ΕΠΛ 674: Εργαστήριο 2
Ο απλοποιημένος αλγόριθμος κρυπτογράφησης S-DES

University of Cyprus
Department of
Computer Science

NETworks Research Laboratory

Παύλος Αντωνίου

Εαρινό Εξάμηνο 2011

S-DES → Γενικά (1)

University of Cyprus

- Ο απλοποιημένος συμμετρικός αλγόριθμος S-DES.
  - Ο S-DES παίρνει σαν είσοδο ένα 8-bit απλό κείμενο και ένα κλειδί 10-bit και παράγει ένα 8-bit κρυπτογράφημα σαν έξοδο:
    - Είσοδος: 01001110
    - Κλειδί: 0101110001
    - Έξοδος: 00110100

S-DES → Γενικά (2)

University of Cyprus

- Ο S-DES εσωκλείει 5 συναρτήσεις για τη διαδικασία κρυπτογράφησης:
  - Συνάρτηση1: αρχική αντιμετάθεση (initial permutation, IP).
  - Συνάρτηση2: σύνθετη συνάρτηση f_K (περιλαμβάνει αντιμετάθεση και αλλαγή και εξαρτάται από το κλειδί εισόδου).
  - Συνάρτηση3: απλή συνάρτηση αντιμετάθεσης των δύο μισών εισόδου (switch, SW).
  - Συνάρτηση4: τη σύνθετη συνάρτηση f_K και πάλι.
  - Συνάρτηση5: τελική αντιμετάθεση, που είναι η αντίστροφη της αρχικής αντιμετάθεσης (IP^{-1}).

S-DES → Γενικά (3)

University of Cyprus

- Ο S-DES εσωκλείει 5 βήματα για την παραγωγή των δύο υποκλειδιών:
  - Βήμα1: Αντιμετάθεση P_{10}.
  - Βήμα2: Αριστερή ολίσθηση LS-1.
  - Βήμα3: Αντιμετάθεση P_8.
  - Βήμα4: Διπλή αριστερή ολίσθηση LS-2.
  - Βήμα5: Αντιμετάθεση P_8 (ξανά).

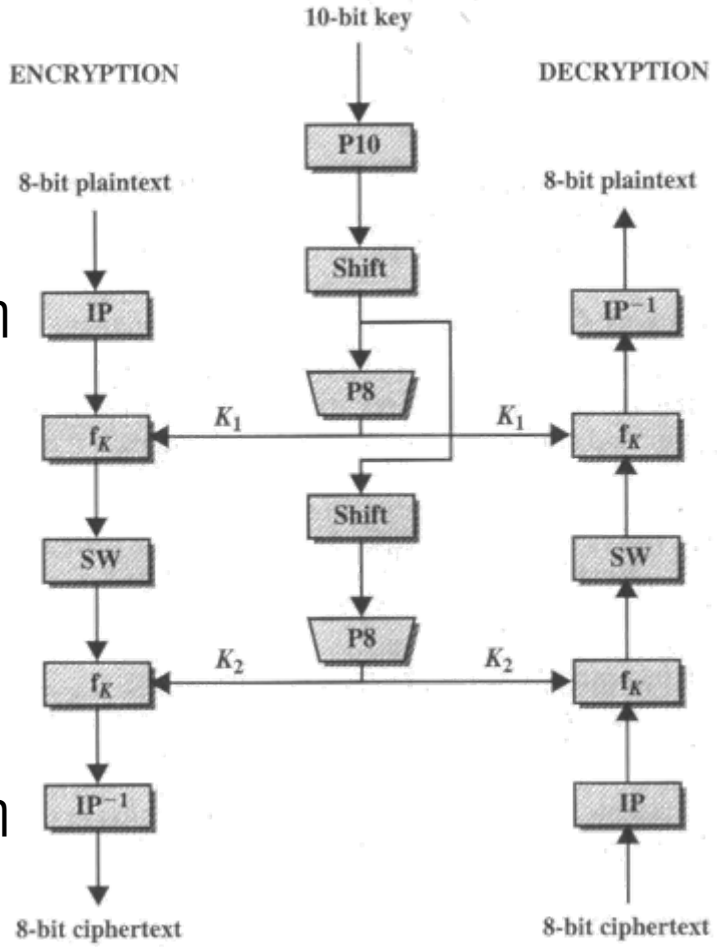
S-DES → Γενικά (4)

- Σχηματικά:

αρχική αντιμετάθεση

απλή συνάρτηση αντιμετάθεσης των δύο μισών εισόδου

τελική αντιμετάθεση



S-DES → Γενικά (5)

University of Cyprus

- Παρατηρήσεις:
  - Οι διαδικασίες P_8 και P_{10} είναι απλές αντιμεταθέσεις.
  - Είναι φανερό ότι από το γράφημα χρησιμοποιούνται δύο κλειδιά, το κλειδί K_1 και το κλειδί K_2, τα οποία προκύπτουν από το αρχικό κλειδί K.
  - Το αρχικό κλειδί K έχει εύρος 10-bit, ενώ τα υποκλειδιά K_1 και K_2 έχουν εύρος 8-bit το καθένα.
  - Η κρυπτογράφηση τροφοδοτείται πρώτα με το υποκλειδί K_1 και στη συνέχεια με το υποκλειδί K_2.

