Ασφάλεια Υπολογιστικών Συστημάτων

7ο Εξάμηνο

Κρυπτογραφία: Συμμετρική Κρυπτογράφηση

Διδάσκων : Δρ. Παρασκευάς Κίτσος

https://ecsalab.ece.uop.gr/

Καθηγητής

Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και Εφαρμογών (ECSA Lab.)

e-mail: kitsos@uop.gr

ΛΙΓΟ ΕΚΠΑΙΔΕΥΤΙΚΗ ΤΗΛΕΟΡΑΣΗ

- Amazing mind reader reveals his 'gift'

ΔΙΑΡΘΡΩΣΗ ΕΝΟΤΗΤΑΣ

1. Βασικοί ορισμοί
2. Αρχές Συμμετρικής Κρυπτογράφησης
3. Συμμετρικοί Αλγόριθμοι (Symmetric Ciphers)
    1. DES, Triple-DES
    2. AES
4. Αλγόριθμοι Τμημάτων (Block Ciphers): Τρόποι Λειτουργίας

ΒΑΣΙΚΟΙ ΟΡΙΣΜΟΙ

- ***Απλό κείμενο*** (***plaintext***) ονομάζεται η αρχική μορφή ενός κειμένου ενώ το κρυπτογραφημένο κείμενο ονομάζεται ***κρυπτοκείμενο*** (***ciphertext***) ή ***κρυπτογράφημα***.
- Ο μετασχηματισμός του απλού κειμένου σε κρυπτοκείμενο ονομάζεται ***κρυπτογράφηση*** (***encryption***) ενώ ο μετασχηματισμός του κρυπτοκειμένου σε απλό κείμενο ονομάζεται ***αποκρυπτογράφηση*** (***decryption***).
- Οι μαθηματικές συναρτήσεις που υλοποιούν τους παραπάνω μετασχηματισμούς ονομάζονται ***αλγόριθμοι κρυπτογράφησης*** και ***αποκρυπτογράφησης*** αντίστοιχα.
- Το ***κλειδί*** (***key***) αποτελεί επιπλέον πληροφορία και χρησιμοποιείται κατά στους παραπάνω μετασχηματισμούς

ΑΣΦΑΛΕΣ ΣΥΣΤΗΜΑ

Ένα κρυπτοσύστημα θεωρείται ασφαλές όταν :

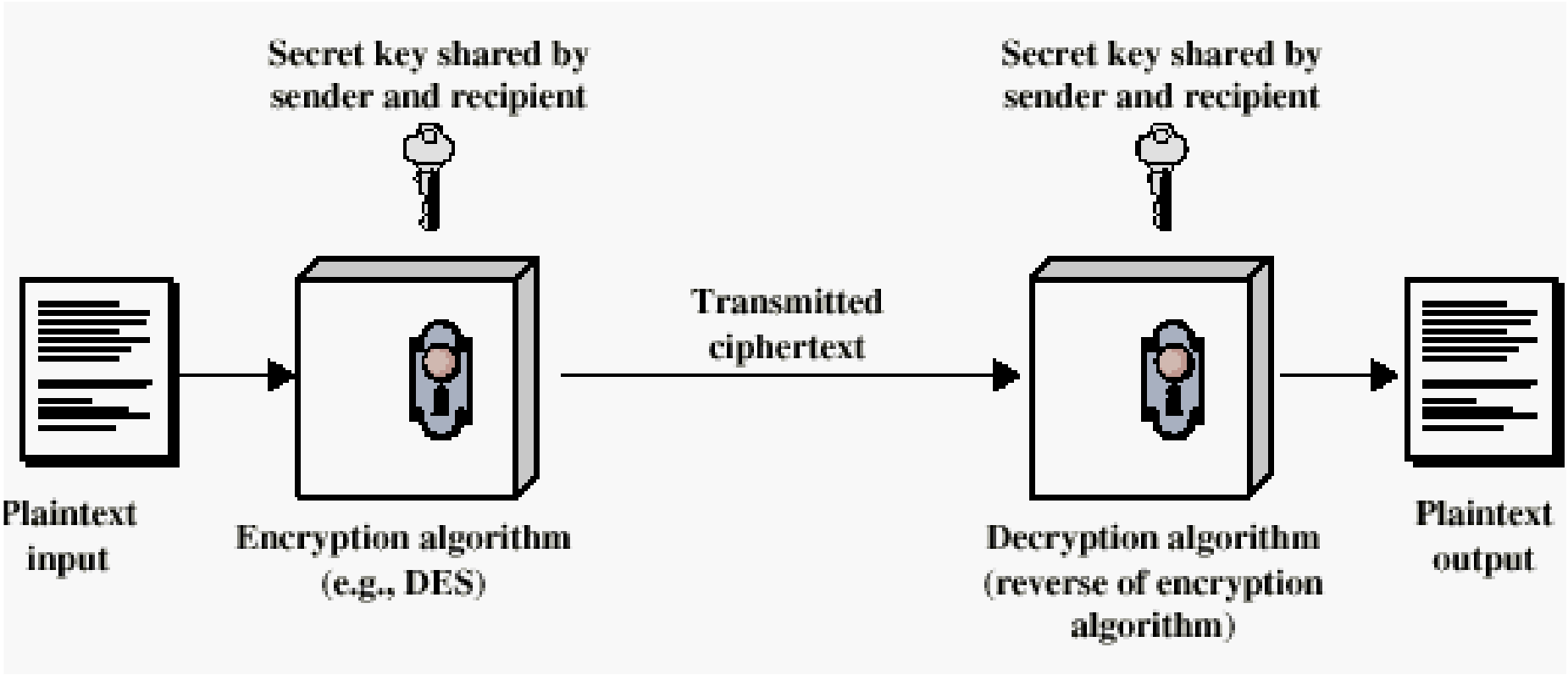
1. Το κόστος για να παραβιαστεί το κρυπτογραφημένο κείμενο, ξεπερνά την αξία των κρυπτογραφημένων δεδομένων
2. Το χρονικό διάστημα που απαιτείται για να αποκρυπτογραφηθεί η εφαρμοζόμενη διαδικασία της κρυπτογράφησης, ξεπερνά την ωφέλιμη διάρκεια ζωής της πληροφορίας

Στόχος δεν είναι η απόλυτη ασφάλεια αλλά δηλώσεις όπως

Η πιθανότητα να σπάσει ο κώδικας σε χρόνο μέχρι 2^{100}s είναι μικρότερη από 2^{-20}

Το κόστος για αυτό είναι τεράστιο

ΜΟΝΤΕΛΟ ΣΥΜΜΕΤΡΙΚΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ



ΣΥΜΜΕΤΡΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ (SYMMETRIC CIPHERS): Η ΛΑΚΕΔΑΙΜΟΝΙΚΗ ΣΚΥΤΑΛΗ

ΜΗΧΑΝΗ ENIGMA

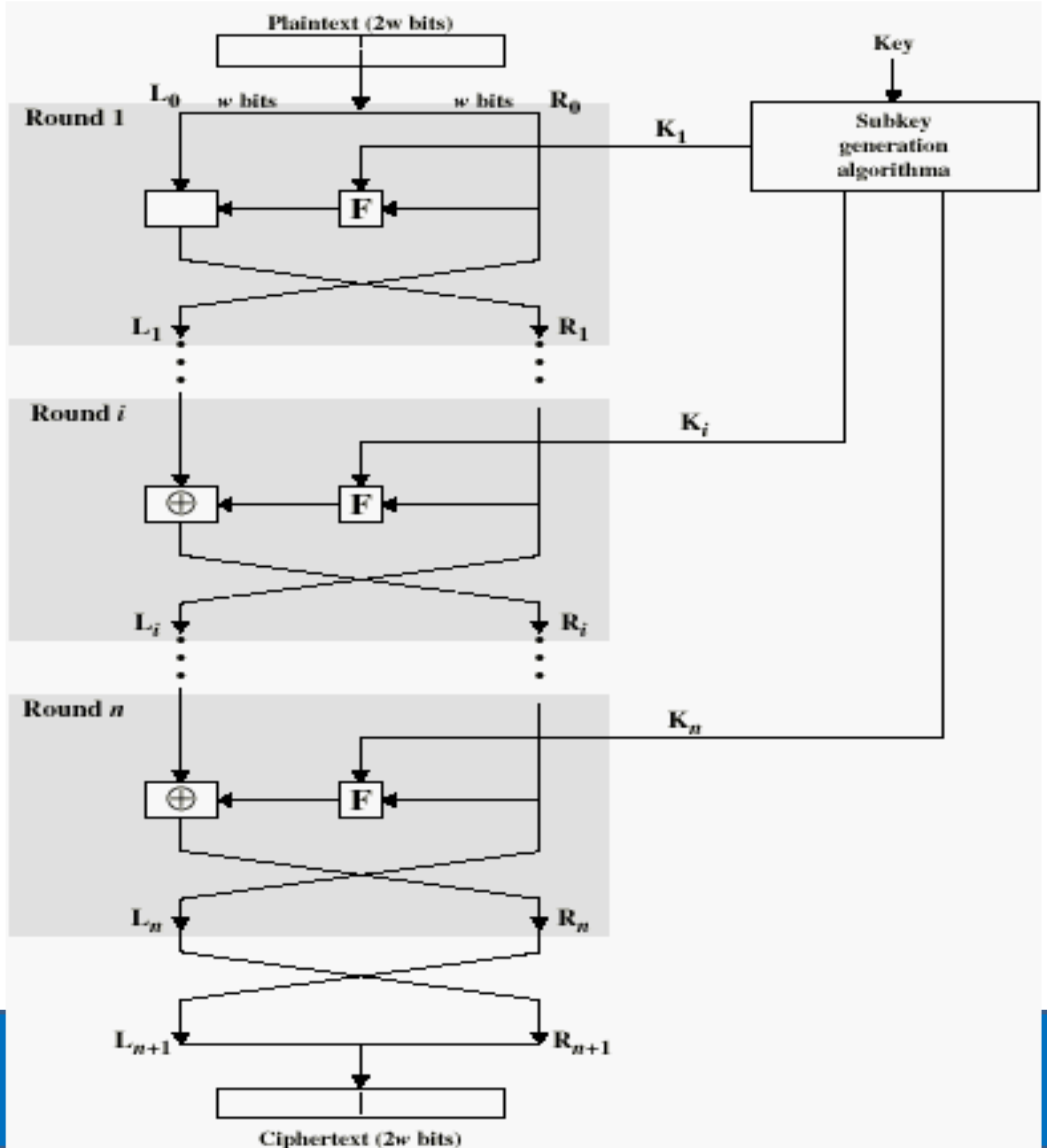
- Enigma: Μηχανή που παρήγε κώδικες αντιμετάθεσης
- Εφευρέθηκε στην Γερμανία (1920) και χρησιμοποιήθηκε κατά τον Β΄ Παγκόσμιο Πόλεμο
- Κρυπτολόγοι των συμμαχικών δυνάμεων (Alan Turing) κατάφεραν να σπάσουν κώδικες και να αποκρυπτογραφήσουν μηνύματα

ΑΛΓΟΡΙΘΜΟΙ ΤΜΗΜΑΤΟΣ: (BLOCK CIPHERS)- ΔΟΜΗ FEISTEL

- Στην πραγματικότητα όλοι οι conventional block encryption algorithms, όπως πχ. ο DES έχουν την δομή που αναπτύχθηκε από τον Horst Feistel of IBM το 1973.

