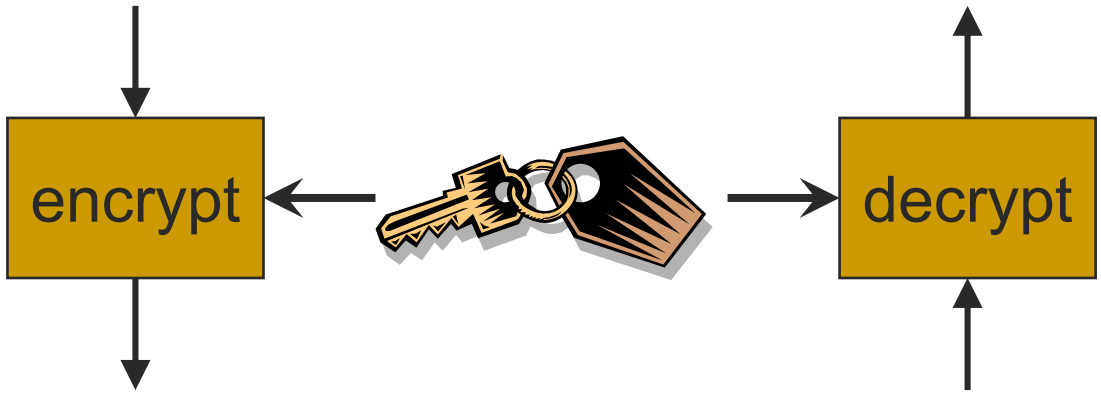
Κρυπτογραφία

Κεφάλαιο 3

Αλγόριθμοι τμήματος – Block ciphers

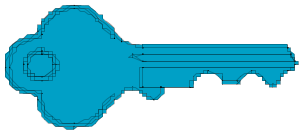
Αλγόριθμοι τμήματος

Τμήμα (μπλοκ) αρχικού μηνύματος μήκους n



Τμήμα (μπλοκ) κρυπτογράμματος μήκους n

Σχηματική αναπαράσταση

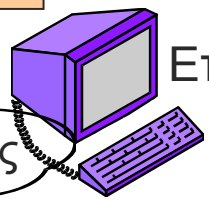


Το ίδιο κλειδί χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση και στα δύο μέρη.

Plaintext "Hello"

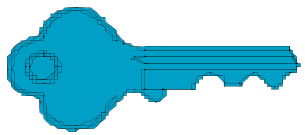
Μέθοδος κρυπτογρά-φησης και κλειδί

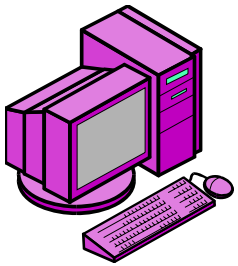
Ciphertext "11011101"



Επιτιθέμενος

Δίκτυο μετάδοσης





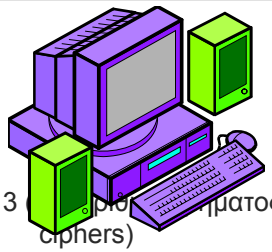
Αποστολέας

Ciphertext "11011101"

Μέθοδος αποκρυπτο-γράφησης και κλειδί

Plaintext "Hello"

Η κρυπτογράφηση λαμβάνει χώρα σε τμήματα του μηνύματος και όχι bit προς bit



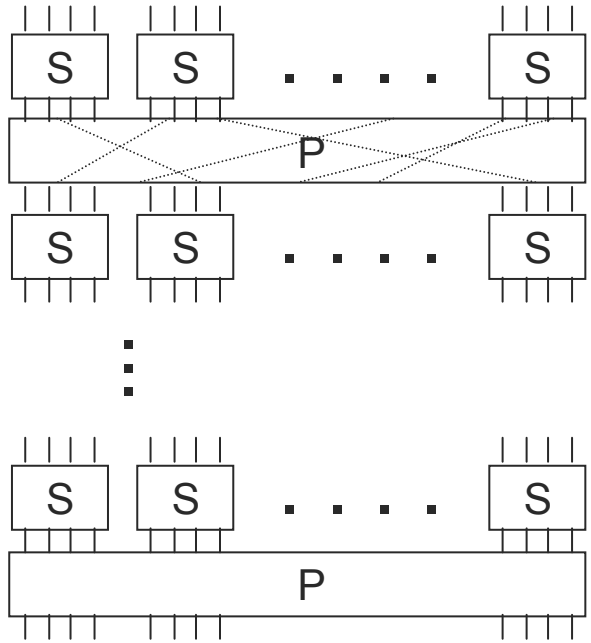
Παραλήπτης

Βασικές αρχές του Claude Shannon

- Το1949 ο Claude Shannon εισήγαγε την ιδέα των δικτύων αντικατάστασης-μετάθεσης (substitution-permutation (S-P) networks ή ΔΑΜ)
- Αποτελούν τη βάση των μοντέρνων αλγορίθμων τμήματος
- Τα ΔΑΜ βασίζονται σε δύο βασικούς κρυπτογραφικούς μετασχηματισμούς:
  - αντικατατάσταση (S-box)
  - *μετάθεση* (P-box)
- Παρέχουν σύγχυση (confusion) και διάχυση (diffusion) αντιστοίχως στο μήνυμα

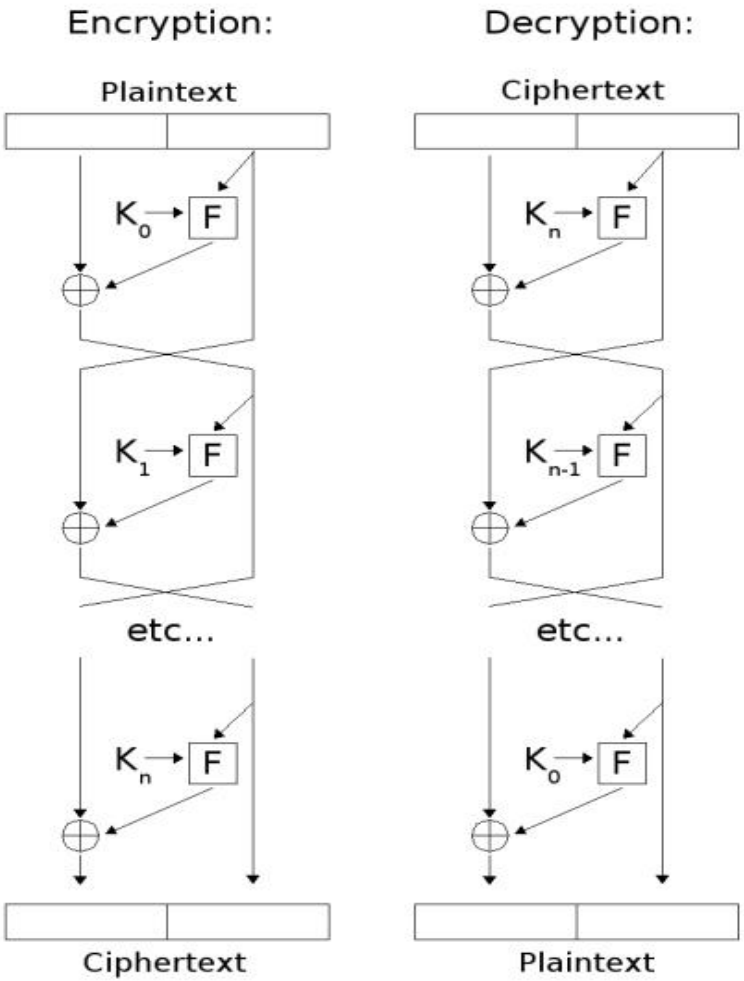
Δίκτυα αντικατάστασης-μετάθεσης κατά Shannon

Δομικά στοιχεία:
• μικρά «κουτιά», κατάλληλα σχεδιασμένα, που κάνουν αντικατάσταση (substitution boxes ή s-boxes)
•Η έξοδός τους περνάει από ένα «κουτί» που κάνει μετάθεση (permutation box ή p-box)
•Αυτό επαναλαμβάνεται πολλές φορές



•Με τον όρο «κουτί» (box) εννοούμε μία συνάρτηση (έναν μετασχηματισμό)

Δομή του δικτύου Feistel

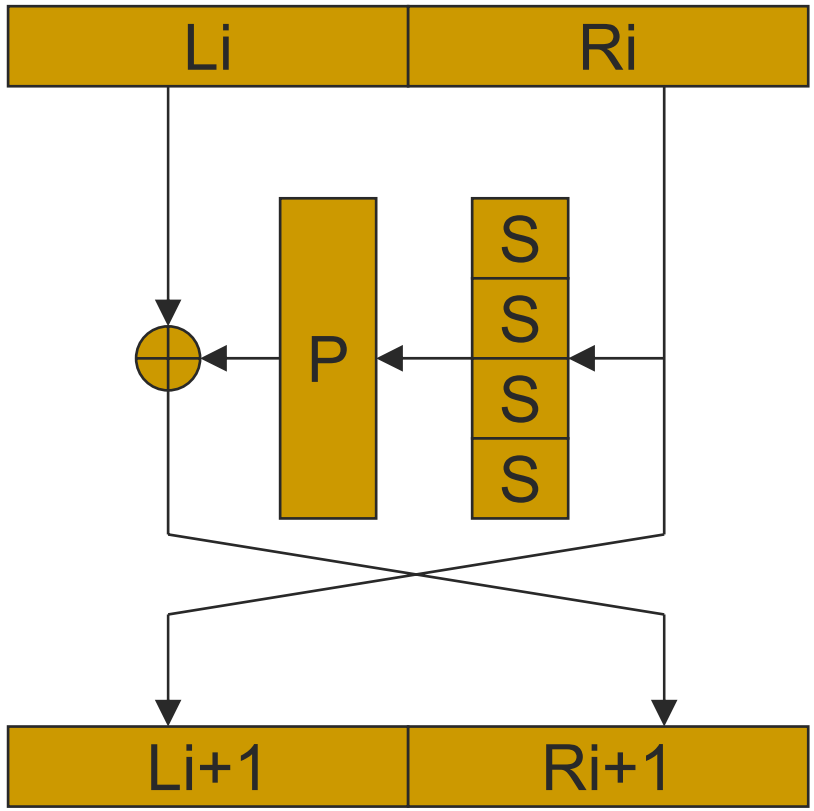


- Ο Horst Feistel όρισε τον αλγόριθμο Feistel (ή δίκτυο Feistel) βασισμένο στις παραπάνω αρχές του Shannon, ο οποίος ορίζεται ως εξής (βλέπε σχήμα):
- Η συνάρτηση f μπορεί να είναι οποιαδήποτε, αποτελούμενη όμως από κουτιά αντικατάστασης και μετάθεσης.
- Αν τα δύο τμήματα στα οποία χωρίζεται το αρχικό μπλοκ μηνύματος είναι ίσα, τότε το δίκτυο Feistel λέγεται **ισορροπημένο** (η πιο συνήθης περίπτωση)
- Η δομή επαναλαμβάνεται σε πολλούς γύρους (rounds)

Γενικά χαρακτηριστικά των δικτύων Feistel

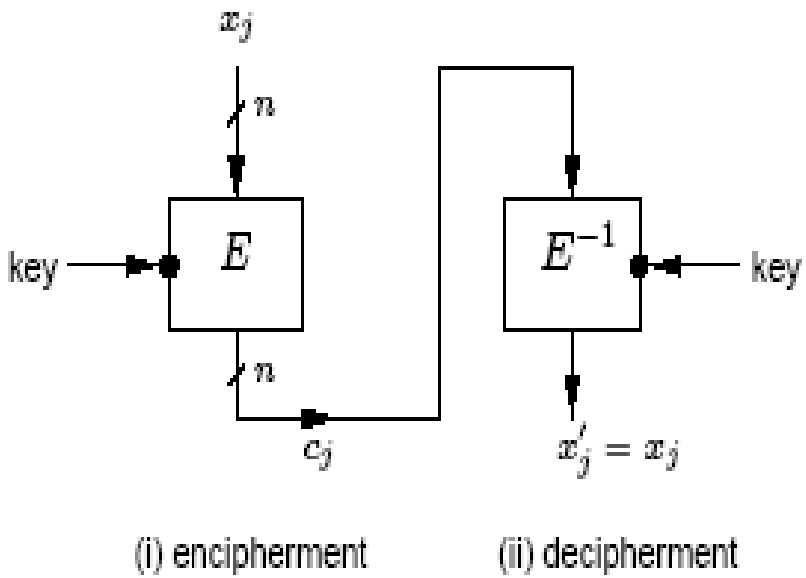
- **Μέγεθος μπλοκ**
  - Όσο πιο μεγάλο το μπλοκ τόσο μεγαλύτερη η ασφάλεια, αλλά και τόσο μικρότερη η ταχύτητα
- **Μέγεθος κλειδιού**
  - Πρέπει να είναι όσο γίνεται πιο μεγάλο (αν και πολύ μεγάλες τιμές ίσως κάνουν υπερβολικά αργό το όλο σύστημα)
- **Αριθμός γύρων**
  - Όσο πιο πολλοί τόσο πιο ασφαλής ο αλγόριθμος, αλλά και τόσο πιο αργός
- **Συνάρτηση f**
  - Όσο πιο σύνθετη είναι, τόσο πιο δύσκολο κάνει το έργο ενός κρυπταναλυτή: αλλά από την άλλη κάνει το σύστημα πιο αργό.

