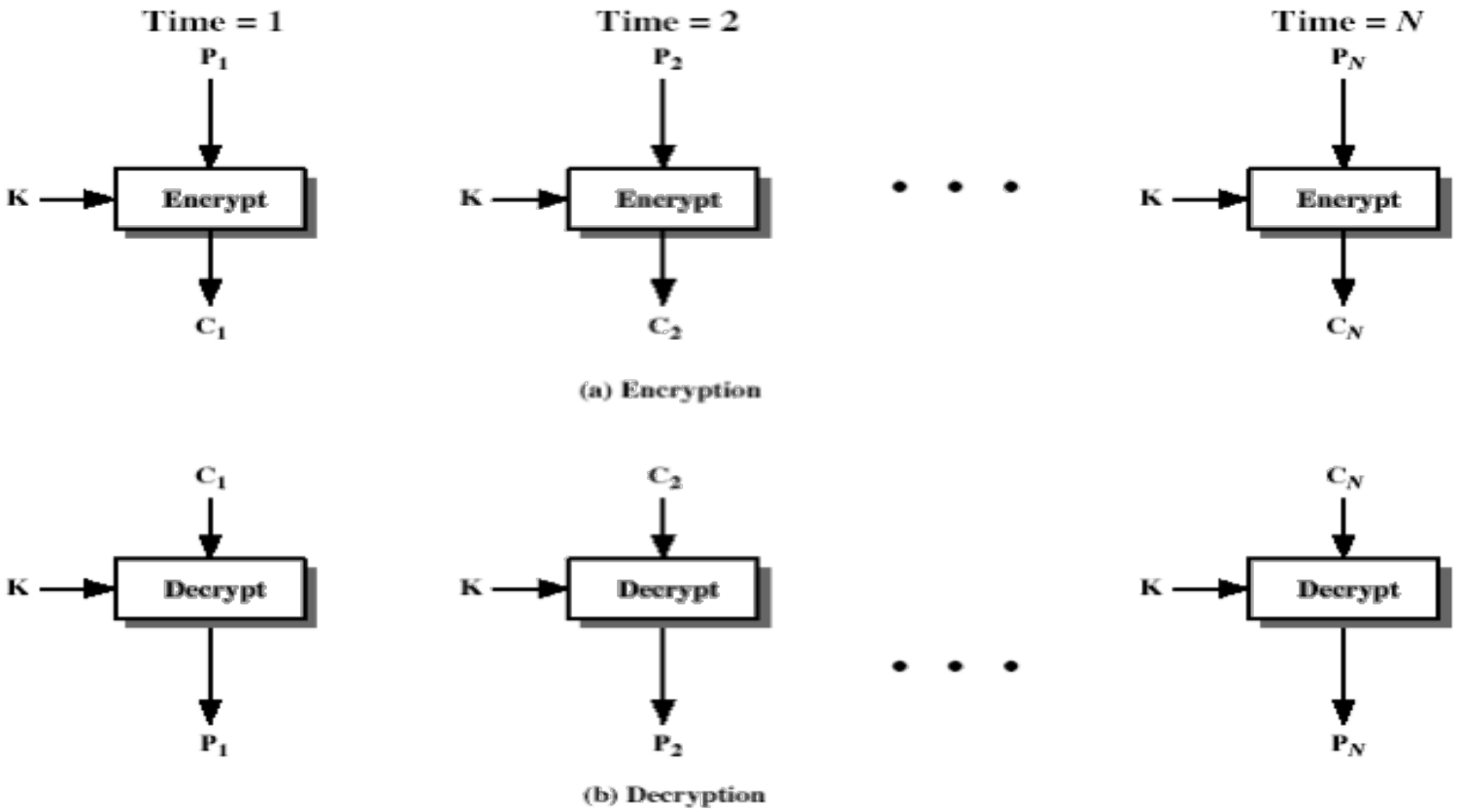
Ρυθμοί λειτουργίας

- Οι κρυπταλγόριθμοι τμήματος μπορούν να λειτουργήσουν με διάφορους τρόπους
- Οι ρυθμοί έχουν διαφορετικά χαρακτηριστικά, όπως:
  - ασφάλεια
  - διάχυση σφαλμάτων
  - αποδοτικότητα
- Οι ρυθμοί ECB, CBC, CFB, και OFB ορίζονται σε πρότυπα FIPS του NIST και ANSI
  - ANSI X3.106-1983 Modes of Use

Ρυθμοί λειτουργίας

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of plaintext bits is encoded independently using the same key.	• Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next block of plaintext and the preceding block of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission • Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.	• Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General-purpose block-oriented transmission • Useful for high-speed requirements