- Η ακριβής δομή-υλοποίηση ενός Feistel Network εξαρτάται από την κατάλληλη επιλογή μιας σειράς από παραμέτρους και χαρακτηριστικά σχεδιασμού όπως Block size, Key Size, Number of rounds και Subkey generation algorithm.

ΑΡΧΙΤΕΚΤΟΝΙΚΗ FEISTEL CIPHER



DATA ENCRYPTION STANDARD (DES) (1/2)

- Πρώτο Πρότυπο Κρυπτογράφησης
- Ευρέως διαδεδομένος και χρησιμοποιούμενος αλγόριθμος
- Ο DES ανήκει στην κατηγορία των block ciphers
- Το plaintext υφίσταται επεξεργασία σε τμήματα (blocks) των 64-bit
- Το χρησιμοποιούμενο κλειδί έχει μέγεθος 56-bit (64-bit)

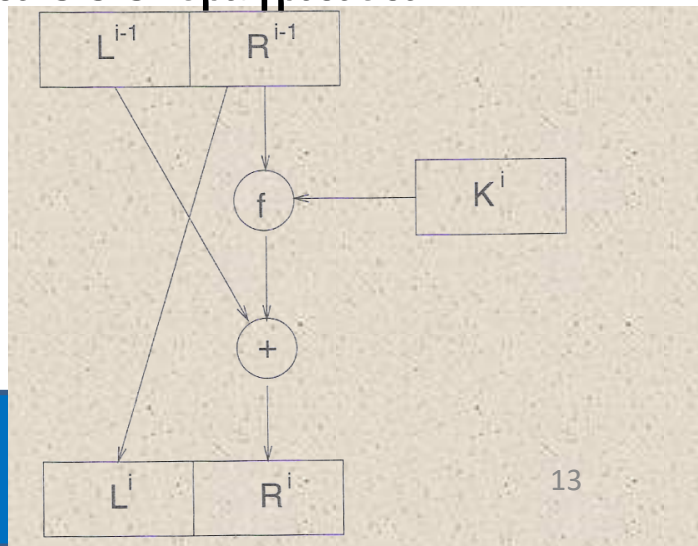
DATA ENCRYPTION STANDARD (DES) (2/2)

Τα κριτήρια σχεδιασμού του DES ήταν

- Υψηλό επίπεδο ασφάλειας
- Πλήρεις και διαφανείς προδιαγραφές
- Η ασφάλειά του δεν θα πρέπει να εξαρτάται από την μυστικότητα του αλγορίθμου
- Διαθέσιμος και προσβάσιμος σε/από όλους τους χρήστες
- Κατάλληλος για ποικιλία εφαρμογών
- Χαμηλό κόστος υλοποίησης
- Να είναι δυνατή η αξιολόγηση του

ΦΙΛΟΣΟΦΙΑ ΜΕΤΑΤΡΟΠΗΣ ΔΕΔΟΜΕΝΩΝ (1/2)

- Ο αλγόριθμος DES βασίζεται στο πρότυπο του Feistel, δηλαδή σε σταδιακές αντιμεταθέσεις του αριστερού και δεξιού τμήματος του αρχικού απλού κειμένου
- Σε κάθε στάδιο i επιδρά μία συνάρτηση f, που λαμβάνει σαν είσοδο το υποκλειδί K_i, και το δεξιό τμήμα των δεδομένων
- Στη συνέχεια στο δεξιό (προκύπτον) και στο αριστερό τμήμα επιδρά μία συνάρτηση XOR και τα δύο τμήματα αντιμετατίθενται



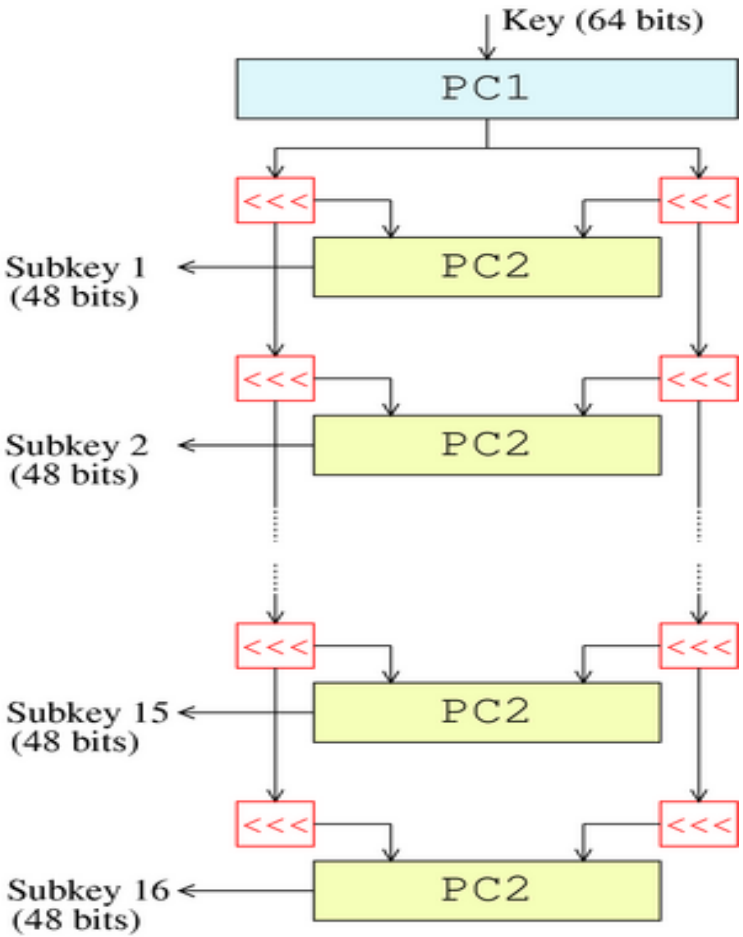
ΦΙΛΟΣΟΦΙΑ ΜΕΤΑΤΡΟΠΗΣ ΔΕΔΟΜΕΝΩΝ (2/2)

- Μετατροπή δεδομένων σε κάθε γύρο:
  - Li = Ri-1,
  - Ri = Li-1 XOR F(Ri-1, Ki)

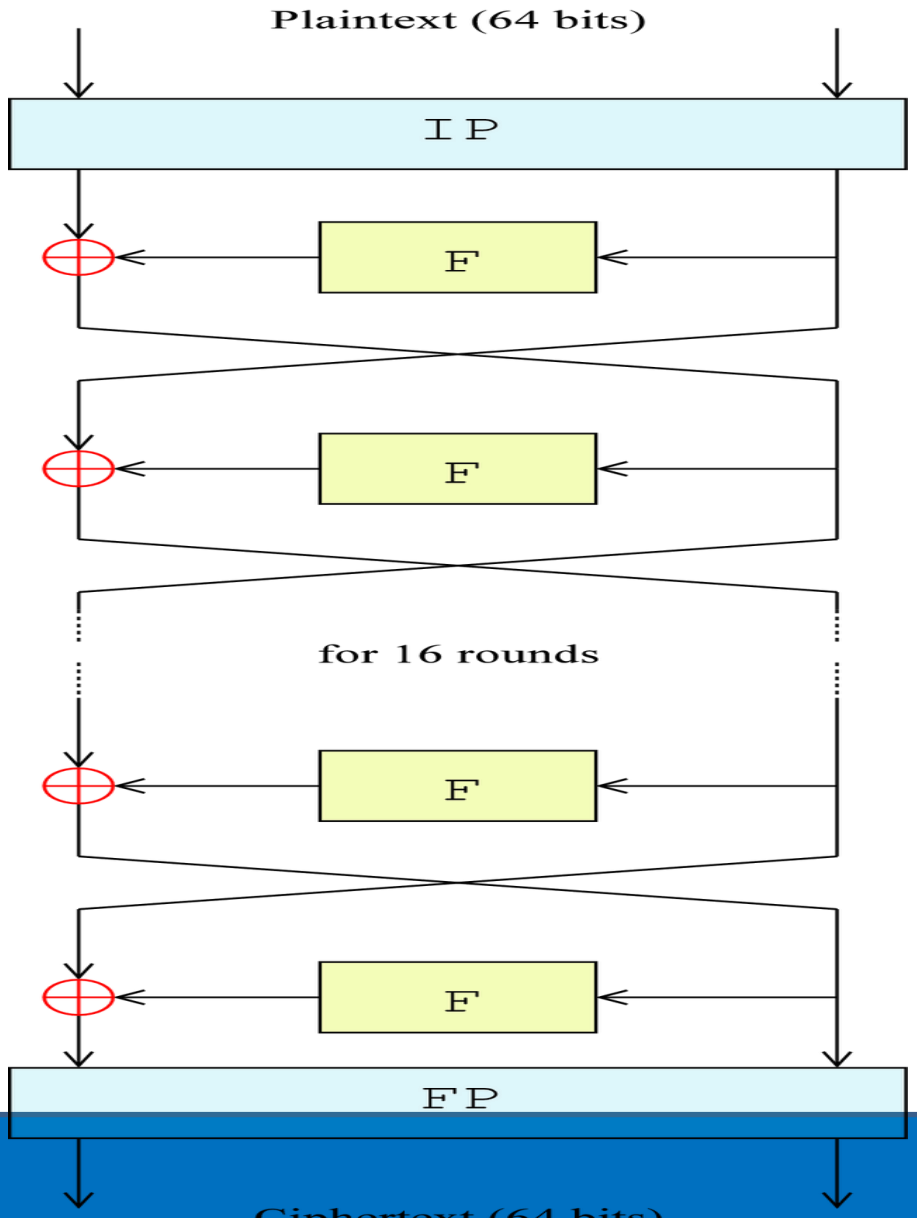
- Κλειδί :
  - *Αρχικό (64-bit)*
  - *Basic Key (56-bit)*
  - *Round Key (48-bit)*