Ένας γύρος στο δίκτυο Feistel



Τρόποι λειτουργίας Block Ciphers (I)

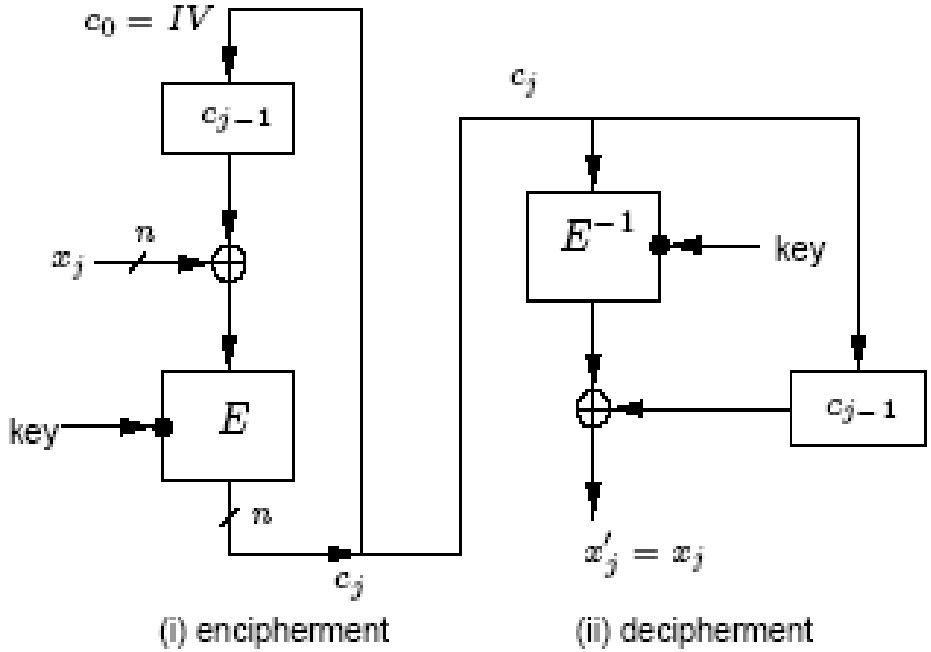
- Ηλεκτρονικό κωδικοβιβλίο (Electronic Codebook (ECB) mode): το κλειδί κρυπτογραφεί το κάθε block στο αντίστοιχο κρυπτόγραμμα. Δύο ίδια μηνύματα οδηγούν πάντα στο ίδιο κρυπτογραμμα (αν τους εφαρμοστεί το ίδιο κλειδί). **Άρα, δεν συνίστανται σε εφαρμογές όπου υπάρχουν επαναλαμβανόμενα μοτίβα δεδομένων στο αρχικό μήνυμα**. Ένα λάθος στη λήψη επηρεάζει το συγκεκριμένο block μόνο.



- Κρυπτογράφηση για $1 \le j \le t$: $c_j = E_K(x_j)$
- Αποκρυπτογράφηση για $1 \le j \le t$: $x_j = E_K^{-1}(c_j)$

Τρόποι λειτουργίας Block Ciphers (II)

- Κρυπταλγόριθμος αλυσιδωτού τμήματος (Cipher block chaining (CBC) mode): το αρχικό μήνυμα υποβάλλεται XOR με το προηγούμενο κρυπτόγραμμα, πριν την κρυπτογράφηση. Συνεπώς, το κάθε κρυπτόγραμμα εξαρτάται από όλα τα προηγούμενα μηνύματα (άρα, δύο ίδια μοτίβα δεν οδηγούν σε ίδια κρυπτογράμματα). Λάθος κατά τη μετάδοση σε ένα απλό bit του κρυπτογράμματος (που μπορεί να οφείλεται είτε σε σφάλμα μετάδοσης είτε σε παρεμβολή ενός «επιτιθέμενου») προκαλεί λάθος σε δύο block του αποκρυπτογραφημένου κειμένου.



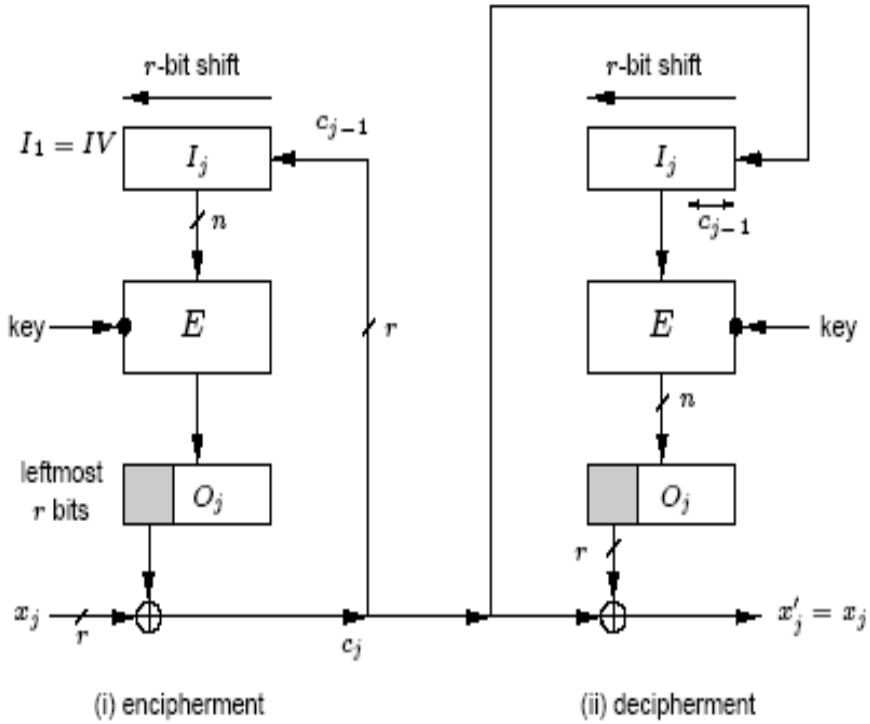
- IV: διάνυσμα αρχικοποίησης
- Κρυπτογράφηση για $1 \le j \le t$: $c_j = E_K(x_j \oplus C_{j-1})$, $C_0 = IV$
- Αποκρυπτογράφηση για $1 \le j \le t$: $x_j = E_K^{-1}(c_j) \oplus c_{j-1}$

Κρυπταλγόριθμος αλυσιδωτού τμήματος (συνέχεια)

- Είναι κρίσιμο το να ξέρουν και ο πομπός και ο δέκτης το διάνυσμα αρχικοποίησης. Αφενός μεταδίδεται από τον έναν στον άλλον κρυπτογραφημένο με ECB, αφετέρου εφαρμόζεται και συνάρτηση κατακερματισμού για έλεγχο της ακεραιότητάς του. Αν κάποιος εχθρός το μεταβάλλει κατά τη μετάδοσή του, ο παραλήπτης θα ανιχνεύσει τη μεταβολή αυτή.
- Είδαμε ήδη ότι αν συμβεί σφάλμα στη μετάδοση του κρυπτογράμματος, το σύστημα τελικά μετά από δύο λανθασμένες αποκρυπτογραφήσεις θα επανέλθει. Αυτό λέγεται ιδιότητα της αυτοεπούλωσης (self healing). Όμως, αν ο επιτιθέμενος παρεμβάλλει bits, τότε χάνεται ο συγχρονισμός και το σύστημα δεν μπορεί να τον επανακτήσει.
- **CBC κρυπτογράφηση εφαρμόζεται επίσης για λόγους πιστοποίησης ταυτότητας και εξασφάλισης της ακεραιότητας δεδομένων. Ο αποστολέας κρυπτογραφεί το μήνυμα και επισυνάπτει το τελευταίο μπλοκ του κρυπτογράμματος (που εξαρτάται από όλα τα προηγούμενα μπλοκ κρυπτογράμματος και, κατ' επέκταση, από ολόκληρο το μήνυμα) στο αρχικό μήνυμα. Ο παραλήπτης κρυπτογραφεί το μήνυμα με τον ίδιο αλγόριθμο σε CBC και ελέγχει αν το τελευταίο μπλοκ του κρυπτογράμματος που βρίσκει ταυτίζεται με το αντίστοιχο που του έστειλε ο αποστολέας.**

Τρόποι λειτουργίας Block Ciphers (III)

- Κρυπταλγόριθμος ανάδρασης (Cipher Feedback (CFB) mode): Τα δεδομένα κρυπτογραφούνται r bits τη φορά. Υπάρχει ένας καταχωρητής ολίσθησης, μεγέθους όσο το μέγεθος του μπλοκ. Κάθε χρονική στιγμή, τα περιεχόμενα του καταχωρητή ολίσθησης κρυπτογραφούνται: από το αποτέλεσμα που προκύπτει, τα r αριστερότερα bits γίνονται xor με τα r bits του μηνύματος και προκύπτουν r bits κρυπτογράμματος. Αυτά για την επόμενη χρονική στιγμή πηγαίνουν στον καταχωρητή ολίσθησης, ο οποίος για να μπορεί να τα «χωρέσει» αποβάλλει τα r αριστερότερά του bits.



Κρυπτογράφηση: I_1=IV,

$O_j = E_K(I_j)$, $1 \le j \le u$, t_j: τα r πιο αριστερά bits του O_j ,

$c_j = x_j \oplus t_j$, $I_{j+1} = 2^r I_j + c_j \bmod 2^n$

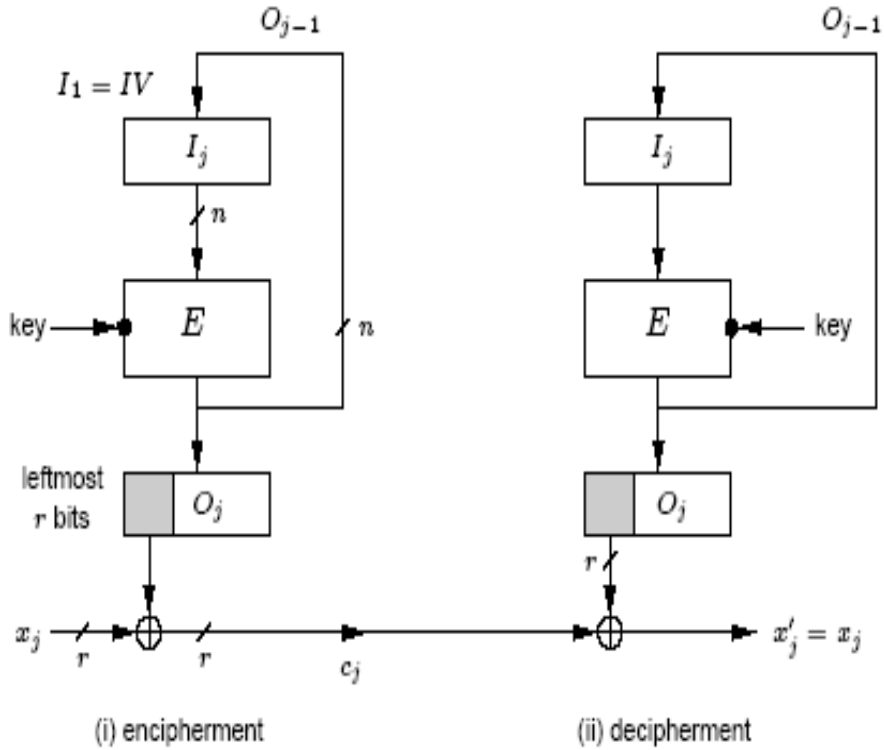
Αποκρυπτογράφηση: I_1 =IV, $x_j = c_j \oplus t_j$

Κρυπταλγόριθμος ανάδρασης (συνέχεια)

- Πέφτει η απόδοση (throughput) του συστήματος σε σχέση με το CBC κατά έναν παράγοντα n/r (όπου n το πλήθος bits του block).
- Λάθος σε ένα bit κρυπτογράμματος επηρεάζει το πολύ τις επόμενες [n/r] αποκρυπτογραφήσεις (το πολύ για [n/r] χρονικές στιγμές θα παραμείνει στον καταχωρητή το λανθασμένο bit, άρα τόσες αποκρυπτογραφήσεις θα είναι λανθασμένες).