Ρυθμοί λειτουργίας: ECB



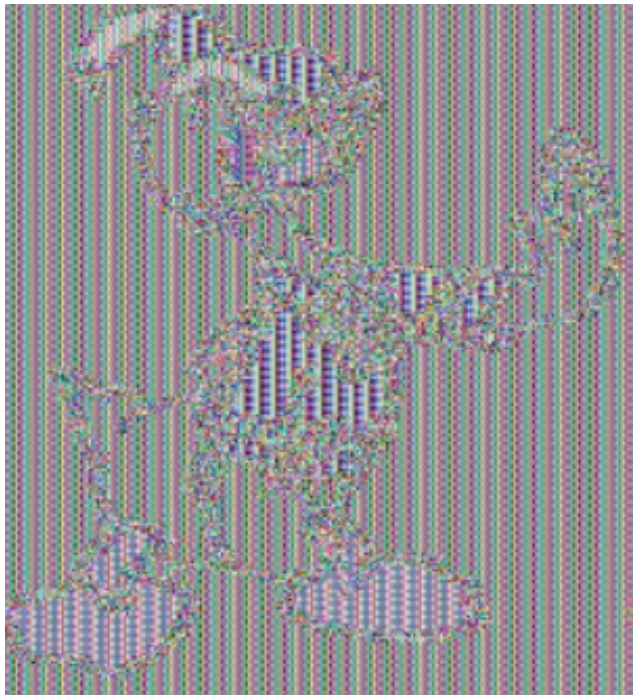
Ρυθμοί λειτουργίας: ECB

- Ξεχωριστή κρυπτογράφηση κάθε τμήματος
  - Τα ίδια δεδομένα κρυπτογραφούνται με τον ίδιο τρόπο
- Μοτίβα στην είσοδο θα εμφανίζονται και στην έξοδο
  - Αντίγραφα αρχείων, κ.λπ., αναγνωρίζονται
- Είναι δυνατή η κατασκευή κωδικοβιβλίου (codebook)
- Μπορούμε να αντικαταστήσουμε ενδιάμεσα δεδομένα
  - Δεν υπάρχει συσχέτιση μεταξύ τμημάτων
- Δεν απαιτείται διάνυσμα αρχικοποίησης (IV)