ΠΑΡΑΓΩΓΗ ΥΠΟΚΛΕΙΔΙΩΝ

- Η παραγωγή υποκλειδιών εμπεριέχει τα παρακάτω βήματα
  - Από το αρχικό 64-bit κλειδί K επιλέγονται μόνο τα 56-bit. Τα υπόλοιπα χρησιμοποιούνται για διόρθωση λαθών
  - Τα 56-bit διαχωρίζονται σε δύο (αριστερό και δεξιό) ίσα μέρη από 28-bit το καθένα
  - Σε κάθε στάδιο τα δύο μέρη ολισθαίνουν αριστερά (ή δεξιά) κατά ένα ή κατά δύο bit (ανάλογα με το στάδιο)
  - Μετά από κάθε ολίσθηση τα δύο μέρη συνενώνονται και εισάγονται σε μία PC2-συνάρτηση, η οποία λαμβάνει 28+28 = 56-bits και παράγει 24+24 = 48-bits που είναι και το υποκλειδί σε κάθε στάδιο



ΔΟΜΗ DES


Plaintext (64 bits)
IP
F
F
for 16 rounds
F
F
FP
Ciphertext (64 bits)

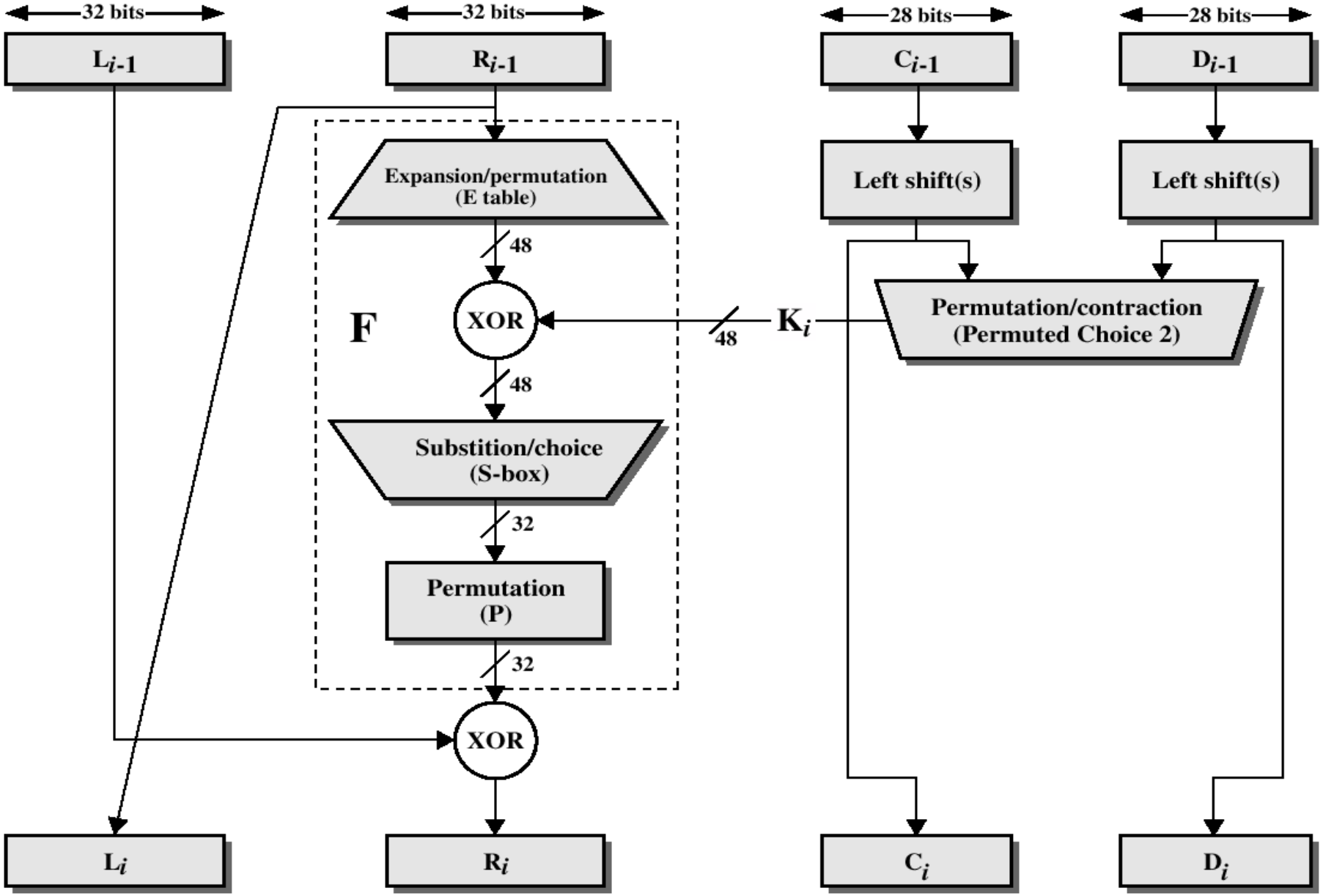
ΑΡΧΙΚΗ ΜΕΤΑΘΕΣΗ

- Η αρχική μετάθεση (IP), είναι ένας πίνακας που αντιμεταθέτει την σειρά των bits της εισόδου σύμφωνα με τον παρακάτω πίνακα

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

- Η τελική μετάθεση (IP^{-1}) είναι ένας πίνακας αντίστροφος από την αρχική μετάθεση και «εργάζεται» με τον ίδιο τρόπο

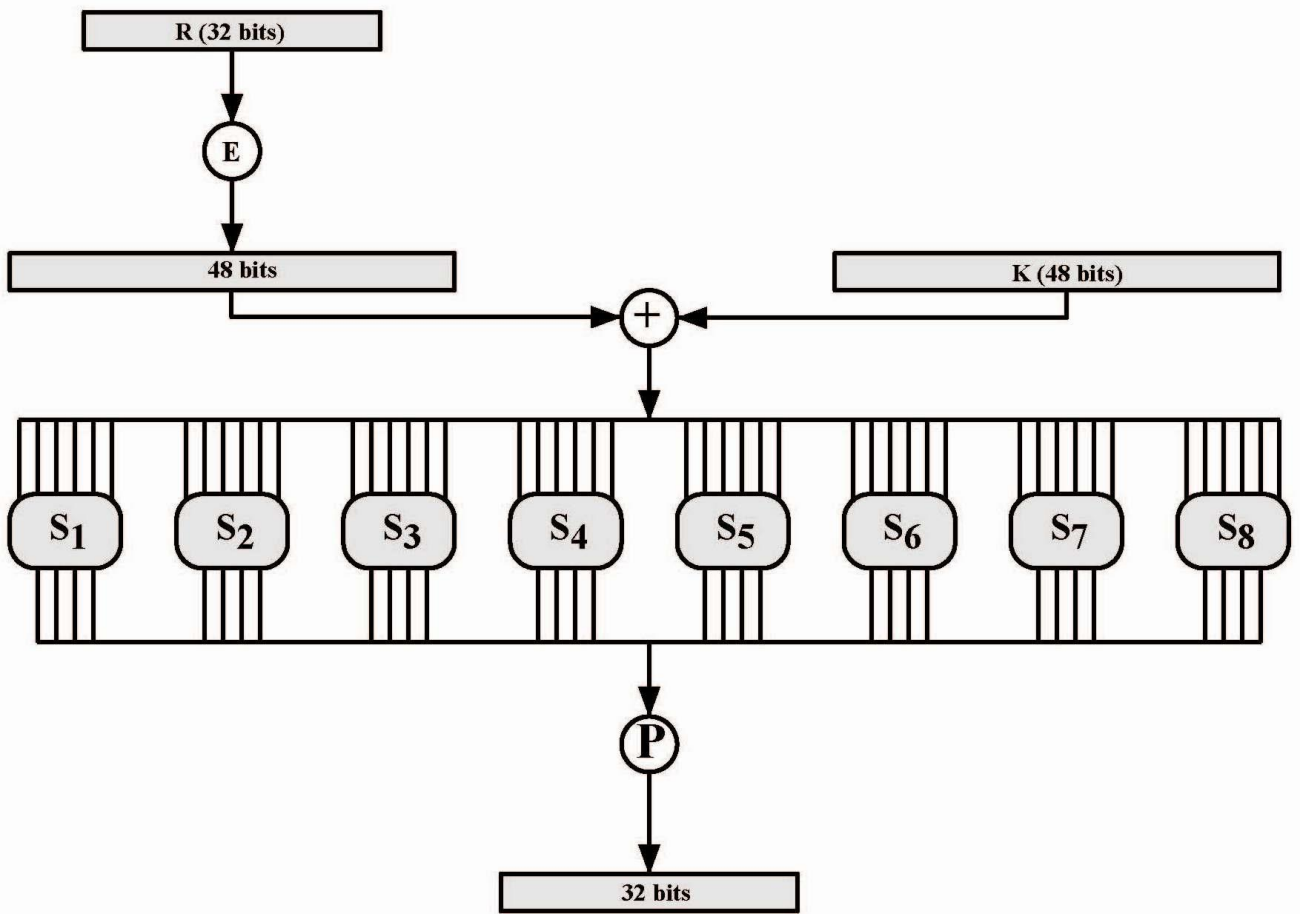
ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ DES



ΣΥΝΑΡΤΗΣΗ F(R,K) (1/2)

- Η συνάρτηση F αποτελείται από 4 στάδια:
  - Επέκταση
    - Η συνάρτηση Ε έχει σαν είσοδο 32-bit και παράγει σαν έξοδο 48-bit
  - Μίξη κλειδιού
    - Η 48-bit έξοδος της συνάρτησης Ε συνδυάζεται με πράξη XOR με το 48-bit υποκλειδί του τρέχοντος σταδίου
  - Αντικατάσταση
    - Η παραπάνω έξοδος διαχωρίζεται σε 8 μέρη των 6-bit και εισάγεται στα S-κουτιά. Κάθε S-κουτί δέχεται 6-bit και παράγει 4-bit σύμφωνα με προδιαγεγραμμένο τρόπο αντικατάστασης
  - Αντιμετάθεση
    - Η 32-bit έξοδος των S-κουτιών αντιμετατίθεται σύμφωνα με την P-συνάρτηση

ΣΥΝΑΡΤΗΣΗ F(R,K) (2/2)



Η συνάρτηση επέκτασης Ε είναι μια μετάθεση στην οποία ορισμένα bits εισόδου εμφανίζονται σε περισσότερες από μια θέσεις στην έξοδο