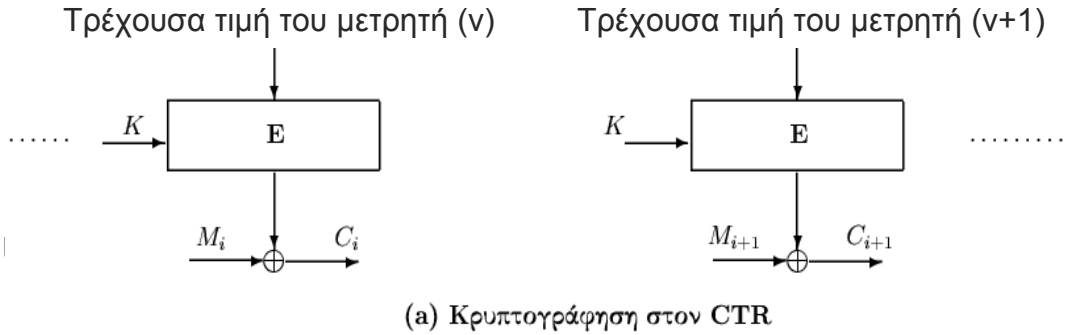
Τρόποι λειτουργίας Block Ciphers (IV)

- Ανάδραση εξόδου (Output Feedback (OFB) mode): σχεδόν ίδιο με το CFB, αλλά με έναν μηχανισμό για την μείωση των λαθών. Η έξοδος της συνάρτησης κρυπτογράφησης F (και όχι το κρυπτόγραμμα) χρησιμοποιείται στην ανάδραση. Έτσι ένα σφάλμα στο κρυπτόγραμμα επηρεάζει μόνο μία αποκρυπτογράφηση. Κατάλληλο για εφαρμογές με μεγάλο αριθμό σφαλμάτων λόγω υψηλού βαθμού θορύβου (π.χ. δορυφορικές επικοινωνίες).
- Μοιάζει πολύ σαν δομή με κρυπταλγόριθμο ροής

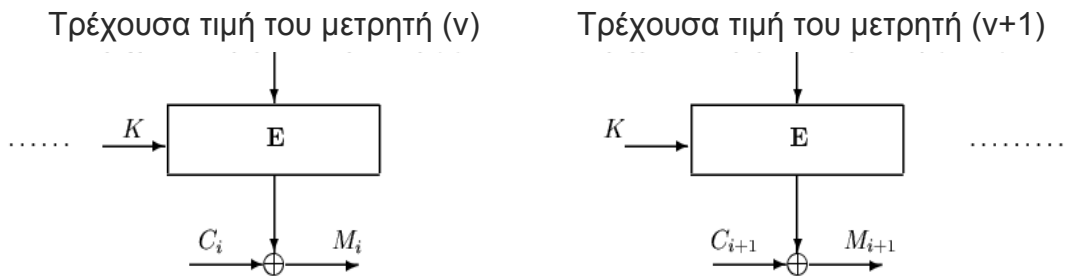


Τρόποι λειτουργίας Block Ciphers (V)

- Τρόπος λειτουργίας μετρητή (CTR - CounTeR mode): Χρησιμοποιείται μετρητής μήκους n, όπου n το μέγεθος το τμήματος του κρυπταλγορίθμου τμήματος. Ο αλγόριθμος τμήματος κρυπτογραφεί κάθε φορά το περιεχόμενο του αθροιστή, και η έξοδός του γίνεται XOR με το τμήμα του μηνύματος.
- Ο μετρητής ξεκινά τη μέτρηση από μία τυχαία αρχική τιμή (IV).



(a) Κρυπτογράφηση στον CTR



(b) Αποκρυπτογράφηση στον CTR

“Λεύκανση” (whitening)

- Είναι η τεχνική κατά την οποία πριν από έναν γύρο ενός block cipher, τόσο ένα τμήμα της εισόδου όσο κι ένα τμήμα της εξόδου γίνεται XOR με το κλειδί. Αυτό καθιστά το σύστημα πιο ασφαλές ως προς επιθέσεις γνωστού αρχικού μηνύματος (known plaintext attack).

Χαρακτηριστικά σχεδίασης block ciphers

- Στόχοι
  - Μεγάλη ταχύτητα
  - Χαμηλή κατανάλωση ισχύος
  - Εύκολη hardware υλοποίηση (απλές πράξεις)
  - Αποδοτική χρήση μνήμης
    - Να μπορεί να εφαρμοστεί σε smart card
  - Να μη χρειάζεται μεγάλη ποσότητα μυστικών πληροφοριών για να είναι ασφαλής
  - Μεγάλου μήκους κλειδί

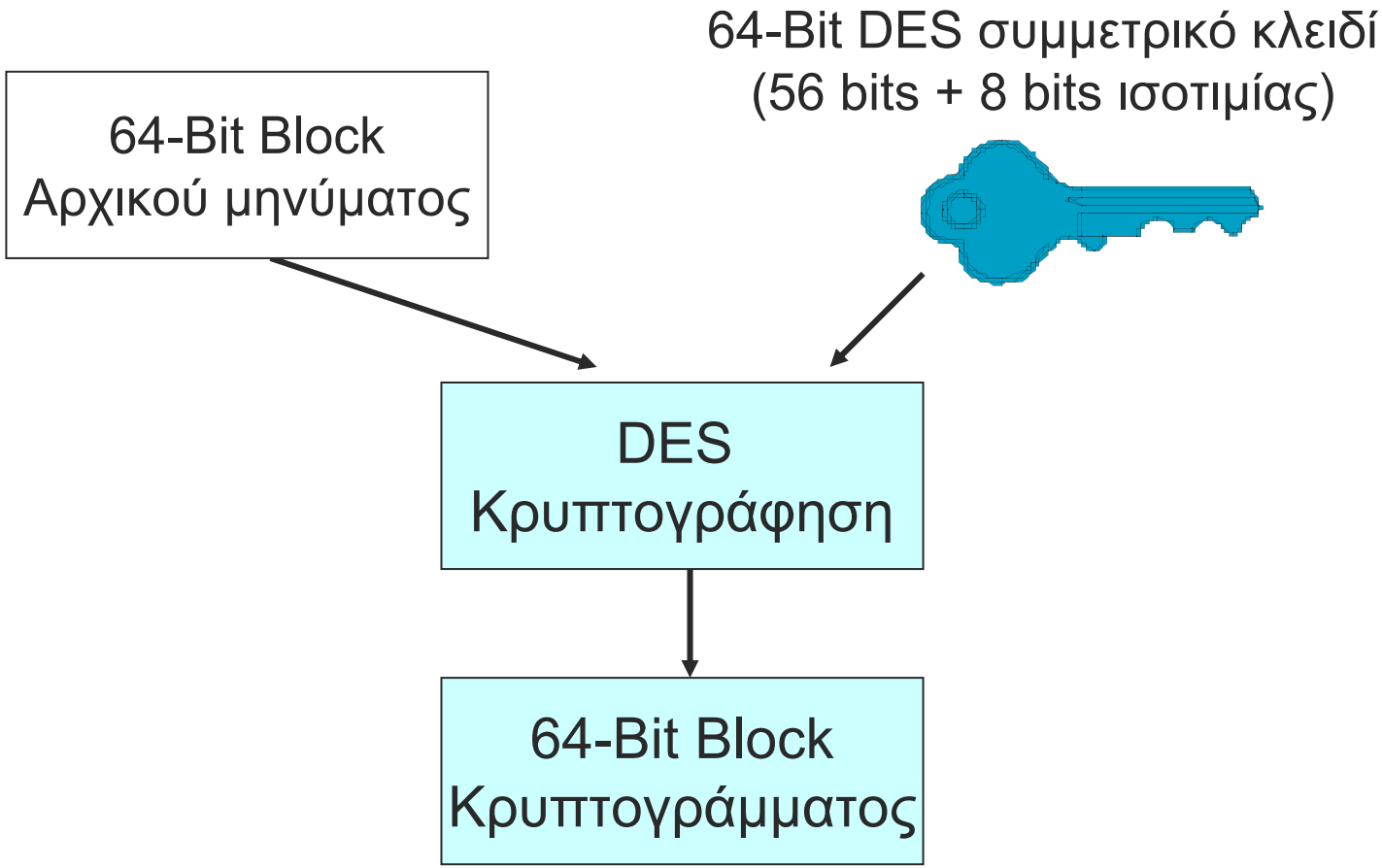
Data Encryption Standard (DES)

- Ανάγκη προτυποποίησης, για τη συνεργασία software and hardware.
- Το 1973, ο οργανισμός NIST (National Institute for Standards and Technology) έθεσε μία δημόσια πρόσκληση για προσφορές κρυπτογραφικών αλγορίθμων. Τα εξής επιθυμητά χαρακτηριστικά τέθηκαν:
  - Παροχή υψηλού επιπέδου προστασίας
  - Πλήρως και με σαφήνεια ορισμένο
  - Η ασφάλεια να έγκειται στην ύπαρξη κλειδιού
  - Διαθεσιμότητα για τον οποιονδήποτε
  - Προσαρμοστικότητα σε ποικίλες εφαρμογές
  - Οικονομική hardware υλοποίηση
  - Αποδοτικό στη χρήση
  - Αξιόπιστο (validated)
  - Δυνατότητα φορητότητας (exportable)

Data Encryption Standard (DES)

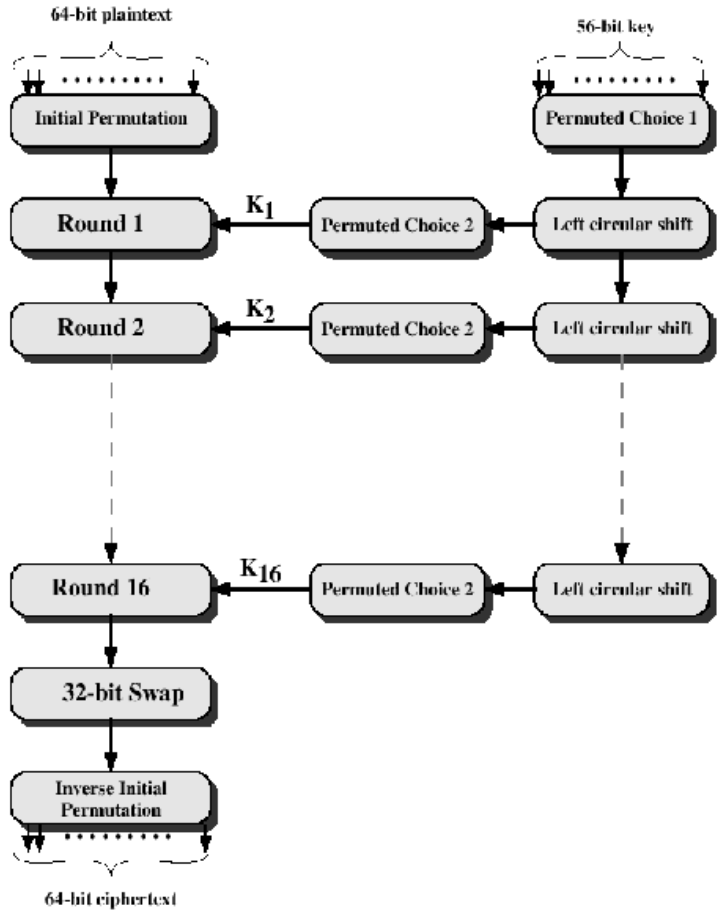
- Η βασική πρόταση ήταν ο αλγόριθμος Lucifer (IBM)
- Υπήρξαν αμφισβητήσεις ότι ο NIST «επηρέασε» τον αλγόριθμο
- Νέα πρόταση από τον NIST (1976)
- 23 Νοεμβρίου 1976: Ο DES ορίστηκε σαν καθολικό πρότυπο
- Ανανέωση της έγκρισης του DES ως πρότυπο κάθε 5 χρόνια
- Το 1987, αν και δεν είχε αποδειχτεί ενδεχόμενη μη-ασφάλειά του, άρχισαν οι πρώτες έντονες αμφισβητήσεις