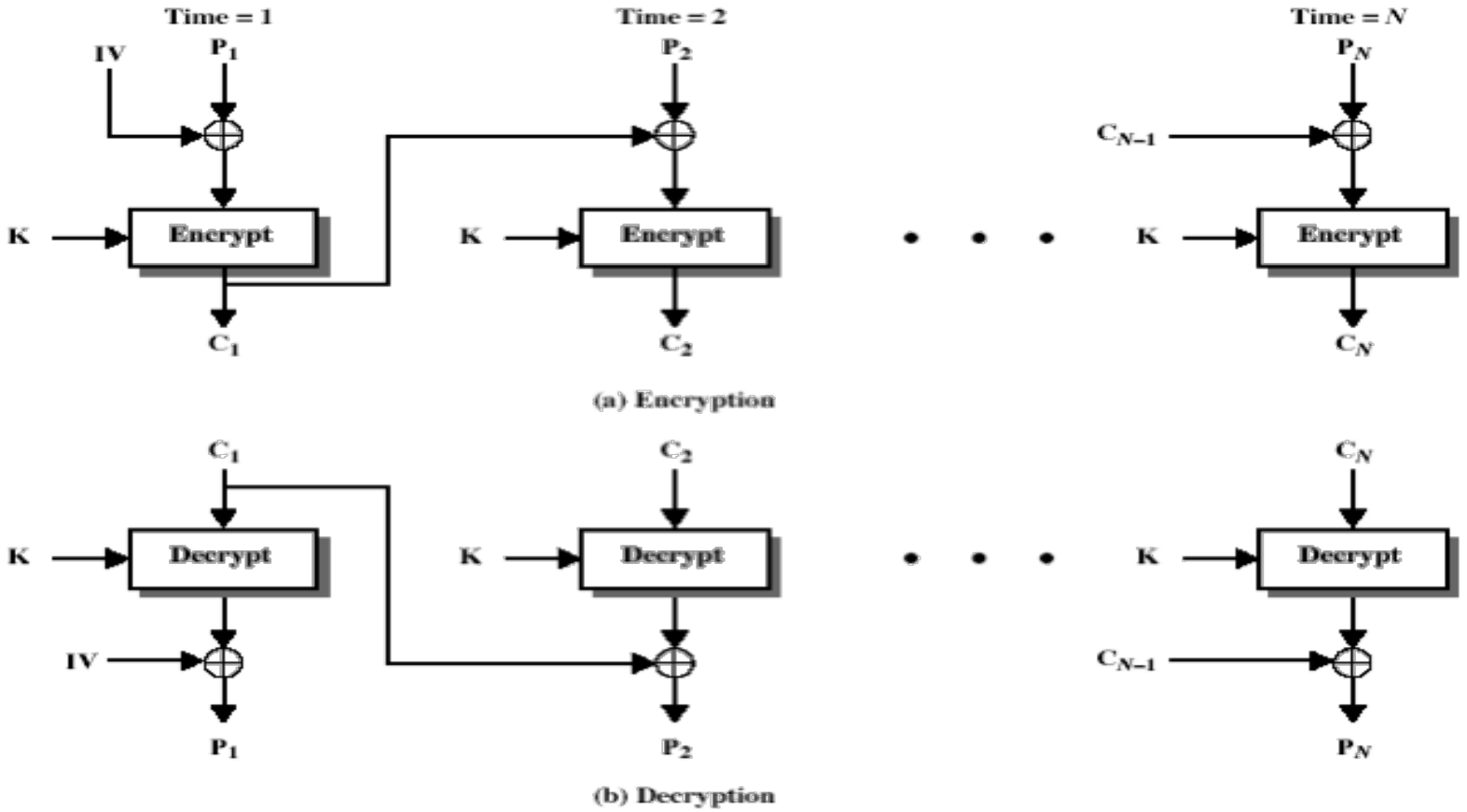
Ρυθμοί λειτουργίας: ECB

ΑΡΧΙΚΗ ΕΙΚΟΝΑ

ΜΕ ΧΡΗΣΗ AES



Ρυθμοί λειτουργίας: CBC



Ρυθμοί λειτουργίας: CBC

- Προσθέτει δυαδικά το απλό κείμενο με το προηγούμενο κρυπτοκείμενο, και μετά κρυπτογραφεί το αποτέλεσμα
- Απαιτείται διάνυσμα αρχικοποίησης (IV) για το πρώτο τμήμα
  - however if IV is sent in the clear, an attacker can change bits of the first block, and change IV to compensate
  - hence either IV must be a fixed value or it must be sent encrypted in ECB mode before rest of message