S-Boxes: S1, S2, S3

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

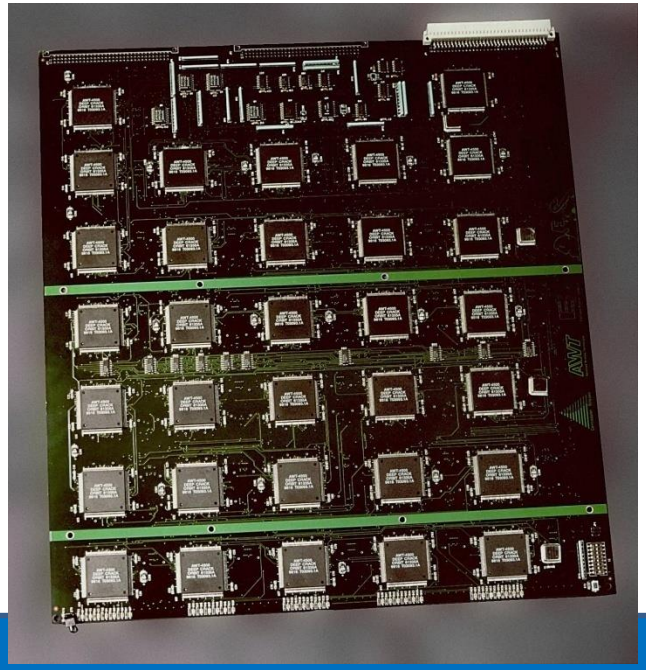
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

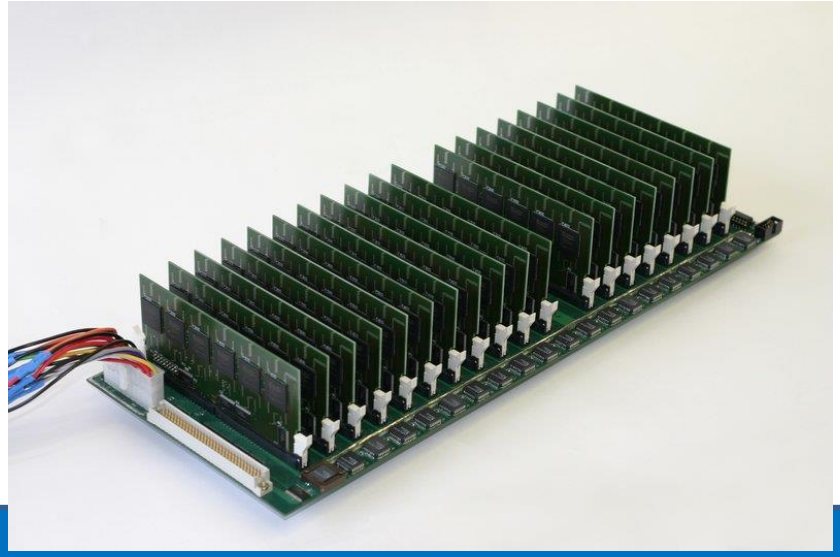
ΠΑΡΑΒΙΑΣΗ ΤΟΥ DES (1/2)

- Ο αλγόριθμος DES παραβιάστηκε το 1997 μέσω της μηχανής EFF που κόστισε 250.000$ μέσα σε χρονικό διάστημα 2 ημερών



ΠΑΡΑΒΙΑΣΗ ΤΟΥ DES (2/2)

- Άλλη μηχανή που αποδεδειγμένα παραβιάζει τα κλειδιά του DES είναι η COPACOBANA αξίας 10.000$. Η μηχανή «παραβιάζει» τον DES σε μέσο χρόνο 6.4 ημερών



Ο ΑΛΓΟΡΙΘΜΟΣ Triple-DES

- Χρησιμοποιεί 3 διαφορετικά κλειδιά και τρεις "υλοποιήσεις" του αλγορίθμου DES:

Encrypt – Decrypt - Encrypt

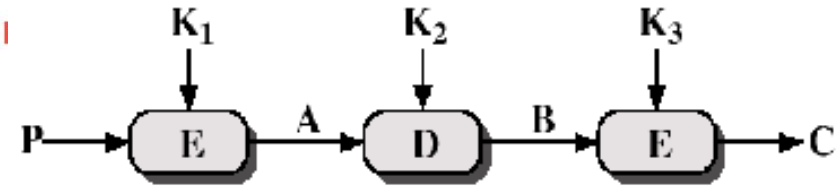
$$C = E_{K3}[D_{K2}[E_{K1}[P]]]$$

  - C = ciphertext
  - P = Plaintext
  - EKi[X] = κρυπτογράφηση του X χρησιμοποιώντας το κλειδί Ki
  - DKj[Y] = αποκρυπτογράφησης του Y χρησιμοποιώντας το κλειδί Kj

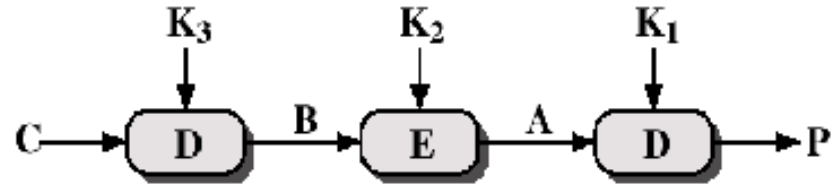
- Συνολικό ενεργό μήκος κλειδιού:

168-bit = (56-bit + 56-bit + 56-bit)

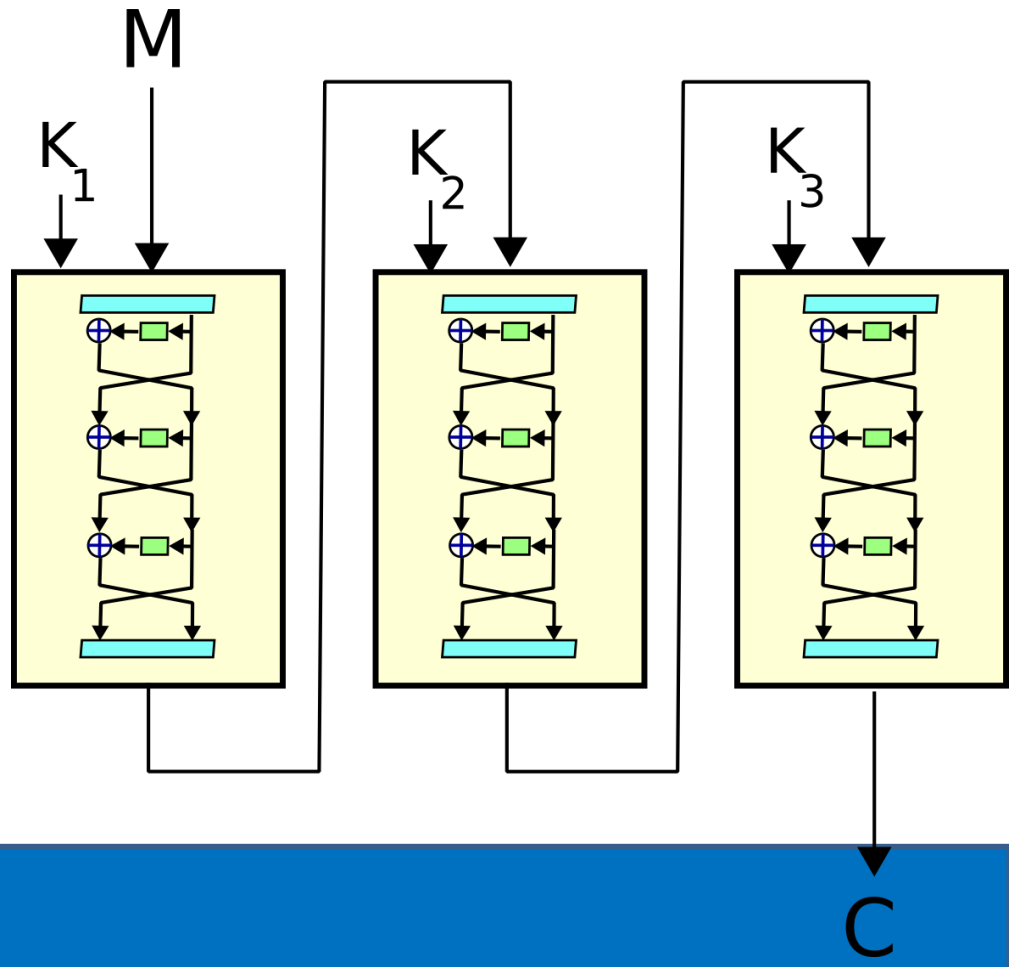
ΑΡΧΙΤΕΚΤΟΝΙΚΗ Triple-DES



(a) Encryption



(b) Decryption



ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΩΝ

- Σχετικά με τα κλειδιά K_1, K_2 και K_3 υπάρχουν τρεις διαφορετικές περιπτώσεις:
  - Τα τρία κλειδιά να είναι ανεξάρτητα ($K_1 \neq K_2 \neq K_3$)
  - Τα κλειδιά K_1 και K_2 να είναι ανεξάρτητα αλλά $K_1 = K_3$
  - Τα τρία κλειδιά να είναι ίδια ($K_1 = K_2 = K_3$) (απαγορευμένη περίπτωση-εκφυλίζεται σε απλό DES)

Ο ΑΛΓΟΡΙΘΜΟΣ AES: ΓΕΝΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ

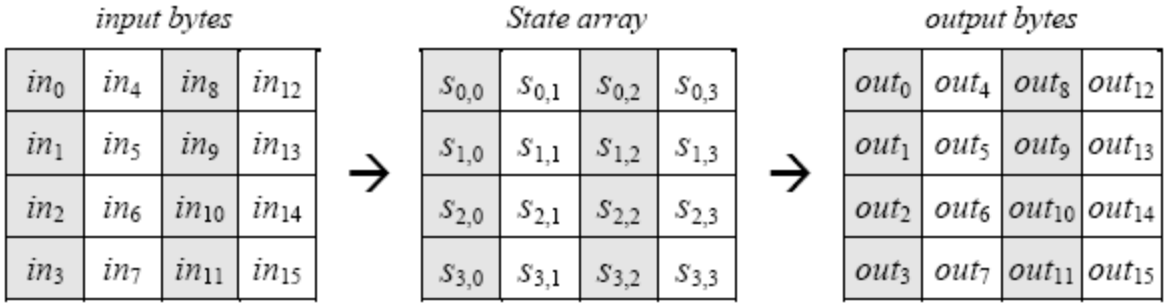
- Το πρότυπο κρυπτογράφησης AES (Advanced Encryption Standard) περιγράφει μια διαδικασία κρυπτογράφησης ηλεκτρονικής πληροφορίας βασισμένη στην λογική της κωδικοποίησης ομάδων δεδομένων με κάποιο μυστικό κλειδί
- Έχει προτυποποιηθεί από το NIST (National Institute of Technology) τον Νοέμβριο του 2001, αντικαθιστώντας το πρότυπο DES (Data Encryption Standard) και πλέον αποτελεί τον προτεινόμενο αλγόριθμο για εφαρμογές κρυπτογράφησης
- Ο AES χρησιμοποιεί ένα υποσύνολο των δυνατοτήτων του Rijndael αλγορίθμου. Το τελικό κείμενο με τις προδιαγραφές του προτύπου εκδόθηκε προς το τέλος του 2001, ως FIPS-PUB-197 (Federal Information Processing Standard Publication)