S-DES → Γενικά (6)

University of Cyprus

- Η κρυπτογράφηση μπορεί να εκφραστεί ως εξής:
  - c = κρυπτογράφημα.
  - m = απλό κείμενο.
  - $c = IP^{-1}(f_{K2}(SW(f_{K1}(IP(m)))))$.
    - Η παραγωγή των υποκλειδιών αναλύεται:

      $K_1 = P8(Shift(P10(K)))$.

      $K_2 = P8(Shift(Shift(P10(K))))$.

S-DES → Γενικά (7)

University of Cyprus

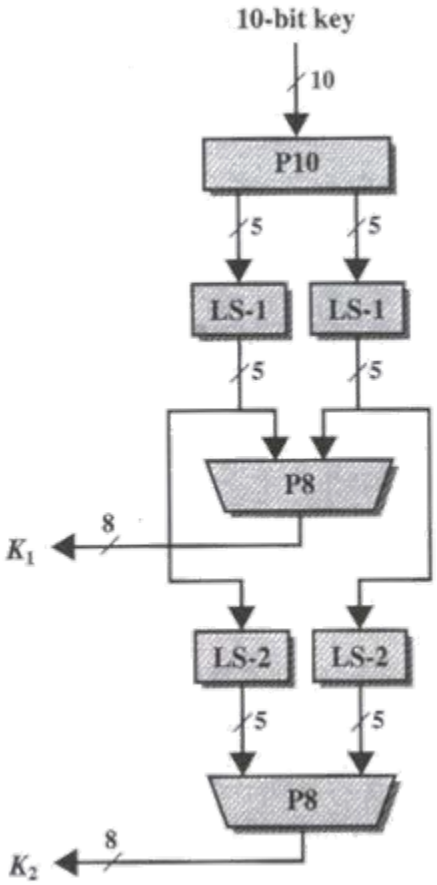
- Η αποκρυπτογράφηση μπορεί να εκφραστεί ως εξής:
  - c = κρυπτογράφημα.
  - m = απλό κείμενο.
  - $m = IP^{-1}(f_{K1}(SW(f_{K2}(IP(c)))))$.
    - Η παραγωγή των υποκλειδιών αναλύεται:

      K_1 = P8(Shift(P10(K))).

      K_2 = P8(Shift(Shift(P10(K)))).

S-DES → Παραγωγή υποκλειδιών (1)

- Η παραγωγή του κλειδιού εμπεριέχει μία σειρά από στάδια όπου σχηματίζονται τα υποκλειδιά K_1 και K_2.



LS-1: Αριστερή ολίσθηση κατά 1 bit

S-DES → Παραγωγή υποκλειδιών (2)

University of Cyprus

- Έάν θεωρήσουμε ότι το 10-bit κλειδί έχει την ακόλουθη μορφή:
  - $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10})$
- Μετά την αντιμετάθεση της συνάρτησης P_{10} το κλειδί αλλάζει μορφή:
  - $(k_3, k_5, k_2, k_7, k_4, k_{10}, k_1, k_9, k_8, k_6)$
  - Αφού η αντιμετάθεση της συνάρτησης P_{10} έχει ως εξής:

P10

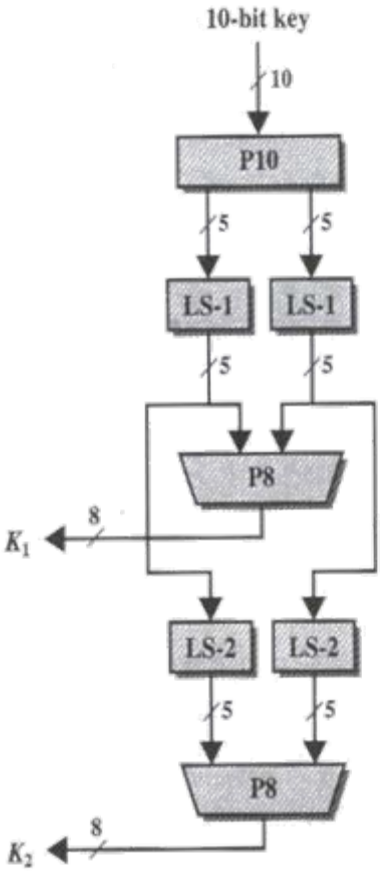
3 5 2 7 4 10 1 9 8 6

S-DES → Παραγωγή υποκλειδιών (3)