Ρυθμοί λειτουργίας: CBC

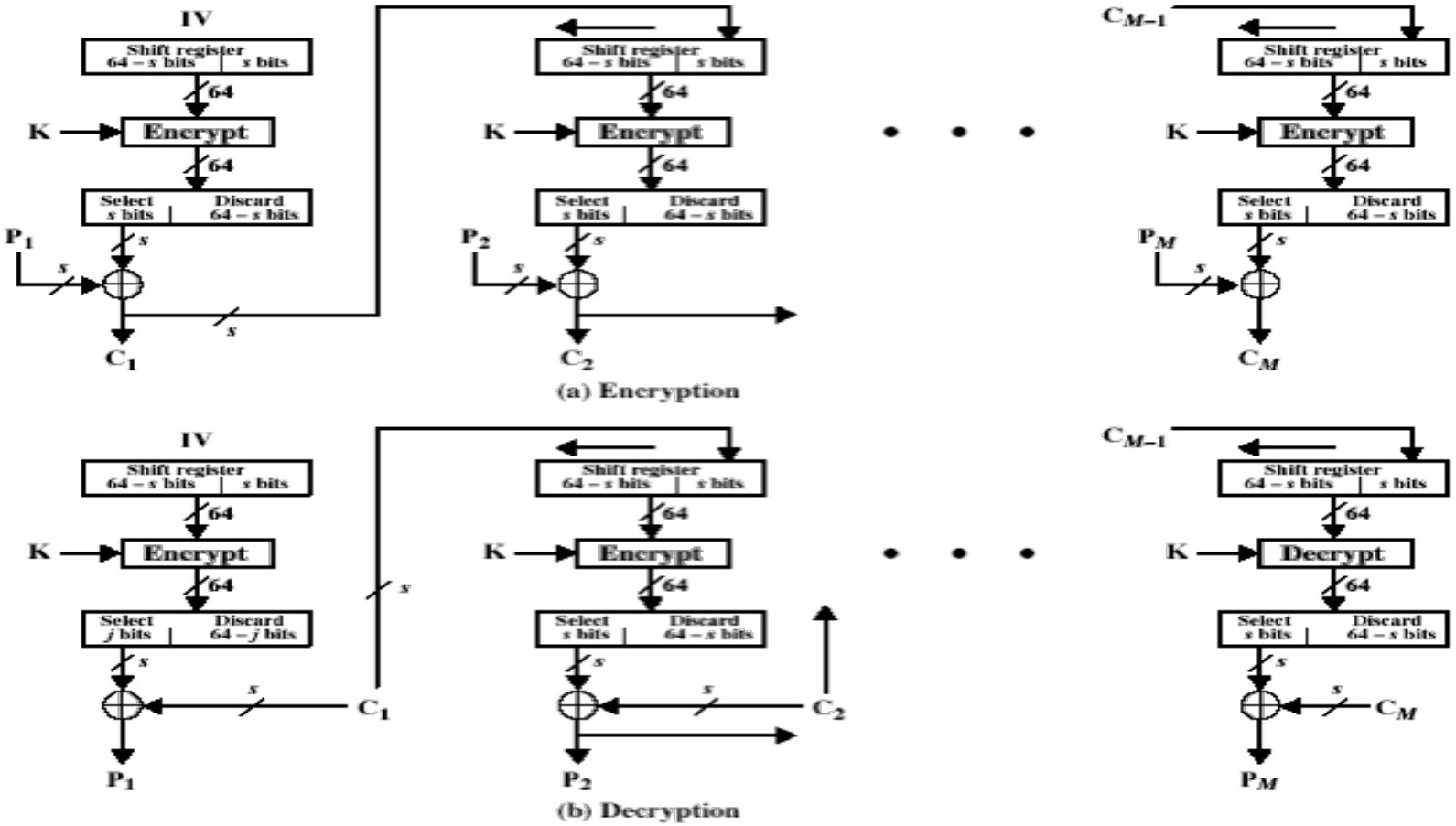
- Ίδια δεδομένα οδηγούν σε διαφορετικά αποτελέσματα
- Η έξοδος εξαρτάται από όλες τις προηγούμενες εισόδους
  - Μπορεί να χρησιμοποιηθεί ως MAC
- Λάθη σε λαμβανόμενο τμήμα διορθώνεται μετά από 2 τμήματα (self-correction)
  - $c_i = \text{Enc}_K(m_i \oplus c_{i-1}) \Rightarrow m_i = \text{Dec}_K(c_i) \oplus c_{i-1}$
  - Επηρεάζονται τα m_i (c_i αρχ. λάθος) και m_{i+1}