Data Encryption Standard (DES)



Data Encryption Standard (DES)

- 64-bit blocks
- 56-bit κλειδί
- 16 γύροι
- Στην αρχή και στο τέλος πραγματοποιείται αλληλομετάθεση των bits)
- Το κλειδί ολισθαίνει κυκλικά σε κάθε γύρο, και 48 bits από αυτά χρησιμοποιούνται



DES (συνέχεια)

- Ένα αρχικό μπλοκ Τ υποβάλλεται πρώτα σε μία μετάθεση IP, έχοντας ως αποτέλεσμα T_0=IP(T).
  - Παράδειγμα: $t_1t_2\ldots t_{64} \rightarrow t_{58}t_{50}\ldots t_7$
- Στη συνέχεια το T_0 περνάει μέσα από 16 επαναλήψεις μίας συνάρτησης f.
- Τέλος, υποβάλλεται στην αντίστροφη μετάθεση IP^{-1} δίνοντας το τελικό κρυπτόγραμμα.

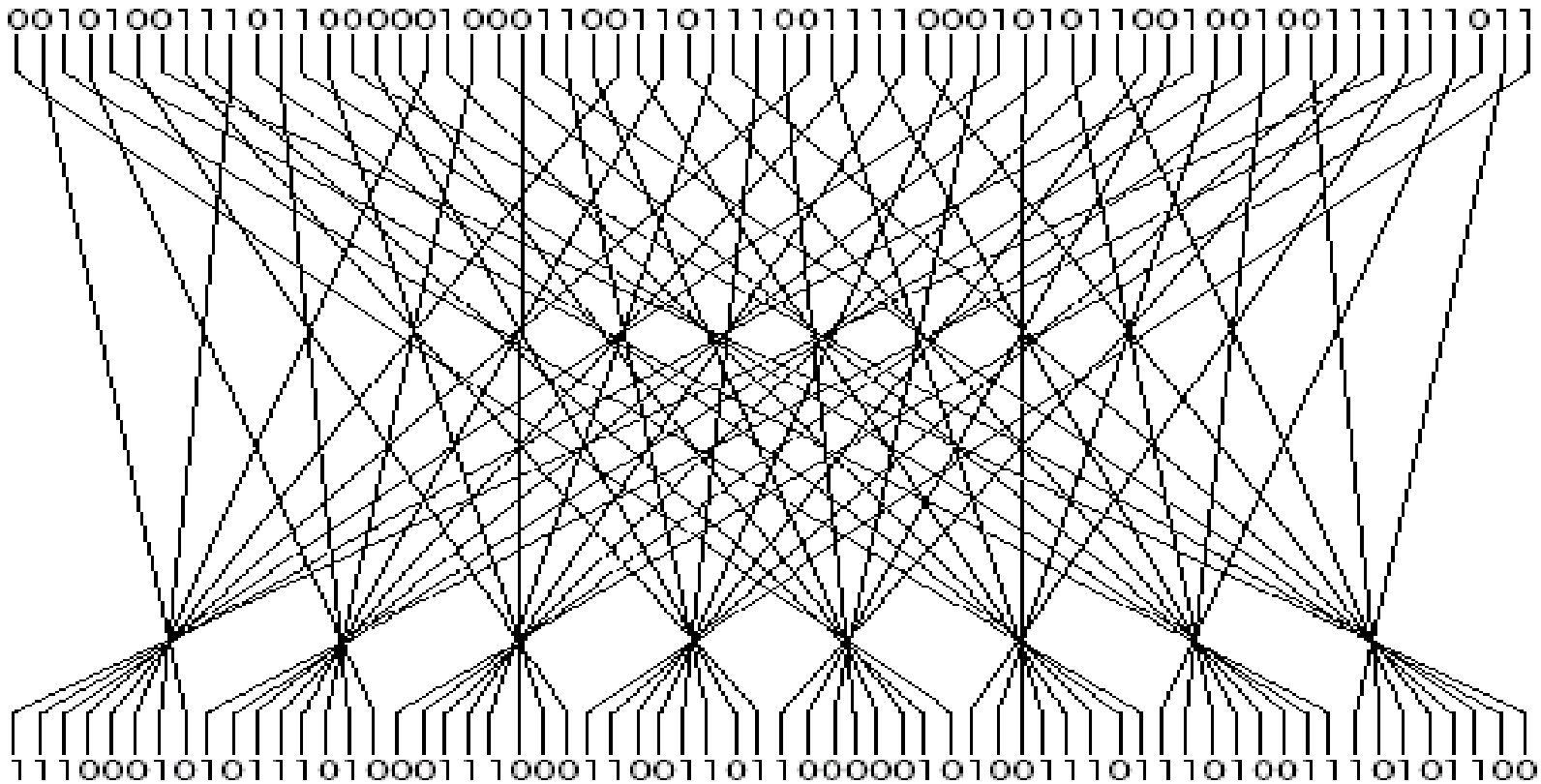
Πίνακες αρχικής μετάθεσης του DES

IP							
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

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

Το 58ο bit πηγαίνει στην πρώτη θέση, το 50ο στη δεύτερη κ.ο.κ.
Το IP^{-1} είναι ακριβώς το αντίστροφο του IP

Παράδειγμα αρχικής μετάθεσης στον DES



DES (συνέχεια)

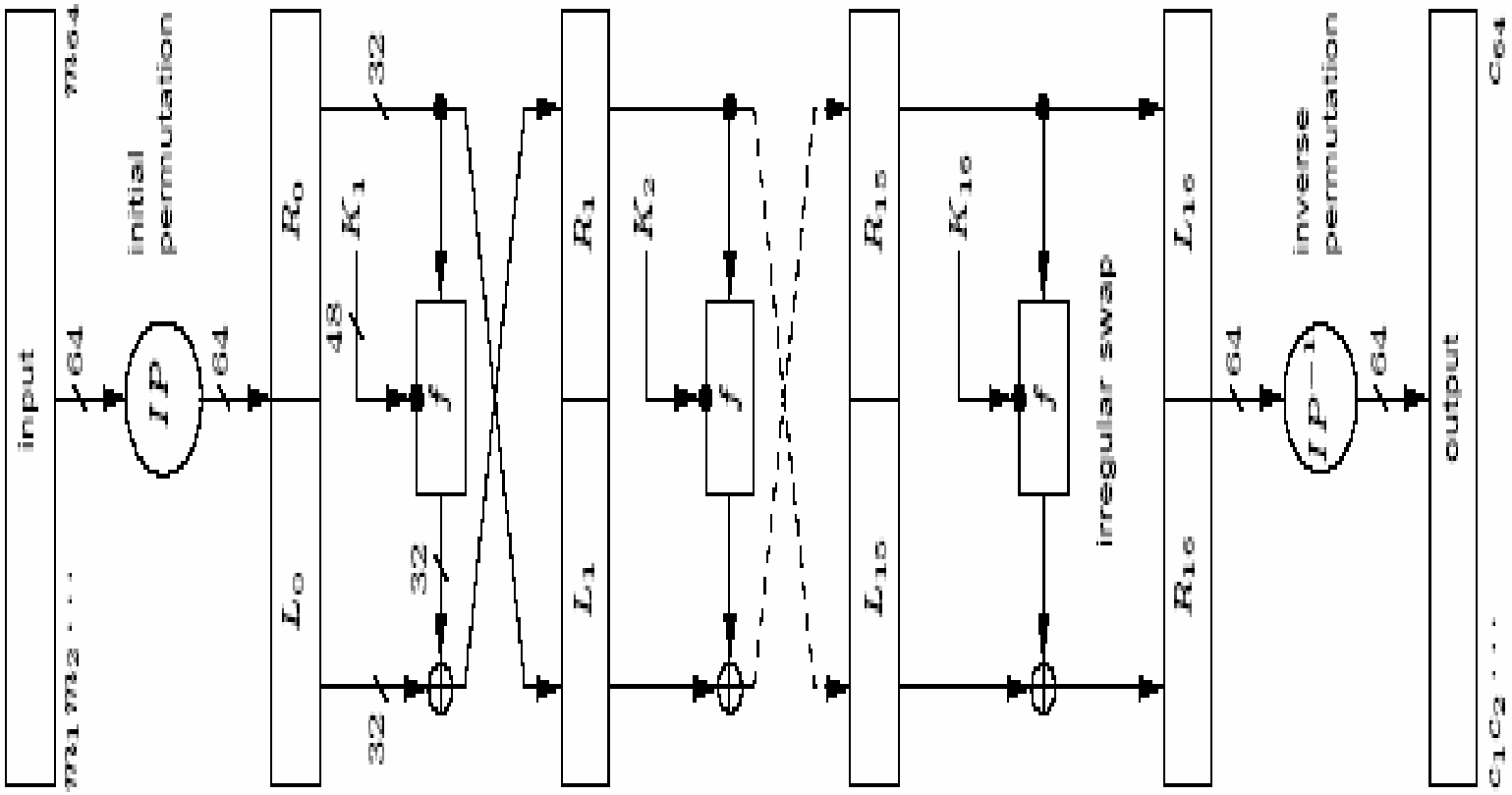
- Αν T_i συμβολίζει την έξοδο από τη i-οστή επανάληψη, και L_i,R_i συμβολίζουν το αριστερό και το δεξί μισό του T_i αντίστοιχα, τότε:

  $$L_i = R_{i-1}$$
  $$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

  όπου $\oplus$ υποδηλώνει την XOR πράξη και K είναι το 48-bit κλειδί.
- Μετά την τελευταία επανάληψη,τα δύο μισά του T_{15} δεν αλλάζουν, απλά τους εφαρμόζεται το IP^{-1}.

DES (σχηματικό διάγραμμα)

Έχει δομή δικτύου Feistel



DES (συνέχεια)

- Υπολογισμός της συνάρτησης $f(R_{i-1}, K_i)$:
  1. Χρήση ενός πίνακα επέκτασης E για τη μετατροπή του 32-bit R_{i-1} σε ένα block 48-bit $E(R_{i-1})$.
  2. Υπολογισμός του exclusive-or μεταξύ $E(R_{j-1})$ και K_i. Στη συνέχεια το αποτέλεσμα διασπάται σε 8 blocks $B_1, \ldots, B_8$ των 6 bit το καθένα.
  3. Κάθε 6-bit B_j $b_1b_2b_3b_4b_5b_6$ χρησιμοποιείται ως είσοδος σε ένα «κουτί» που υλοποιεί substitution (S-box) και επιστρέφει ένα 4-bit block $S_j(B_j)$.

     $b_1b_6 \rightarrow$ καθορίζουν τη γραμμή του S-box

     $b_2b_3b_4b_5 \rightarrow$ καθορίζουν τη στήλη του S-box
  4. Οι έξοδοι των S-boxes υποβάλλονται σε μία μετάθεση, όπως αυτή ορίζεται από έναν πίνακα μετάθεσης P.