Ο ΑΛΓΟΡΙΘΜΟΣ AES (1/3)

- Ο AES
  - Είναι αλγόριθμος τμήματος με απλό κείμενο και κρυπτοκείμενο 128-bit
  - Με κλειδί 128-, 192- ή 256-bit
- Μεγάλος κλειδοχώρος που καθιστά την εξαντλητική αναζήτηση πρακτικά αδύνατη
- Ο αριθμός των γύρων r εξαρτάται από το κλειδί
  - Για $r_{128}=10$, $r_{192}=12$, $r_{256}=14$
- Σε κάθε γύρο κρυπτογραφείται όλη η είσοδος

Ο ΑΛΓΟΡΙΘΜΟΣ AES (2/3)

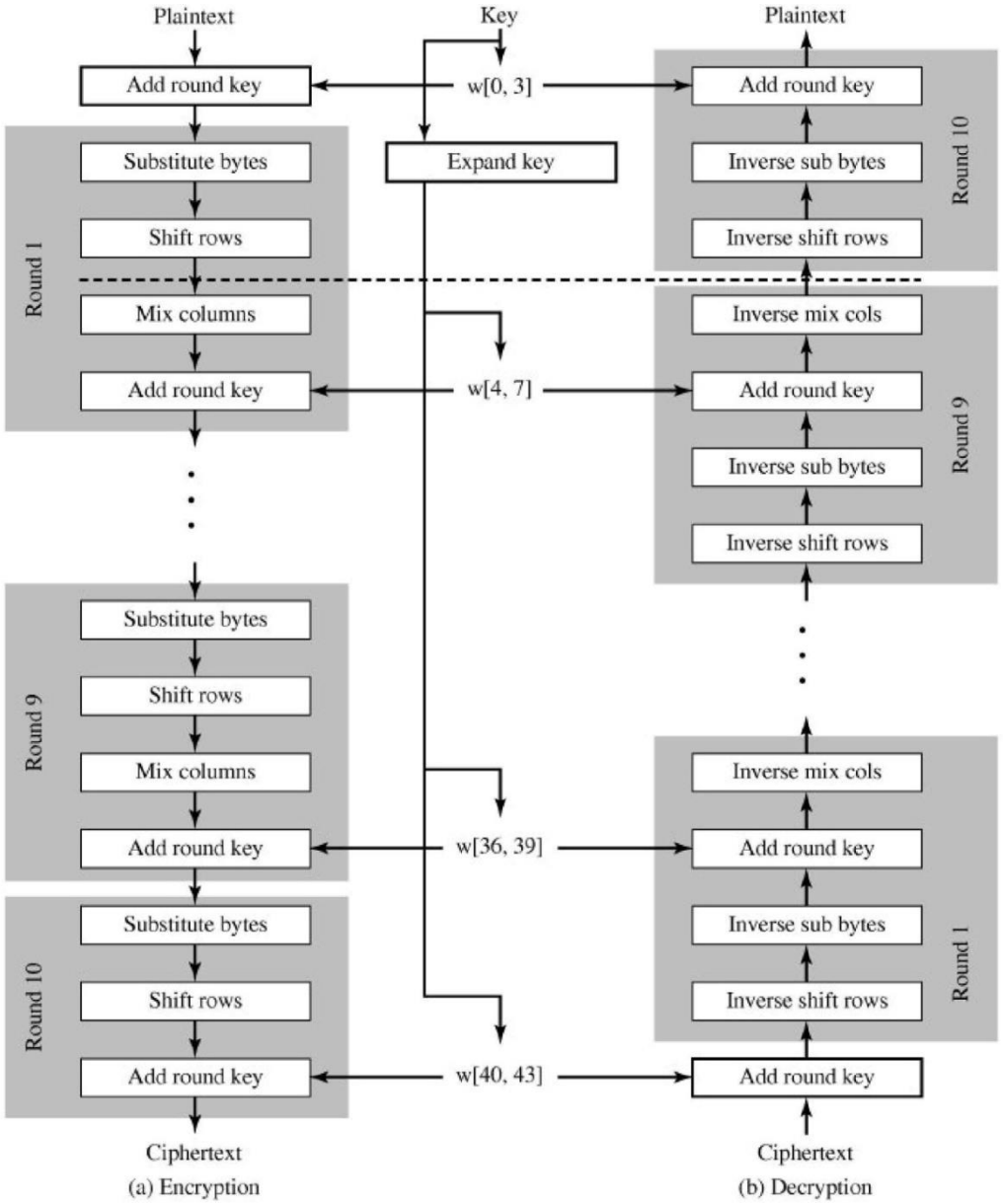
- Βασικό συστατικό του αλγόριθμου είναι ένας 4X4 (4X4X8=128) πίνακας που περιέχει bytes και ονομάζεται κατάσταση (state)
- Ο πίνακας κατάσταση περιέχει 4 γραμμές και Nb στήλες. Επειδή χρησιμοποιούμε 128 bit εισόδου ο αριθμός των στηλών είναι 128/32=4



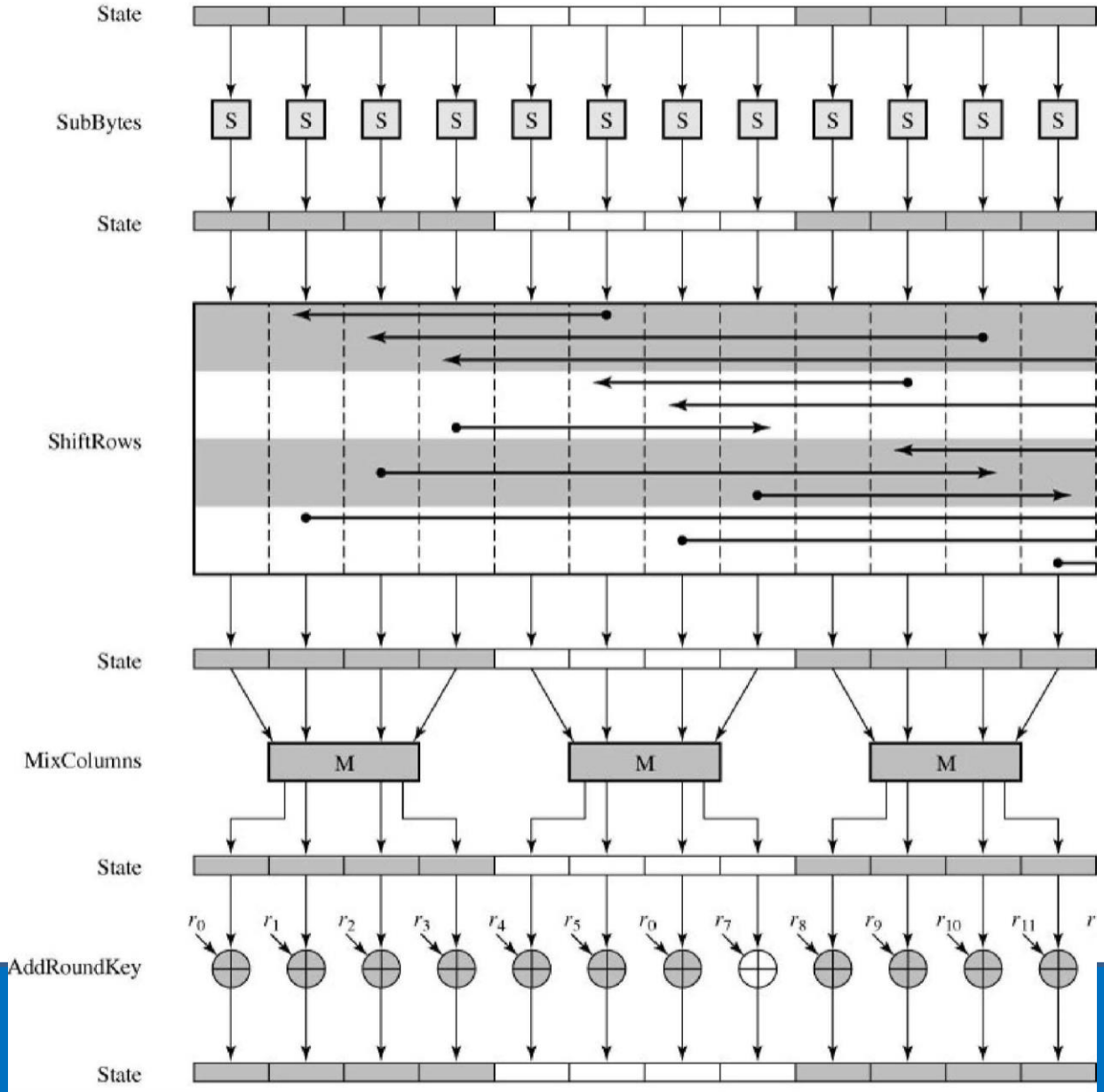
Ο ΑΛΓΟΡΙΘΜΟΣ AES (3/3)

- Ο αλγόριθμος εκτελείται σύμφωνα με τα παρακάτω βήματα:
  - Επέκταση κλειδιού (Γεννήτρια Παραγωγής υποκλειδιών)
  - Αρχικό στάδιο πρόσθεσης κλειδιού
  - Ενδιάμεσα στάδια όπου περιλαμβάνονται οι εξής συναρτήσεις:
    - Συνάρτηση SubBytes (μετασχηματισμός αντικατάστασης)
    - Συνάρτηση ShiftRows (μηχανισμός ολίσθησης)
    - Συνάρτηση MixColumns (διαδικασία μίξης)
    - Συνάρτηση AddroundKey (πρόσθεση κλειδιού).
  - Τελικό στάδιο (χωρίς την εφαρμογή της συνάρτησης MixColumns)