Ρυθμοί λειτουργίας: CBC

ΑΡΧΙΚΗ ΕΙΚΟΝΑ

ΜΕ ΧΡΗΣΗ AES

Ρυθμοί λειτουργίας: CFB



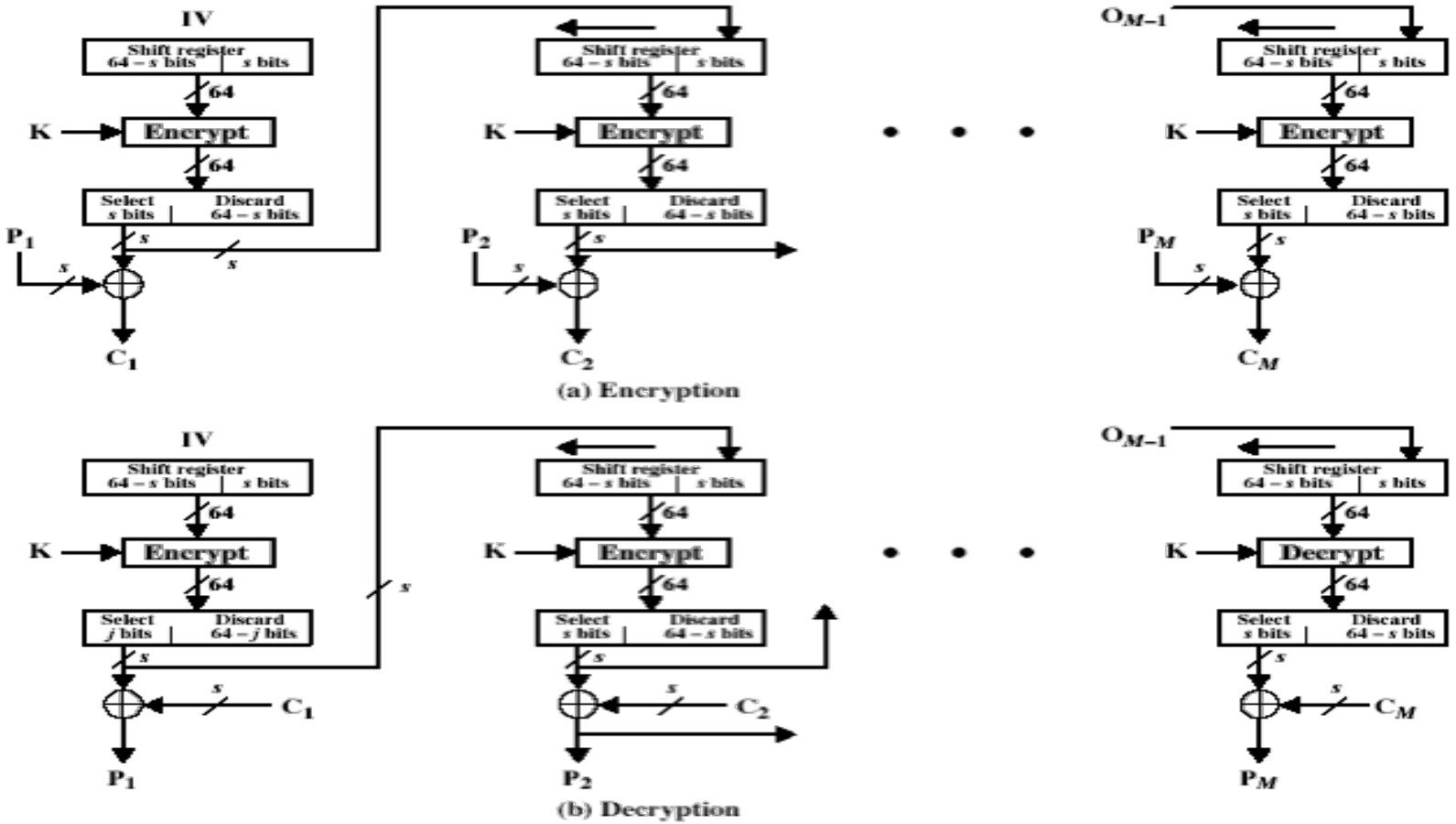
Ρυθμοί λειτουργίας: CFB

- Το προηγούμενο κρυπτοκείμενο κρυπτογραφείται, και το αποτέλεσμα προστίθεται δυαδικά με το απλό κείμενο
- Δεν είναι αναγκαία η τροφοδοσία όλου του τμήματος
  - Μπορεί να γίνει σε μέρη, π.χ. telnet
- Έχει επίσης την ιδιότητα της αυτοδιόρθωσης
- Πολλές ιδιότητες μοιάζουν με αυτές του CBC
- Λιγότερο αποδοτικός

Ρυθμοί λειτουργίας: CFB

- Standard allows any number of bit (1,8 or 64 or whatever) to be feed back
  - Denoted CFB-1, CFB-8, CFB-64 etc
- Is most efficient to use all 64 bits (CFB-64)