DES – Παράδειγμα ενός γύρου (συνάρτηση f)

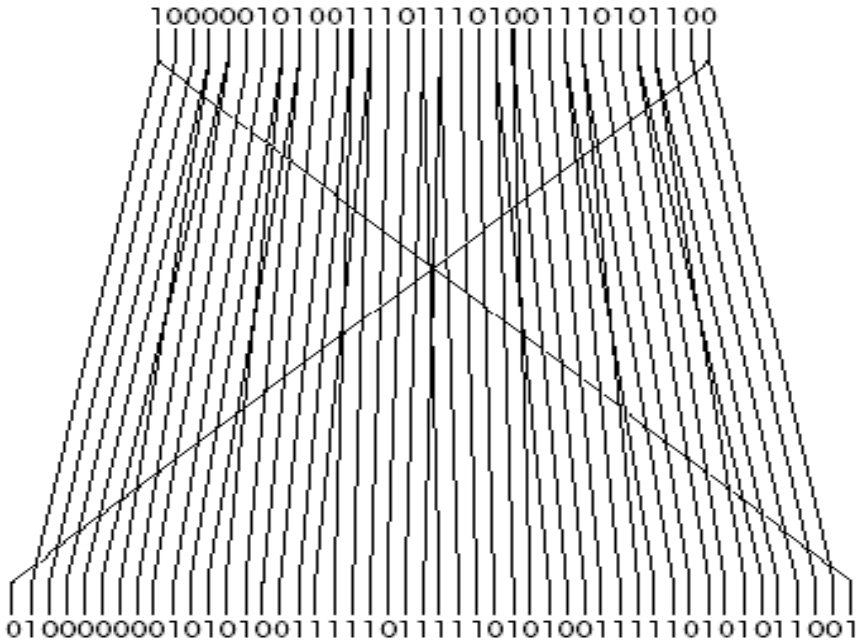
- Το 64-bit block εισόδου διαιρείται σε δύο block των 32-bit:
  - Block εισόδου (64 bits)
    - **1110001010111010001110001100110100000101001110111010011101 01100**
  - Αριστερό μισό = 11100010101110100011100011001101
  - Δεξιό μισό = 10000010100111011101001110101100
- Το δεξιό μισό υπόκειται σε μετάθεση – επέκταση, βάση του κατάλληλου πίνακα επέκτασης Ε. Προκύπτουν έτσι 48 bits, που είναι αναδιάταξη των αρχικών, ενώ κάποια εμφανίζονται σε περισσότερες από μία θέσεις.

Πίνακας Επέκτασης Ε →

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

DES – Δράση του πίνακα E

- Δεξιό μισό block (32 bits):
  - 10000010100111011101001110101100



48 bit εξόδου:

- 01000000010101001111101111101010011111010101011001

DES – XOR με το κλειδί

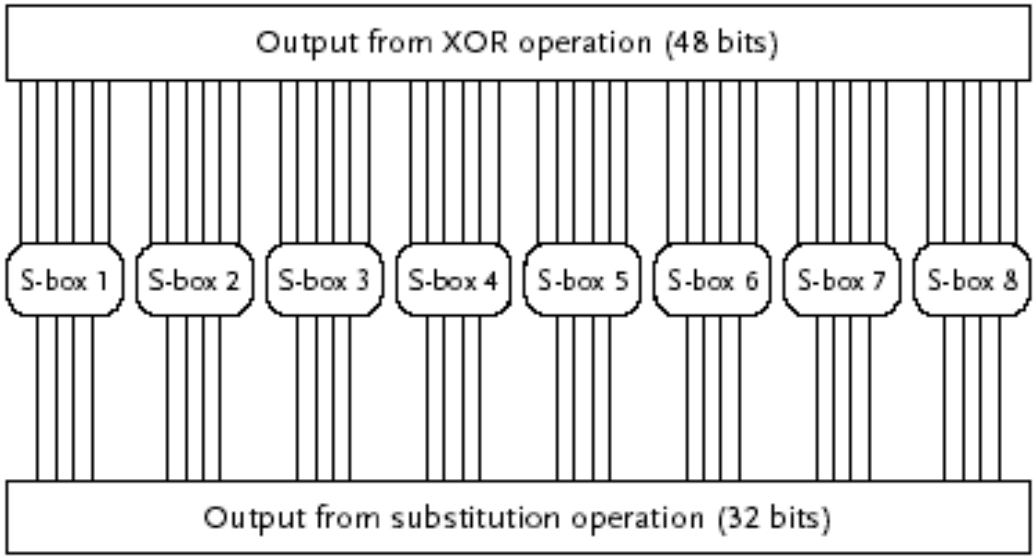
- Μία **exclusive-or** (XOR) λειτουργία πραγματοποιείται μεταξύ των 48 bit της εξόδου του πίνακα E και του τμήματος κλειδιού που αντιστοιχεί σε αυτόν τον γύρο:

```
      011000000010101001111101111110101001111101010111001  (result of expansion permutation)
XOR   100011111111001101011000001111101001110010001000   (round 1 subkey)
      ---------------------------------------------------
      110011111101100100100101110010111010001000100100 1
```

- Τα νέα 48 bits περνάνε από τα **S-boxes**

DES – S-boxes

- 8 διαφορετικά S-boxes
- Κάθε S-box έχει 6 εισόδους και παράγει 4 bits εξόδου:



- Τα bits 1-6 είναι η είσοδος στο πρώτο S-box
- Τα bits 7-12 είναι η είσοδος στο δεύτερο S-box κ.ο.κ.

DES – Λειτουργία των S-box

- Κάθε S-box έχει 4 γραμμές και 16 στήλες
- Παράδειγμα - S-box 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

- Το πρώτο και το έκτο bit από τις εισόδους ενός S-box συνιστούν ένα δυαδικό αριθμό που καθορίζει μία από τις 4 γραμμές
  - 00 για την πρώτη γραμμή, 01 για τη δεύτερη γραμμή, 10 για την τρίτη γραμμή, και 11 για την τέταρτη γραμμή
- Τα μεσαία 4 bits συνιστούν ένα δυαδικό αριθμό που καθορίζει μία από τις 16 στήλες
  - 0000 για την πρώτη στήλη, 0001 για τη δεύτερη στήλη, . . ., και 1111 για την δέκατη έκτη στήλη

DES – Λειτουργία των S-box (II)

- Παράδειγμα για το πρώτο S-box:

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

- 011010 (είσοδος) = γραμμή 1, στήλη 14 = 9 = 1001 (έξοδος)
- 110010 (είσοδος) = γραμμή 3, στήλη 10 = 12 = 1100 (έξοδος)
- 000011 (είσοδος) = γραμμή 2, στήλη 2 = 15 = 1111 (έξοδος)

DES – Τα 8 S-boxes

S-box 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-box 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-box 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

S-box 4:

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

S-box 5:

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

S-box 6:

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

S-box 7:

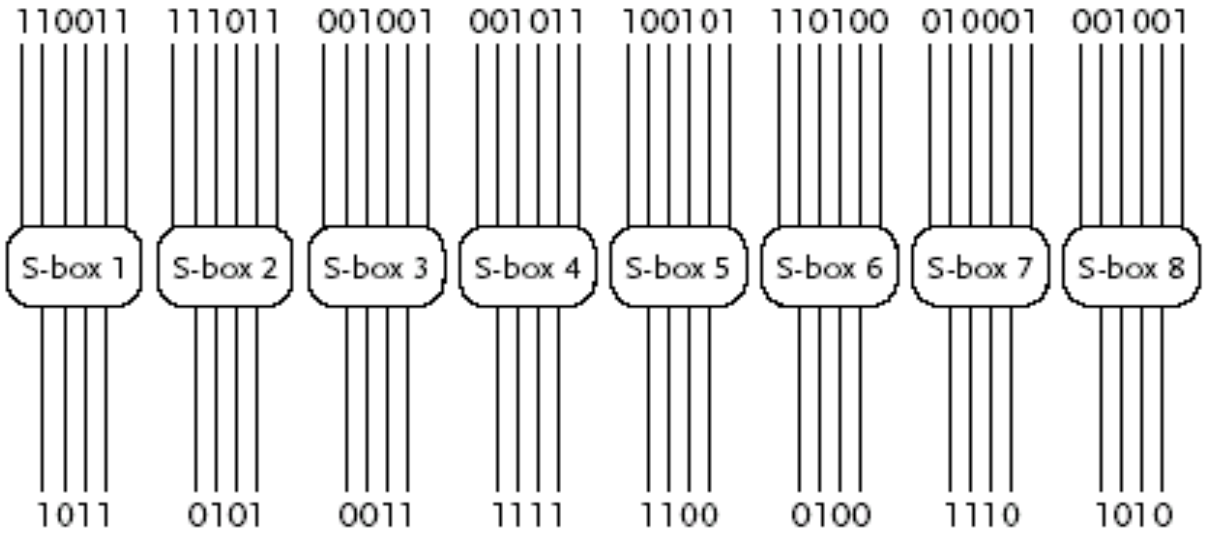
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S-box 8:

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

DES – Παράδειγμα της λειτουργίας των S-boxes

- Για τα 48 bits που έχουμε:
  - 110011111011001001001011100101110100010001001001



- 32-bit έξοδος:
  - 10110101001111111100010011101010

DES – Μετάθεση (P-box)

- Η 32-bit έξοδος από τα S-boxes περνά από ένα **P-box.** Αυτό μεταθέτει τα bits, με βάση τον πίνακα:

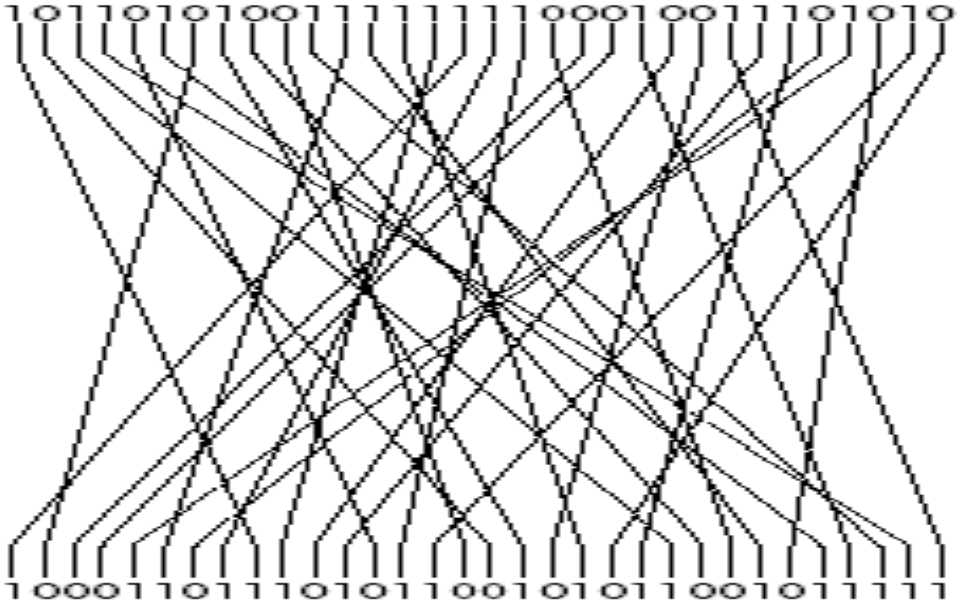
Πίνακας Μετάθεσης P

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

  - Το 1ο bit εξόδου από το P-box θα είναι το 16ο bit της εισόδου κ.ο.κ.