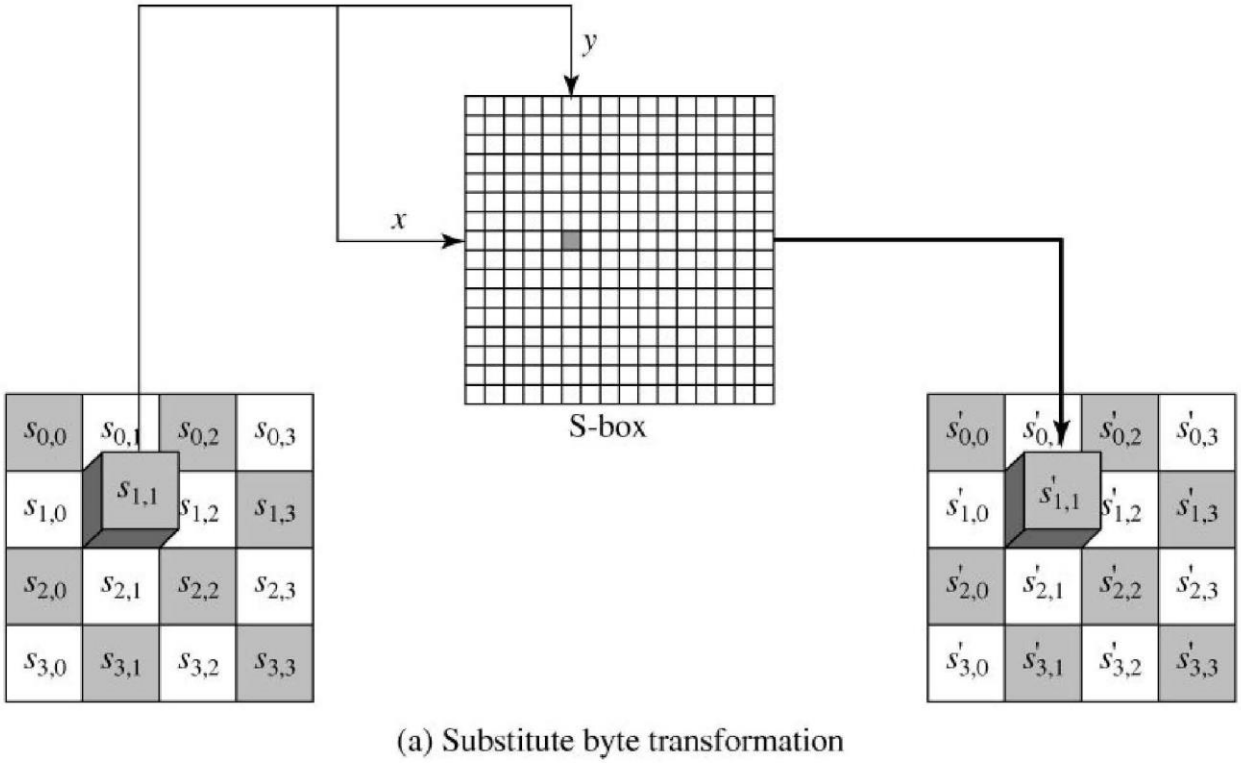
Ο ΑΛΓΟΡΙΘΜΟΣ AES: ΒΑΣΙΚΗ ΔΟΜΗ



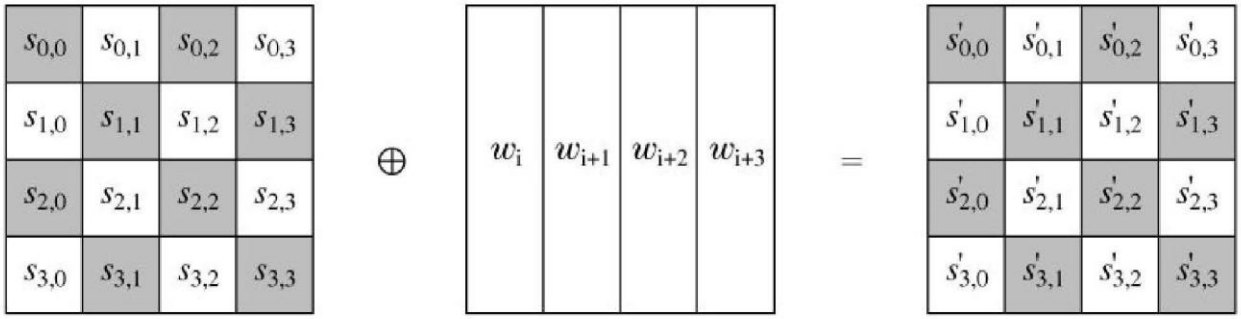
ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ ΔΕΔΟΜΕΝΩΝ



ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΙ: S-Box ΚΑΙ Add Round Key



(a) Substitute byte transformation



(b) Add Round Key Transformation

ΔΙΑΧΥΣΗ ΔΕΔΟΜΕΝΩΝ

- Η διαδικασία διάχυσης αποτελείται από τις πράξεις shift_rows και mix_columns στον AES
- **Διάχυση (Diffusion)** είναι η ικανότητα του αλγορίθμου κρυπτογράφησης όπου ένα τμήμα του απλού κειμένου να έχει τη δυνατότητα να επηρεάζει όσο το δυνατόν περισσότερα τμήματα του κρυπτοκειμένου
  - Ένας αλγόριθμος έχει υψηλή διάχυση όταν ένα στοιχειώδεις τμήμα του απλού κειμένου έχει την δυνατότητα να επηρεάσει όλα τα τμήματα του κρυπτοκειμένου, ανεξάρτητα της τοποθεσίας του τμήματος αυτού στο απλό κείμενο

ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ Shift Row

Η διαδικασία διάχυσης αποτελείται από τις πράξεις shift_rows και mix_columns

- Στην shift_rows η είσοδος χωρίζεται σε 16 bytes και το κάθε byte διατάσσεται κάθετα σε έναν πίνακα 4x4. Στη συνέχεια πραγματοποιείται ολίσθηση των bytes ως προς τις γραμμές

S0	S4	S8	S12
S1	S5	S9	S13
S2	S6	S10	S14
S3	S7	S11	S15

→

S0	S4	S8	S12
S5	S9	S13	S1
S10	S14	S2	S6
S15	S3	S7	S11

ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ Mix Columns

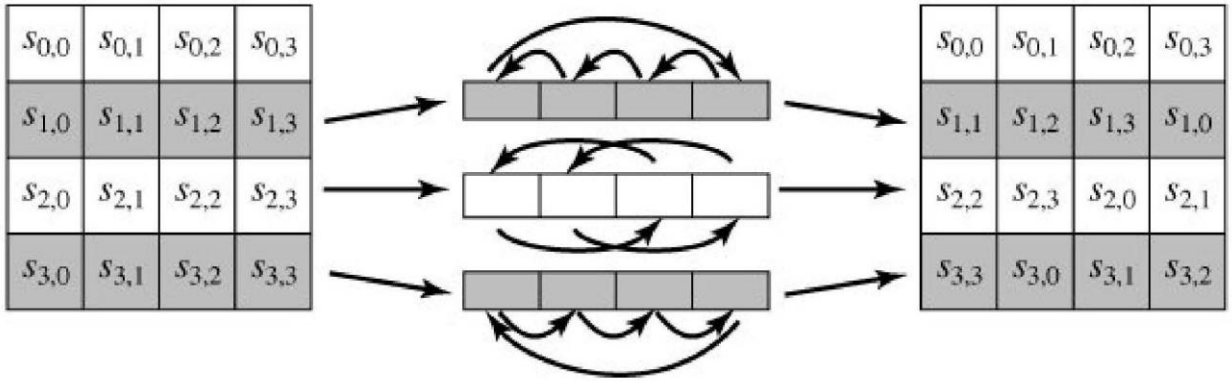
- Η διαδικασία mix_columns δέχεται τις λέξεις (bytes) ανά τετράδες και εφαρμόζει τον παρακάτω πολλαπλασιασμό

$$\begin{pmatrix} c_i \\ c_j \\ c_k \\ c_l \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} s_i \\ s_j \\ s_k \\ s_l \end{pmatrix}$$

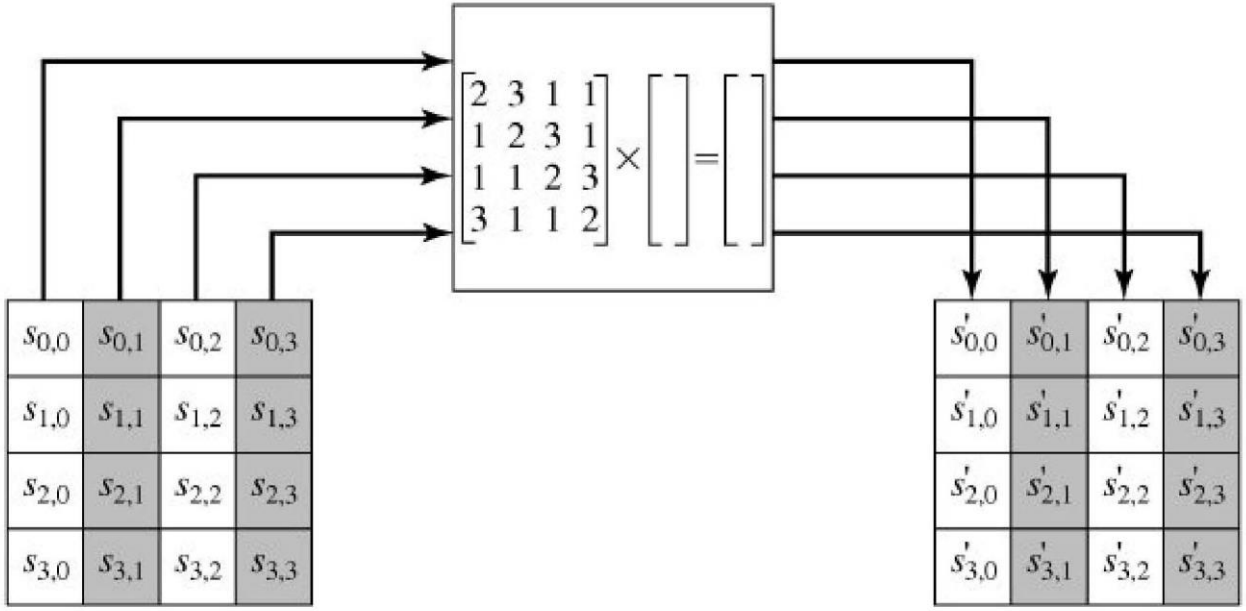
ΣΥΓΧΥΣΗ ΔΕΔΟΜΕΝΩΝ

- Η διαδικασία sub_bytes είναι υπεύθυνη για την αύξηση της σύγχυσης. Ουσιαστικά είναι ένα κουτί αντικατάστασης και αποτελεί τον μη γραμμικό μετασχηματισμό του αλγορίθμου. Η είσοδος χωρίζεται σε 16 bytes και η μη γραμμικότητα εφαρμόζεται σε κάθε byte χωριστά
- **Σύγχυση (Confusion)** είναι η ικανότητα του αλγορίθμου κρυπτογράφησης όπου ο αντίπαλος δεν είναι σε θέση να προβλέψει ποιες μεταβολές θα συμβούν στο κρυπτοκείμενο, δεδομένης μιας μεταβολής στο απλό κείμενο
  - Δηλαδή ένας αλγόριθμος έχει υψηλή σύγχυση όταν οι σχέσεις μεταξύ του απλού κειμένου και του κρυπτοκειμένου είναι αρκετά πολύπλοκες, ώστε να χρειάζεται ο αντίπαλος να ξοδέψει σημαντικό χρόνο προκειμένου να τις προσδιορίσει

ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΙ: Mix Column ΚΑΙ Shift Row



(a) Shift row transformation



(b) Mix column transformation

ΜΗΧΑΝΙΣΜΟΙ: S-Boxes

(a) S-box

		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	32	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

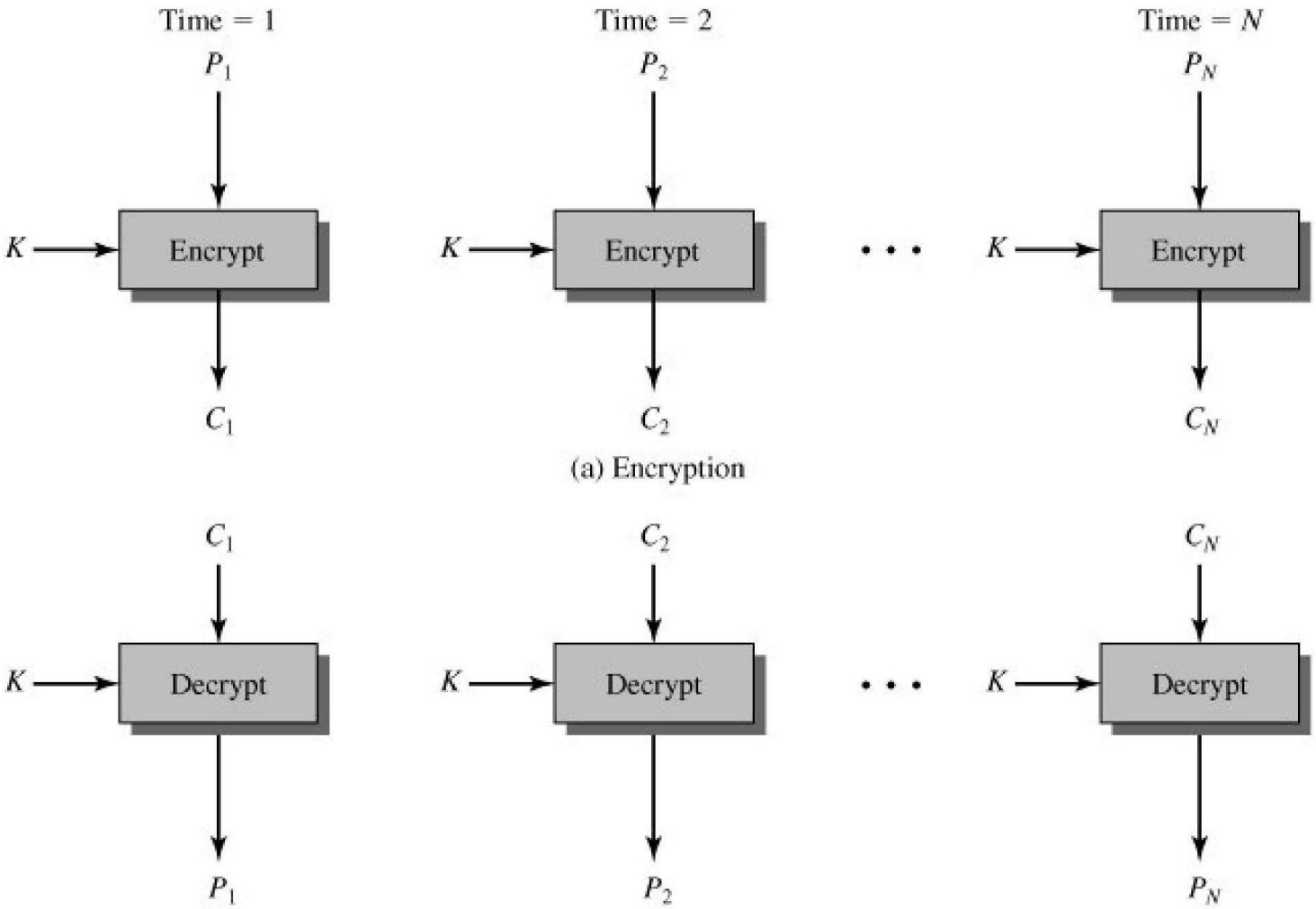
(b) Inverse S-box

		y														
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
	1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
	2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
	3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
	4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
	5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
	6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
	7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
	8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
	9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
	A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
	B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
	C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
	D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
	E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
	F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

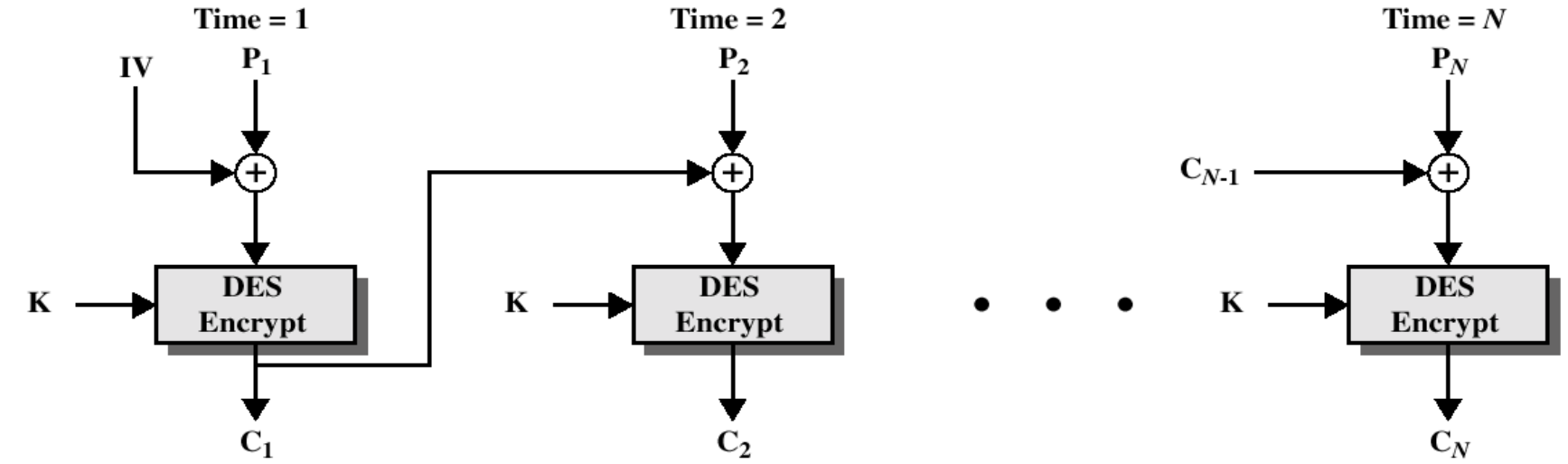
ΤΡΟΠΟΙ ΛΕΙΤΟΥΡΓΙΑΣ ΑΛΓΟΡΙΘΜΩΝ ΤΜΗΜΑΤΟΣ

- Είναι τρόποι διασύνδεσης των Block ciphers με σκοπό την περαιτέρω αύξηση της κρυπτογραφικής δύναμης και την αποτελεσματικότερη απόκρυψη πιθανών υπολειμμάτων πληροφορίας του απλού κειμένου στο κρυπτοκείμενο
- Κυριότεροι τυποποιημένοι τρόποι λειτουργίας
  - **Ηλεκτρονικό κωδικοβιβλίο (electronic codebook)**
  - **Κρυπταλγόριθμος αλυσιδωτού τμήματος (cipher block chaining, CBC)**
  - **Ανάδραση κρυπταλγορίθμου (cipher feedback, CFB)**
  - **Ανάδραση εξόδου (output feedback, OFB)**

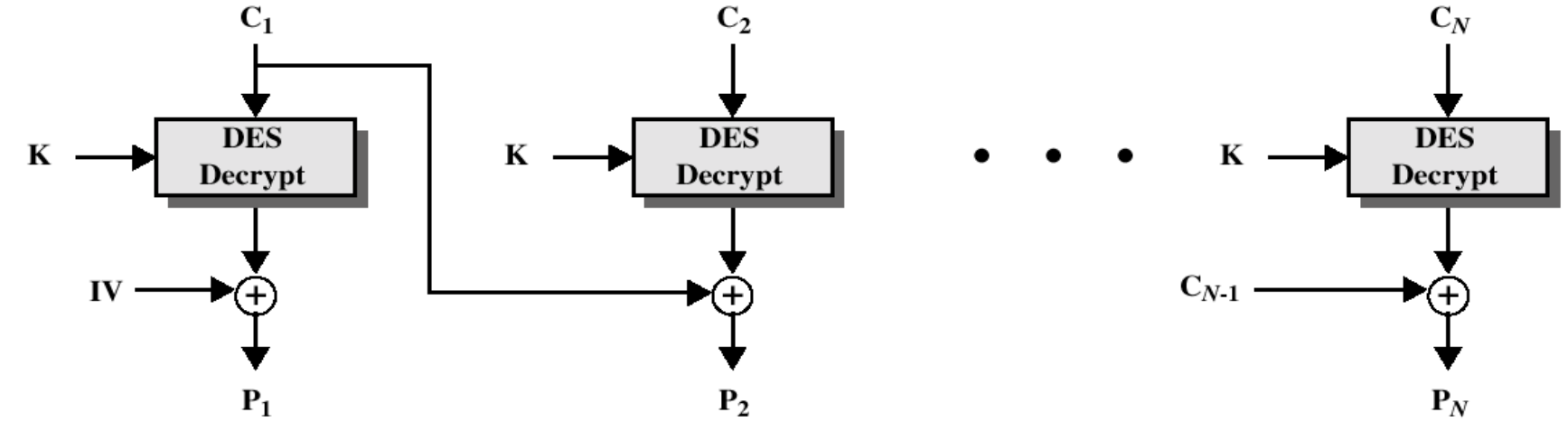
ELECTRONIC CODEBOOK (ECB)



ΑΡΧΙΤΕΚΤΟΝΙΚΗ CIPHER BLOCK CHAINING (CBC)