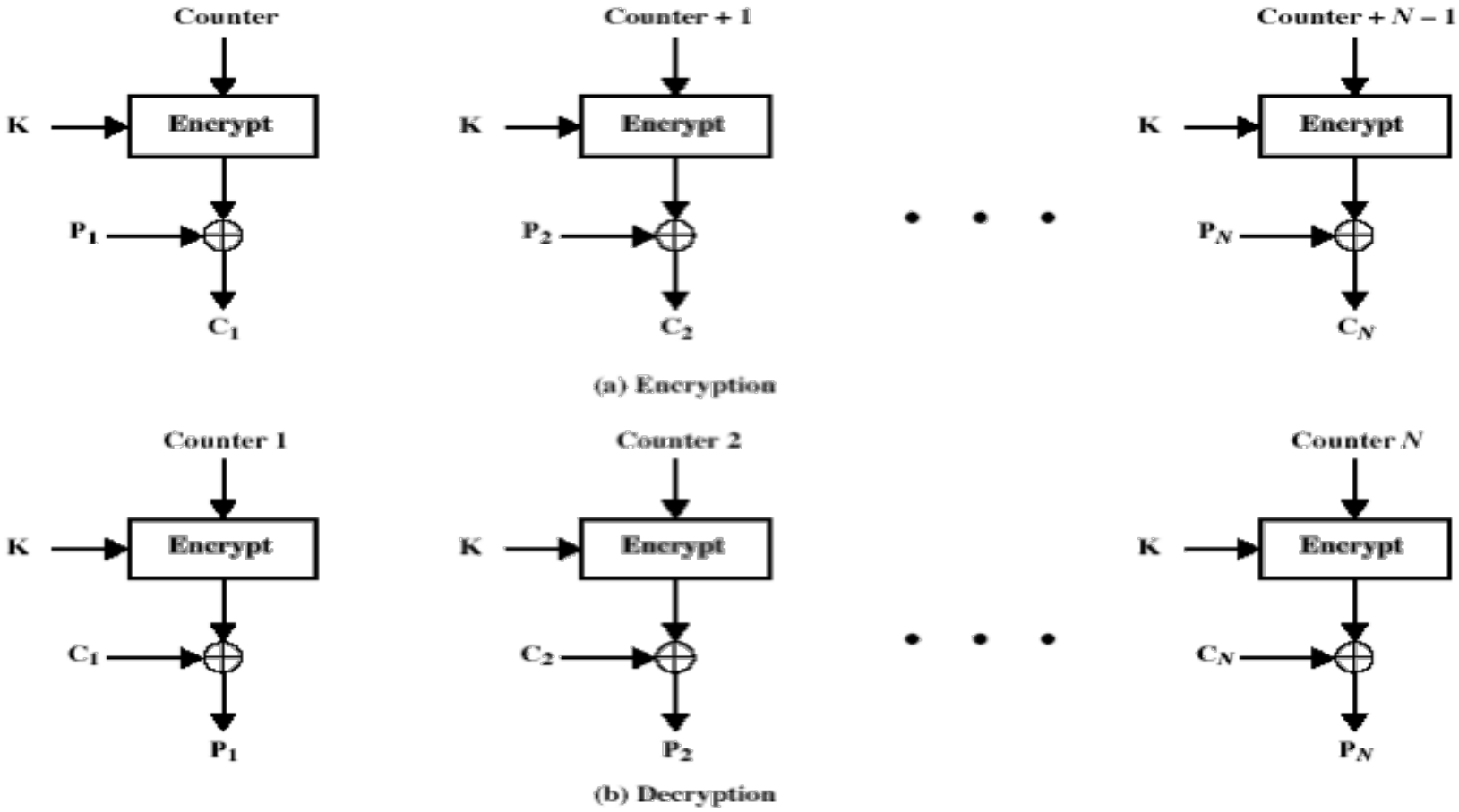
Ρυθμοί λειτουργίας: OFB



Ρυθμοί λειτουργίας: OFB

- Είναι αποδοτικός τρόπος για να μετατρέψουμε έναν κρυπταλγόριθμο τμήματος σε ροής
- Κρυπτογράφηση του IV και μετά δυαδική πρόσθεση με το απλό κείμενο για να πάρουμε το κρυπτοκείμενο
- Used when there is a need for encryptions are available before the message

Ρυθμοί λειτουργίας: CTR



Ρυθμοί λειτουργίας: CTR

- Είναι αποδοτικός τρόπος για να μετατρέψουμε έναν κρυπταλγόριθμο τμήματος σε ροής
- Σε κάθε βήμα ο μετρητής κρυπτογραφείται και μετά προστίθεται δυαδικά με το απλό κείμενο
  - Αρχίζουμε από κάποιο σημείο και αυξάνουμε συνεχώς
- Must have a different key and counter value for every plaintext block (never reused)
- Provable security (good as other modes)
- Uses: high-speed network encryptions

One-way hash functions

- Accepts a variable-size message *M* as input and produces a fixed-size message digest H(*M*) as output
- Does not take a secret key as input
- To authenticate a message, the message digest is sent with the message in such a way that the message digest is authentic

OWHF: Security

1. H can be applied to a block of data of any size.
2. H produces a fixed-length output.
3. H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.

OWHF: Security

4

- $H^{-1}(h)$ is computationally infeasible to find for any given h; such a hash function is called *one-way* or *preimage resistant*.

5

- For any given x, it is computationally infeasible to find y with H(y) = H(x); such a hash function is called *second preimage resistant* or *weak collision resistant*.

6

- It is computationally infeasible to find any pair (x, y) with H(x) = H(y); such a hash function is called *collision resistant* or *strong collision resistant*.