DES – Παράδειγμα P-box

- Για την 32-bit έξοδο των S-boxes:
  - 10110101001111111100010011101010



- Η 32-bit έξοδος από το P-box:
  - 10001101110101100101011001011111

DES – Δεύτερη XOR Λειτουργία

- Η 32-bit έξοδος από το P-box γίνεται XOR με το αριστερό μισό του αρχικού 64-bit block εισόδου:
  - Έξοδος από P-box (32 bits)
    - 10001101110101100101011001011111
  - Αριστερό μισό του block εισόδου (32 bits)
    - 11100010101110100011100011001101

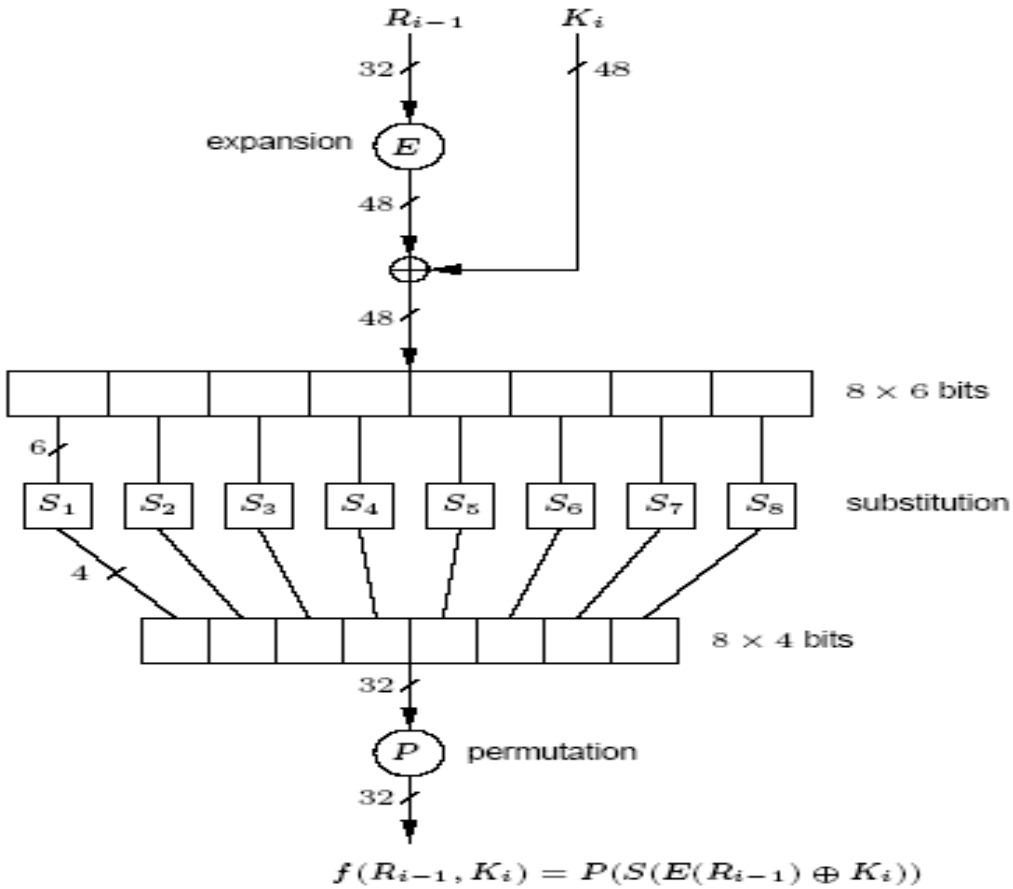
```
      10001101110101100101011001011111
XOR   11100010101110100011100011001101
      --------------------------------
      01101111011011000110111010010010
```

- Τα 32 bit αποτελέσματος :
  - 01101111011011000110111010010010

DES - Έξοδος ενός γύρου

- Το 32-bit δεξιό μισό του αρχικού μηνύματος ενώνεται με την έξοδο του δεύτερου XOR. Το αποτέλεσμα θα είναι η έξοδος του γύρου αυτού
  - Δεξιό μισό του αρχικού block (32 bits):
    - 10000010100111011101001110101100
  - Έξοδος από το δεύτερο XOR (32 bits):
    - 01101111011011000110111010010010
  - Έξοδος του γύρου (64 bits):
    - 10000010100111011101001110101100011011110110001101110010010010
- Η 64-bit έξοδος του γύρου k είναι η είσοδος στο γύρο k+1

DES (εσωτερική συνάρτηση f)



DES (υπολογισμός κλειδιού)

- Υπολογισμός κλειδιού
  - Κάθε επανάληψη i χρησιμοποιεί ένα διαφορετικό 48-bit κλειδί K_i που προέρχεται από το αρχικό κλειδί K: αυτό αποτελείται από 56 bit συν 8 bits ισοτιμίας στις θέσεις 8, 16, …, 64.
  - Το PC-1 διώχνει τα bits ισοτιμίας και αλληλομεταθέτει τα εναπομείναντα 56 bits για να προκύψει το PC-1(K).

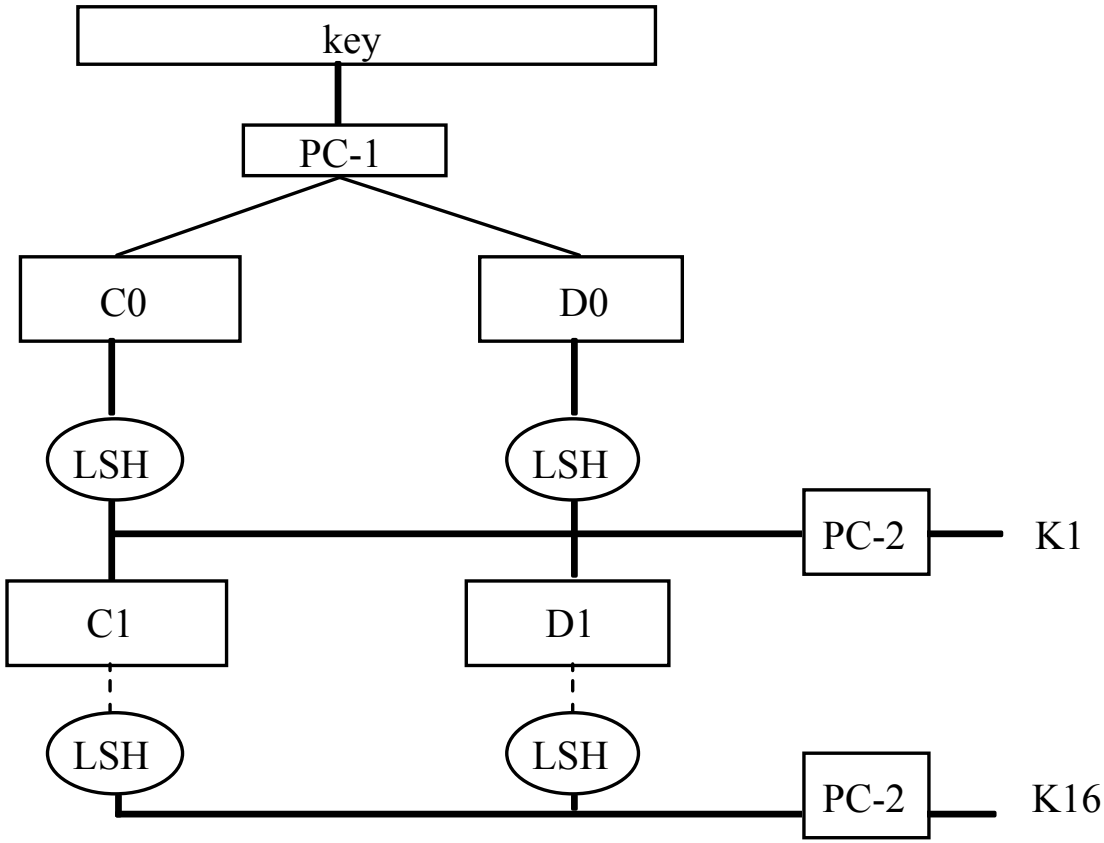
    $C_i=LS_i(C_{i-1})$, $D_i=LS_i(D_{i-1})$
  - $K_i=PC\text{-}2(C_iD_i)$.

Πίνακες PC1 και PC2 εξαγωγής του κλειδιού

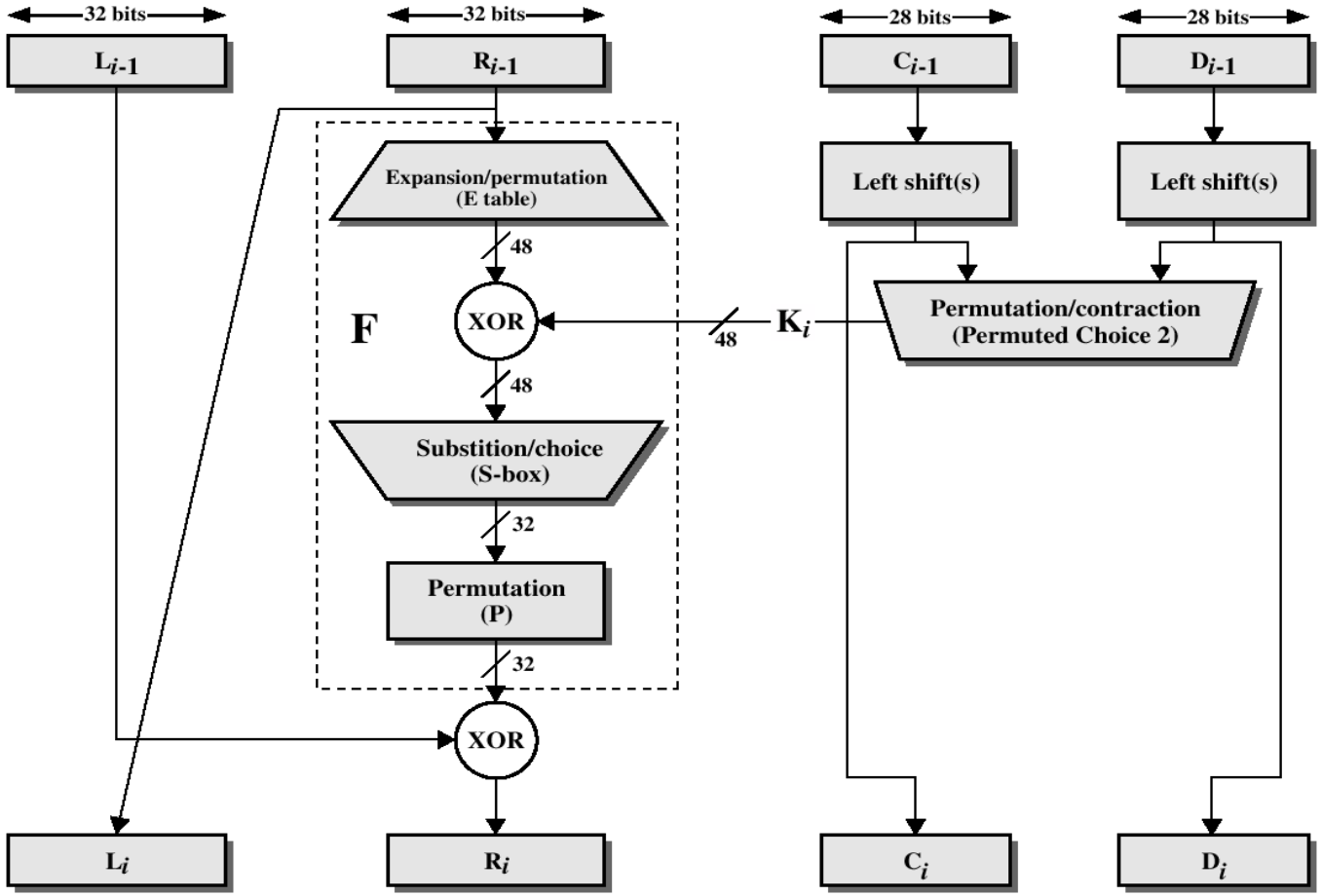
PC1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
above for C_i; below for D_i						
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

PC2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Σχηματικό διάγραμμα δημιουργίας κλειδιού στον DES