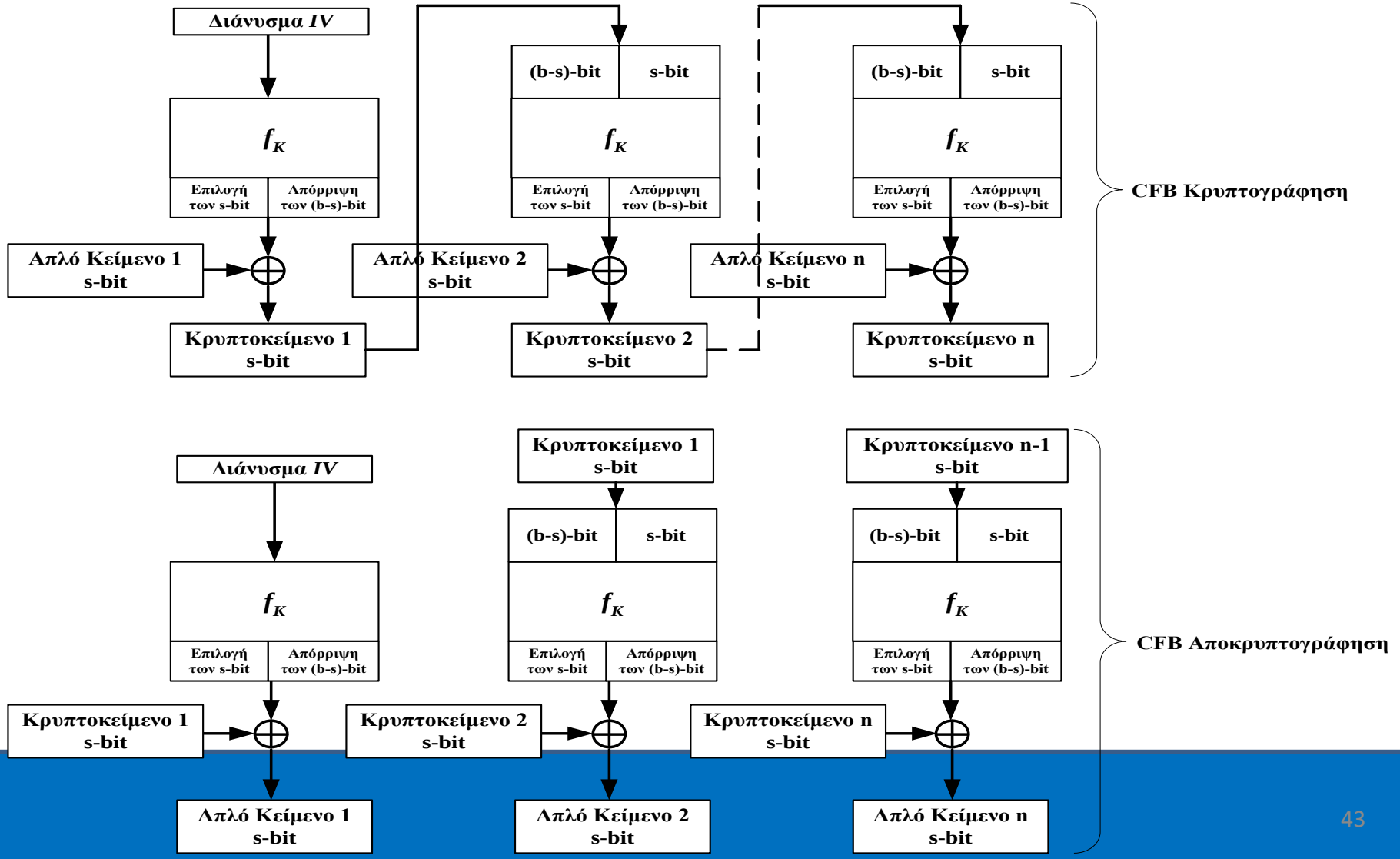


(a) Encryption

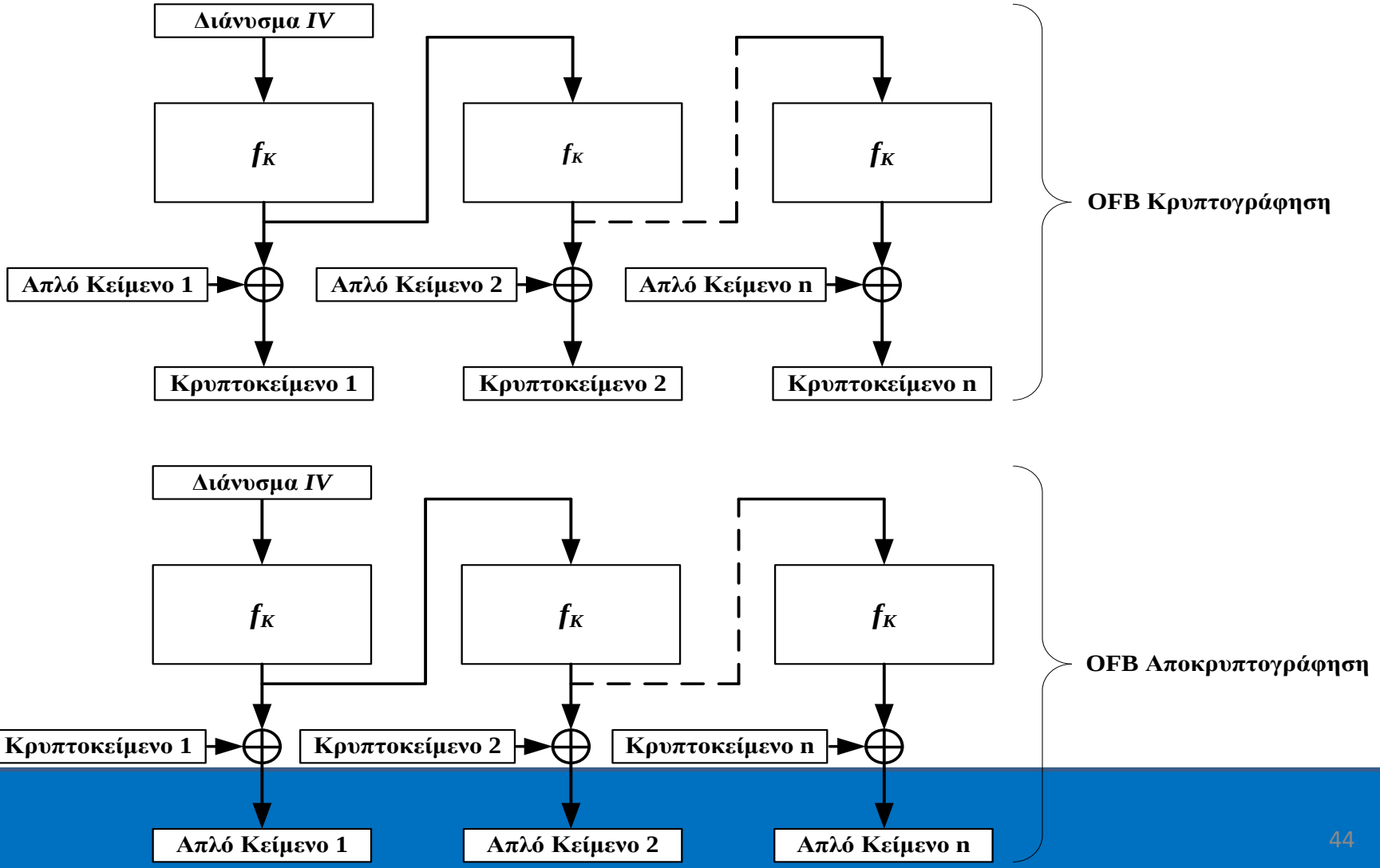


(b) Decryption

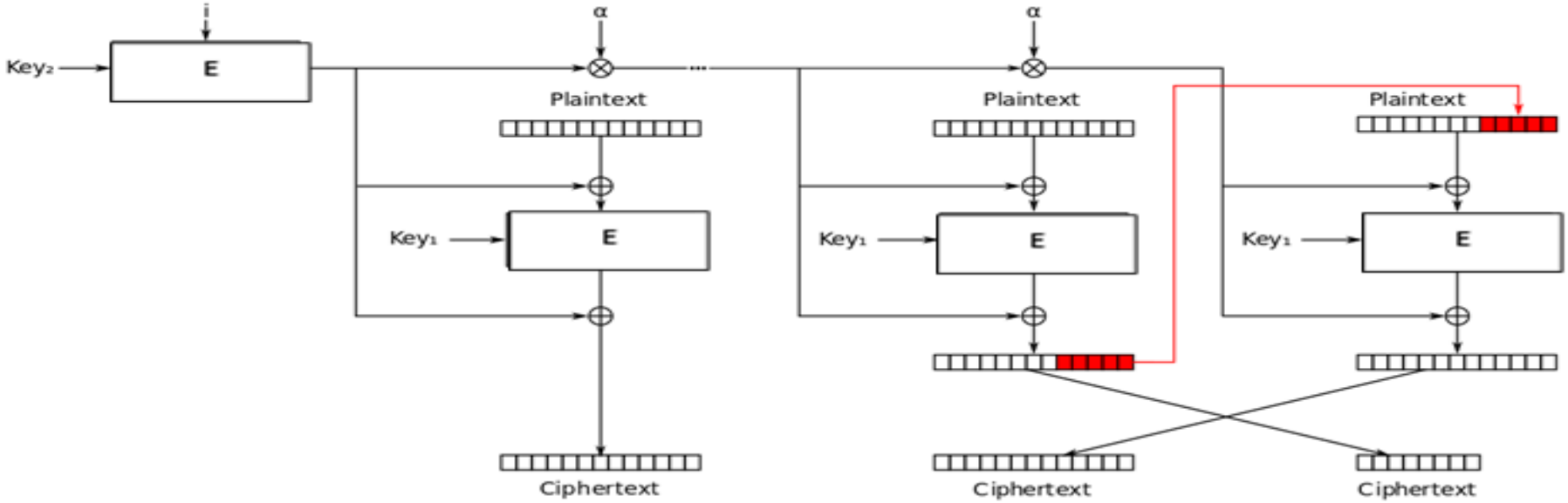
ΑΡΧΙΤΕΚΤΟΝΙΚΗ CIPHER FEEDBACK (CFB)



ΑΡΧΙΤΕΚΤΟΝΙΚΗ OUTPUT FEEDBACK (OFB)



ΑΡΧΙΤΕΚΤΟΝΙΚΗ AES-XTS



- Προσανατολισμένος στον AES – Χρήση δύο κλειδιών (διπλάσιο μέγεθος κλειδιού από τον AES)
- Ειδικά σχεδιασμένος για την κρυπτογράφηση αρχείων που τηρούνται σε αποθηκευτικά μέσα, όπου εκεί υπάρχουν ειδικότερες απαιτήσεις ως προς την ασφάλεια και την προσπέλαση (π.χ. εφαρμογές Veracrypt, Truecrypt, Bitlocker)
- Εάν το τελευταίο block του μηνύματος δεν έχει το κατάλληλο μέγεθος, συμπληρώνεται με τεχνική γνωστή ως “ciphertext stealing”

ECSALab

Απορίες??