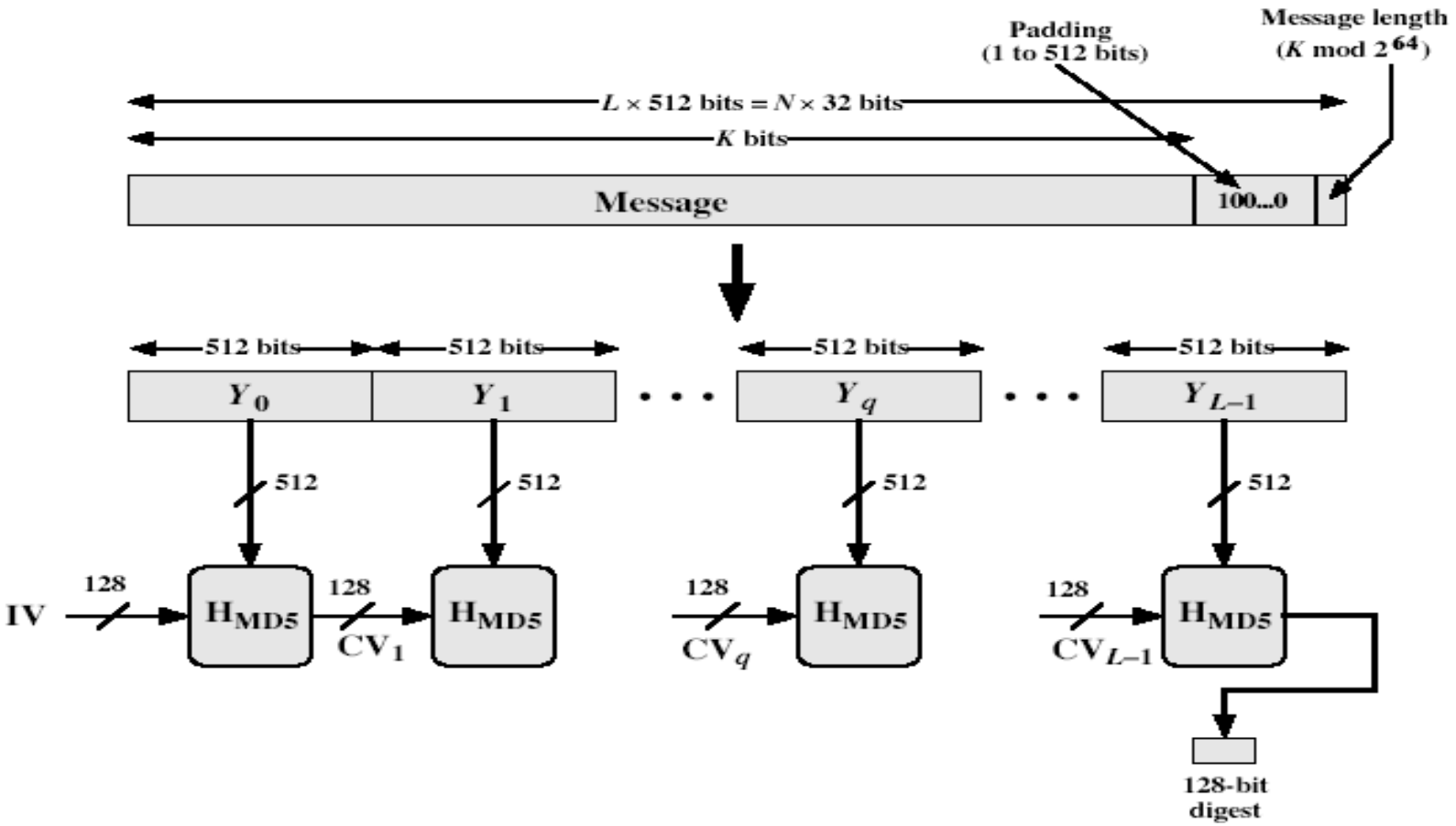
OWHF: Overview

	MD5	RIPEMD-160	SHA-1
Μήκος σύνοψης	128 bits	160 bits	160 bits
Μήκος μηνύματος	απεριόριστο	απεριόριστο	$< 2^{64}$ bits
Βασική μονάδα επεξεργασίας	512 bits	512 bits	512 bits
Μέγεθος λέξης	32	32	32
Πλήθος βημάτων	64	160	80