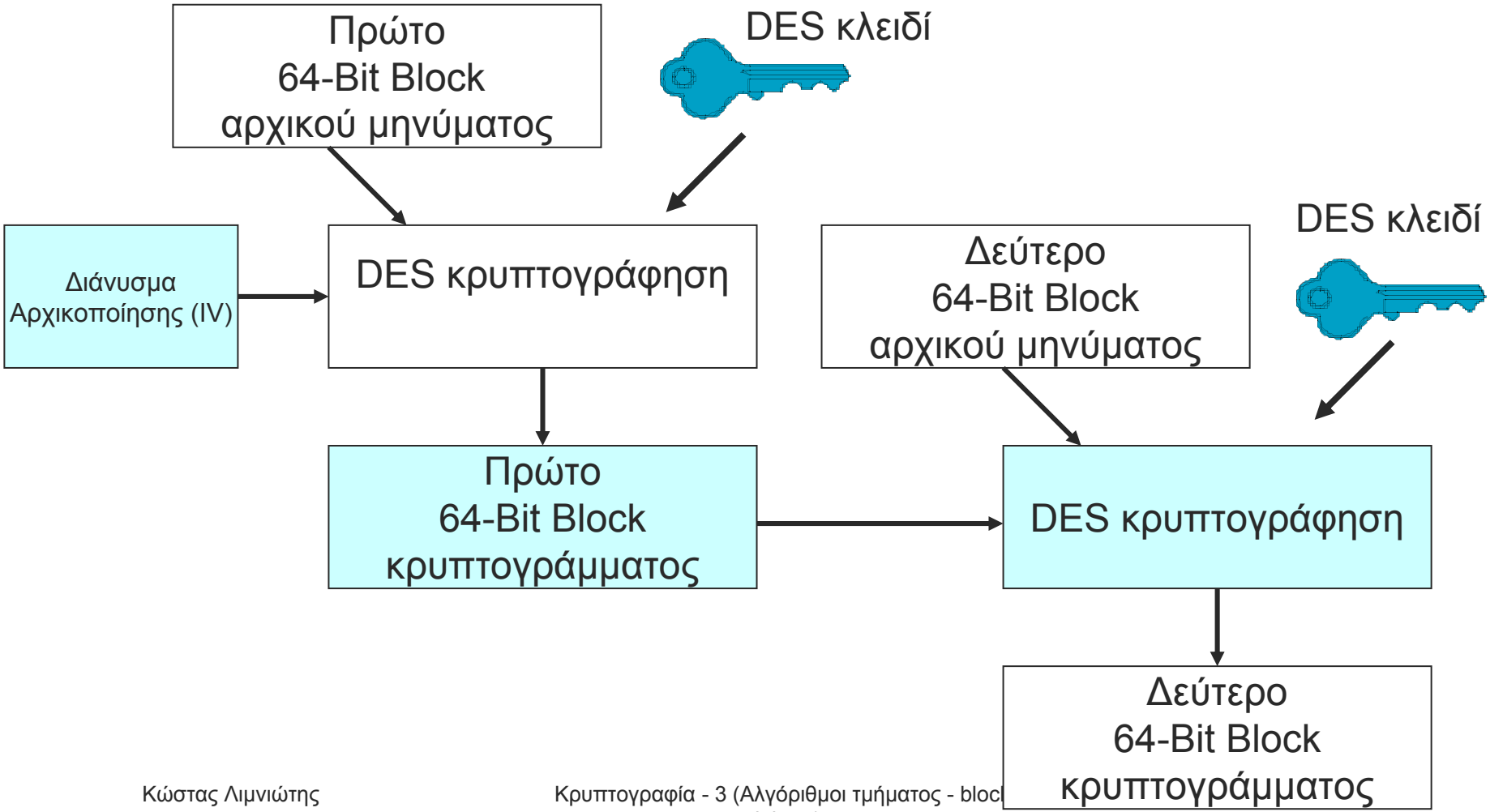
Ένας γύρος στον DES (σύνοψη)



DES (συνέχεια)

- Αποκρυπτογράφηση
  - Ο ίδιος αλγόριθμος χρησιμοποιείται, εκτός του ότι αντιστρέφεται η σειρά χρησιμοποίησης των κλειδιών κάθε γύρου. Έτσι, το K_{16} χρησιμοποιείται στην πρώτη επανάληψη, το K_{15} στη δεύτερη κ.ο.κ.
- Τρόποι λειτουργίας: ECB, CBC

DES-CBC
(DES-Cipher Block Chaining)



Χαρακτηριστικά του DES που προάγουν ασφάλεια

- Η επέκταση του R_i από 32 σε 48 bits (όσο το μέγεθος του κλειδιού) προκαλεί διάχυση (diffusion) – κάποια bits εμφανίζονται 2 φορές
- Τα S-boxes έχουν επιλεγεί έτσι ώστε να είναι ισχυρά μη γραμμικά

Ανεπιθύμητα χαρακτηριστικά του DES

- 4 μη ασφαλή κλειδιά
  (π.χ. 00….011…1)

- 12 ημι-ανασφαλή (semi-weak) κλειδιά
  (ζευγάρια κλειδιών που οδηγούν στο ίδιο κρυπτόγραμμα ένα δεδομένο αρχικό μήνυμα)

- Συμπληρωματική ιδιότητα
  - $DES_k(m) = c \Rightarrow DES_{k'}(m') = c'$

- Κάποιες όχι καλές ιδιότητες των S-boxes
  - Όχι τυχαία κατανομή μονών και ζυγών αριθμών
  - Ο NIST άλλαξε τα S-boxes που είχε προτείνει αρχικά η ομάδα σχεδίασης του DES, και αυτό πάντα γεννούσε ερωτηματικά.

Κρυπτανάλυση στον DES

- Όντας πρότυπο για πολλά χρόνια, ο DES κίνησε το ενδιαφέρον πολλών κρυπταναλυτών για την εύρεση μεθόδων που θα μπορούσαν να τον «σπάσουν»
- Βασικοί 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

Διαφορική Κρυπτανάλυση

- Εξετάζει ζεύγη κρυπτογραμμάτων, των οποίων τα αρχικά μηνύματα διαφέρουν σε συγκεκριμένες θέσεις (chosen-plaintext attack)
- Προσομοιώνοντας τον αλγόριθμο, κάποια κλειδιά είναι πιο πιθανά από κάποια άλλα, με δεδομένη την παραπάνω συνθήκη
- Όσο πιο πολλά κρυπτογράμματα αναλύονται, τόσο πιο πολλά κλειδιά «απορρίπτονται» ως λιγότερο πιθανά
- Οι λεπτομέρειες της μεθόδου πολύ σύνθετες
- Οι 8 γύροι του DES «σπάνε» με γνωστά 2^{14} επιλεγμένα αρχικά μηνύματα (chosen plaintexts). Όλοι οι 16 γύροι του DES όμως χρειάζονται 2^{47} επιλεγμένα αρχικά μηνύματα

Αναφορά: «Differential Cryptanalysis of DES-like cryptosystems», E. Biham, A. Shamir, Crypto 1990

Γραμμική Κρυπτανάλυση

- Αναζητείται γραμμικότητα στο σύστημα
- Έστω ότι γίνονται XOR τα bits ενός αρχικού μηνύματος, XOR τα bits του αντίστοιχου κρυπτογράμματος και XOR τα δύο αποτελέσματα. Ιδανικά, η πιθανότητα αυτού του bit αποτελέσματος να είναι 1 ή 0 θα έπρεπε να είναι ½. Όταν δεν ισχύει, μπορεί να εξαχθεί κάποια πληροφορία για το κλειδί
- Η παραπάνω πιθανότητα εξαρτάται κύρια από τη γραμμικότητα των S-boxes
- Οι λεπτομέρειες της μεθόδου είναι επίσης σύνθετες
- Καλά αποτελέσματα για λίγους γύρους του DES, όχι όμως για το σύνολό του (όπου χρειάζονται 2^{43} επιλεγμένα γνωστά αρχικά μηνύματα)
- Σε αντίθεση με τη διαφορική, για τη γραμμική κρυπτανάλυση ειπώθηκε ότι δεν είχε ληφθεί υπ' όψιν στη σχεδίαση του DES

  Αναφορά: «Linear Cryptanalysis Method for DES Cipher», Matsui M., *Advances in Cryptology -- EUROCRYPT '93.* 386-397.

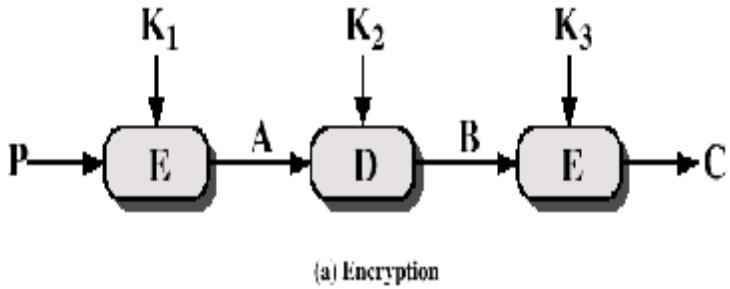
Σήμερα : ο DES μη ασφαλής

- Το 1996, διεθνής διάλογος άρχισε για την ασφάλεια του DES.
- Electronic Frontier Foundation DES Cracker project

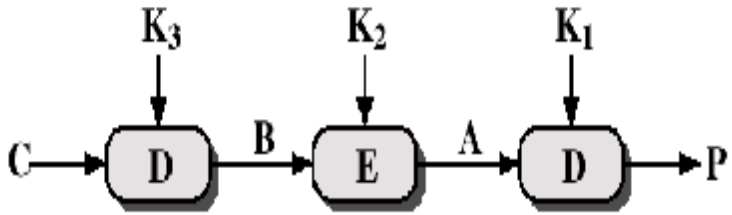
  Αποτελέσματα
  - 8-byte known plaintext attack σε λιγότερο από μία εβδομάδα
  - 16-byte known ciphertext στον ίδιο χρόνο
  - … τα παραπάνω σε 40 MHz chips…
- Το 1998, μία ειδικά σχεδιασμένη μηχανή, κόστους $250,000, τον «έσπασε» σε 56 ώρες
  - Έλεγχος 90 δισεκατομμυρίων κλειδιών το δευτερόλεπτο
- Το 1999, έσπασε σε 22 ώρες (με έλεγχο 245 δισεκατομμυρίων κλειδιών το δευτερόλεπτο).

Triple DES (3DES)

- Παραλλαγή του DES, η οποία παρέχει περισσότερη ασφάλεια
- Ο 3DES χρησιμοποιεί τρία 56-bit κλειδιά
  - $C=E_{k3}(D_{k2}(E_{k1}(P)))$
  - $P=D_{k1}(E_{k2}(D_{k3}(C)))$
- Σημείωση: αν K1=K2, τότε 3DES=DES
- Το μεσαίο στάδιο επιτελεί αποκρυπτογράφηση και όχι κρυπτογράφηση, προκειμένου να μπορεί ο 3DES να αποκρυπτογραφεί μηνύματα που έχουν κρυπτογραφηθεί με τον απλό DES (πώς??)



(a) Encryption



(b) Decryption

AES- Advanced Encryption Standard

- Το 1997, ο NIST προσκάλεσε δημόσια για ορισμό νέου προτύπου
  - Ως ελάχιστο μήκος κλειδιού τέθηκε 128 bits
  - Δυνατότητα υλοποίησης σε επεξεργαστές 8 bit
- Το 1998, επελέχθησαν 15 επικρατέστεροι
- Αργότερα, έμειναν 5 επικρατέστεροι
  - MARS (IBM - ΗΠΑ)
  - RC6 (RSA Labs - ΗΠΑ)
  - Rijndael (**Rij**men & **Dae**men – Βέλγιο)
  - SERPENT (Anderson, Biham, and Knudsen – Μεγάλη Βρετανία, Ισραήλ, Νορβηγία)
  - TWOFISH (Schneier, Kelsey, και άλλοι - ΗΠΑ)

Advanced Encryption Standard (AES) (II)

- Τελικοί βαθμοί των 5 επικρατέστερων αλγορίθμων:

	MARS	RC6	Rijndael	Serpent	Twofish
General Security	3	2	2	3	3
Implementation of Security	1	1	3	3	2
Software Performance	2	2	3	1	1
Smart Card Performance	1	1	3	3	2
Hardware Performance	1	2	3	3	2
Design Features	2	1	2	1	3

Τον Οκτώβρη του 2000, ανακοινώθηκε ως νικητής ο αλγόριθμος Rijndael.

Αλγόριθμος Rijndael

- Μήκη κλειδιού 128, 192, 256 bits
- Μήκη blocks δεδομένων 128, 192, 256 bits
- Εύκολη υλοποίηση hardware

- 10-15 γύροι, ανάλογα με το μήκος του κλειδιού
- Κάθε γύρος έχει 4 βήματα:
  - Αντικατάσταση byte (Byte substitution) – χρήση s-boxes με καλά χαρακτηριστικά
  - Ολίσθηση (Shift row)
  - Συνδυασμός πολλών bit (Mix Column)
  - Πρόσθεση (XOR) του κλειδιού

Παράμετροι του AES

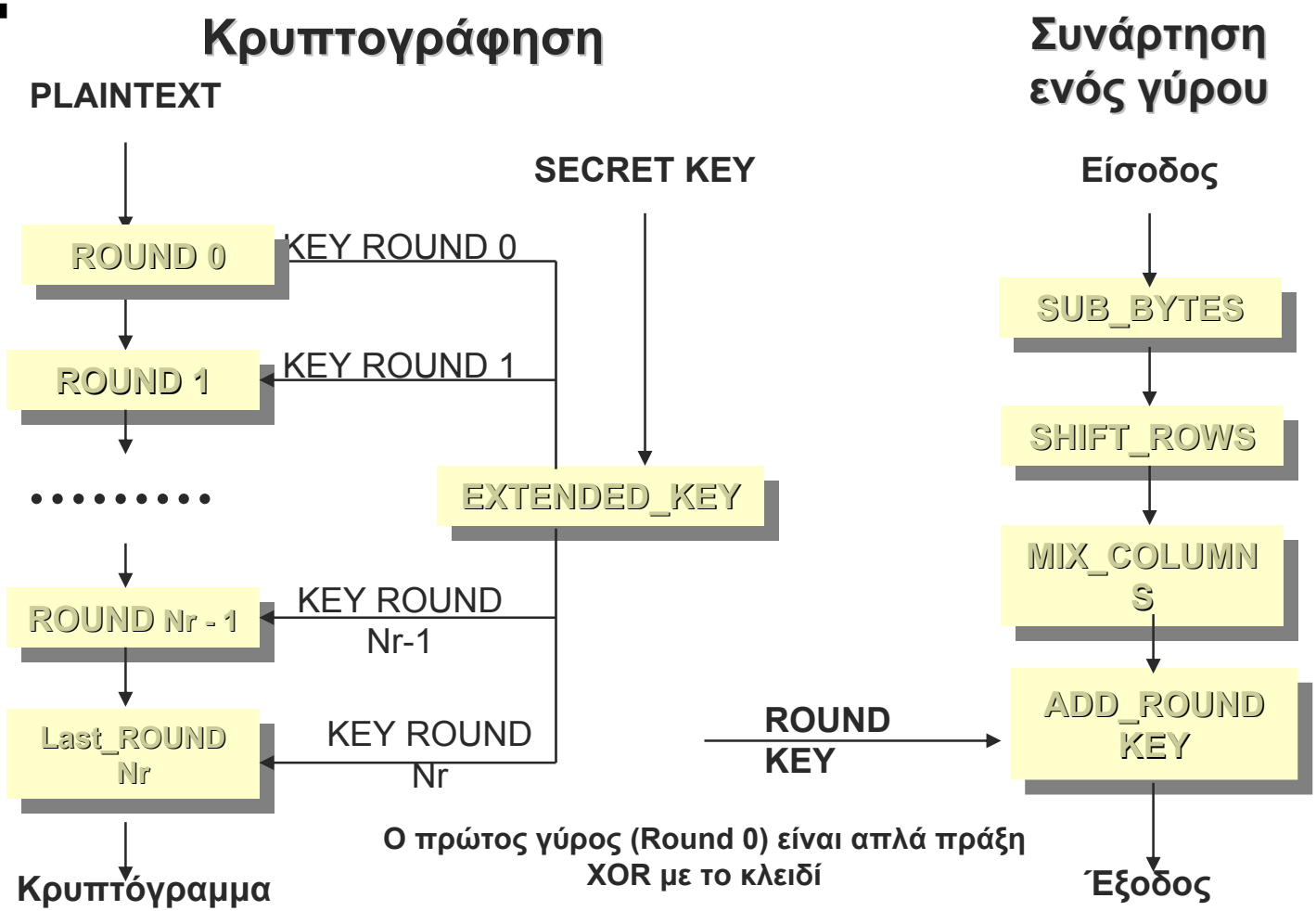
- Μεγέθη μπλοκ:128, 192, 256 bit (B)
- Μεγέθη κλειδιού: 128, 192, 256 bit (K)
- Για μήκος 128 bits: το κάθε μπλοκ θεωρείται σαν ένας 4 x 4 πίνακας, όπου κάθε στοιχείο του πίνακα είναι 1 byte.
- Ο αλγόριθμος αποτελείται από έναν αρχικό γύρο, και άλλους r - 1 τυπικούς γύρους (όπου το r είναι είτε 10 είτε 12 είτε 14 αναλόγως τα μήκη των μπλοκ), καθώς επίσης και από έναν τελευταίο γύρο.

Πλήθος γύρων στον AES

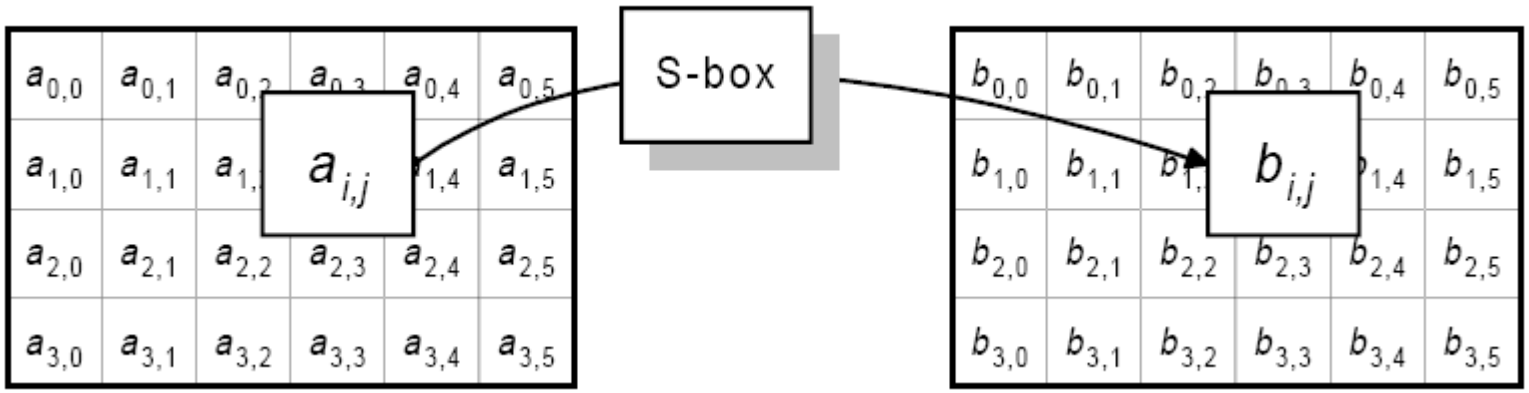
- Nb = πλήθος στηλών στον μπλοκ πίνακα
- Nk = πλήθος στηλών στον πίνακα κλειδιού

	Nb = 4	Nb = 6	Nb = 8
Nk = 4	10	12	14
Nk = 6	12	12	14
Nk = 8	14	14	14

Σχηματικό διάγραμμα του AES



S-Box (Sub_bytes)



•Κάθε byte a_{ij} μετατρέπεται σε ένα νέο, μέσω μιας μη γραμμικής συνάρτησης.

•**Είναι το μόνο τμήμα του αλγορίθμου που είναι μη γραμμικό, συνεπώς αυτό που καθορίζει σε μεγάλο βαθμό την ασφάλεια.**

•*Οι λεπτομέρειες του συγκεκριμένου S-box βασίζονται σε ιδιότητες των πεπερασμένων σωμάτων (δεν θα μελετηθούν εδώ)*

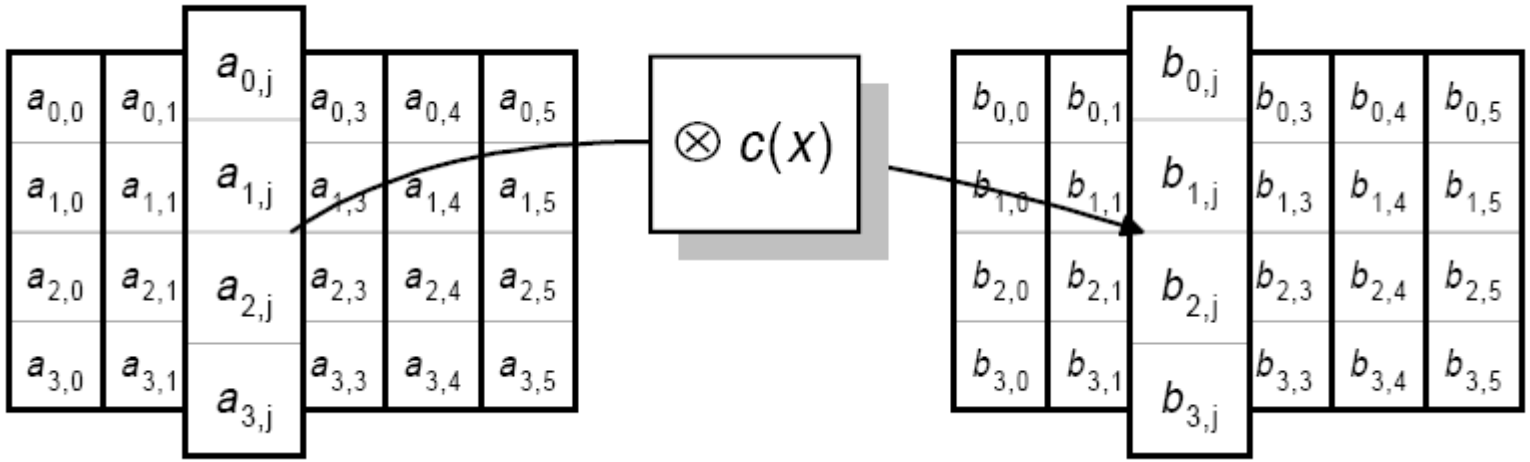
Ολίσθηση γραμμών (Shift_Rows)

State [0,0]	State [0,1]	State [0,2]	State [0,3]
State [1,0]	State [1,1]	State [1,2]	State [1,3]
State [2,0]	State [2,1]	State [2,2]	State [2,3]
State [3,0]	State [3,1]	State [3,2]	State [3,3]

Shift_Rows(..)

State[0,0]	State[0,1]	State[0,2]	State[0,3]
State[1,1]	State[1,2]	State[1,3]	State[1,0]
State[2,2]	State[2,3]	State[2,0]	State[2,1]
State[3,3]	State[3,0]	State[3,1]	State[3,2]

Ανακάτωμα στηλών (MixColumn)



- Πολλαπλασιασμός με έναν κατάλληλο (πάντα σταθερό και συγκεκριμένο) πίνακα C διαστάσεων 4x4 (όπου κάθε στοιχείο του C είναι 1 Byte).
- Η MixColumn πράξη είναι αυτή η οποία δεν συντελείται στον τελευταίο γύρο του AES. (Κατά τα άλλα, ο τελευταίος γύρος είναι ίδιος με τους υπόλοιπους)

Αποκρυπτογράφηση

- Ίδια με την κρυπτογράφηση, απλά όλα τα βήματα γίνονται αντίστροφα (π.χ. η ολίσθηση γραμμών είναι δεξιά αντί για αριστερή κ.ο.κ.)

Συγκριτικό στοιχείο

- Αν υπήρχε μηχανή που, με εξαντλητική αναζήτηση κλειδιών, να έσπαγε τον DES σε 1 δευτερόλεπτο, τότε αυτή η μηχανή θα χρειαζόταν 128 τρισεκατομμύρια χρόνια για να σπάσει τον AES με μήκος κλειδιού 128 bit.

Σύγκριση DES, 3DES, AES

	DES	3DES	AES
Key Length (bits)	56	112 or 168	128, 192, 256
Strength	Weak	Strong	Strong
Processing Requirements	Moderate	High	Modest
RAM Requirements	Moderate	High	Modest

Άλλοι Block Ciphers

- Blowfish (Schneier) (http://www.schneier.com/blowfish.html)
- CAST (http://adonis.ee.queensu.ca:8000/cast/)
- Int'l Data Encryption Alg (IDEA), Lai and Masey (http://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm)
- Safer (Secure and Fast Encryption Routine) (http://home.ecn.ab.ca/~jsavard/crypto/co040301.htm)
- RC5 (http://www.funet.fi/pub/crypt/cryptography/papers/rc5/)
- …και πληθώρα άλλων