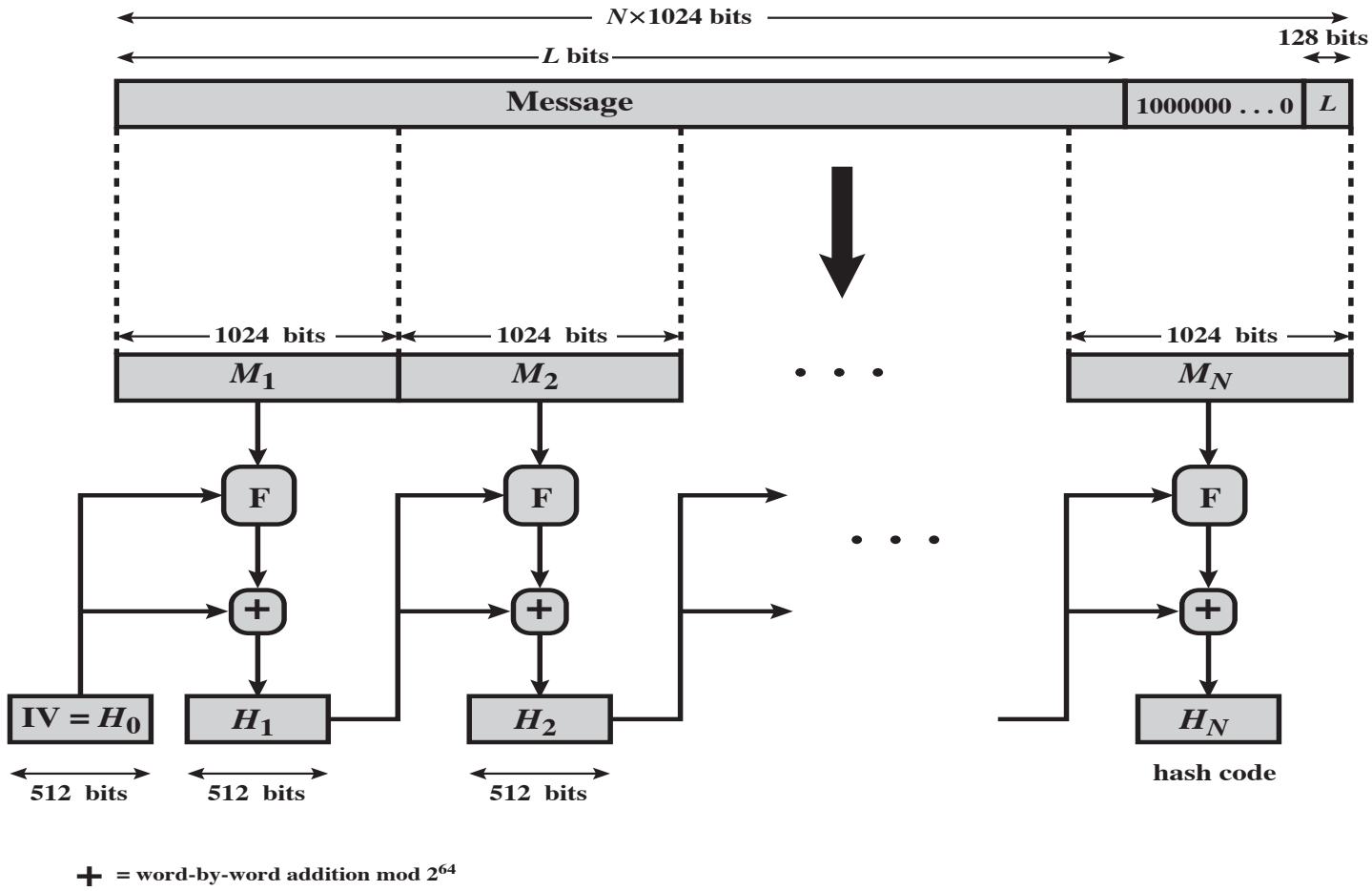
OWHF: Overview

	SHA-224	SHA-256	SHA-384	SHA-512
Μήκος σύνοψης	224 bits	256 bits	384 bits	512 bits
Μήκος μηνύματος	$< 2^{64}$ bits	$< 2^{64}$ bits	$< 2^{128}$ bits	$< 2^{128}$ bits
Βασική μονάδα επεξεργασίας	512 bits	512 bits	1024 bits	1024 bits
Μέγεθος λέξης	32	32	64	64
Πλήθος βημάτων	64	64	80	80

MD5 overview



SHA-512 overview



OWHF: Attacks

There are two approaches to attack a secure hash function:

- Cryptanalysis
  - Involves exploiting logical weaknesses in the algorithm
- Brute-force attack
  - The strength of a hash function against this attack depends solely on the length of the hash code produced by the algorithm

Προτεινόμενη βιβλιογραφία

- W. Stallings
  Cryptography and Network Security: Principles & Practice
  7th Ed., Prentice Hall, 2017
- A. Menezes, P. van Oorschot, and S. Vanstone
  Handbook of Applied Cryptography
  CRC Press, 1997
- B. Schneier
  Applied Cryptography: Protocols, Algorithms, and Source Code in C
  2nd Ed., Wiley & Sons, 1996