University of Cyprus

- Παράδειγμα:
  - Το κλειδί K πριν την εφαρμογή της P_{10}:
    - 1010000010
  - Το κλειδί K μετά την εφαρμογή της P_{10}:
    - 1000001100

Παραγωγή υποκλειδιών



S-DES → Παραγωγή υποκλειδιών (4)

University of Cyprus

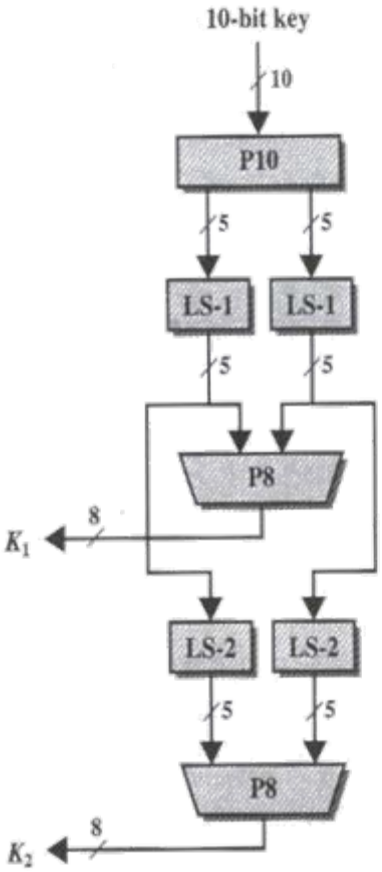
- Στη συνέχεια το κλειδί διαχωρίζεται στη μέση και στο κάθε κομμάτι ξεχωριστά εφαρμόζεται η ολίσθηση LS-1.

S-DES → Παραγωγή υποκλειδιών (5)

University of Cyprus

- Παράδειγμα:
  - Το κλειδί K πριν την μετατόπιση της LS-1:
    - Μέρος1: 10000
    - Μέρος2: 01100
  - Το κλειδί K μετά την μετατόπιση της LS-1:
    - Μέρος1: 00001
    - Μέρος2: 11000

Παραγωγή υποκλειδιών



S-DES → Παραγωγή υποκλειδιών (6)

University of Cyprus

- Ακολούθως εφαρμόζεται η αντιμετάθεση P_8 στα δύο μέρη του κλειδιού και προκύπτει το υποκλειδί K_1.
- Στην μετατόπιση P_8 εισάγονται δύο μέρη των 5-bit και εξάγεται ένα ενιαίο υποκλειδί των 8-bit.

S-DES → Παραγωγή υποκλειδιών (7)

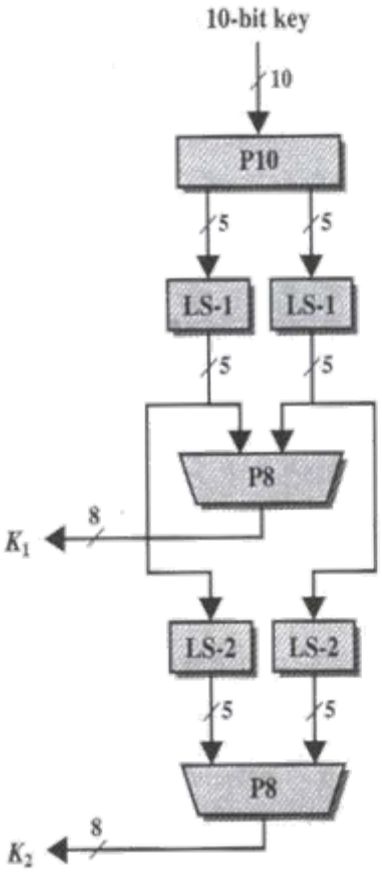
University of Cyprus

- Έάν θεωρήσουμε ότι το 10-bit κλειδί έχει την ακόλουθη μορφή:
  - Μέρος1: (k_1, k_2, k_3, k_4, k_5)
  - Μέρος2: (k_6, k_7, k_8, k_9, k_{10})
- Μετά την αντιμετάθεση της συνάρτησης P_8 σχηματίζεται το υποκλειδί K_1:
  - (k_6, k_3, k_7, k_4, k_8, k_5, k_{10}, k_9)
  - Αφού η αντιμετάθεση της συνάρτησης P_8 έχει ως εξής:

P_8

6 3 7 4 8 5 10 9

Παραγωγή υποκλειδιών



S-DES → Παραγωγή υποκλειδιών (8)

University of Cyprus

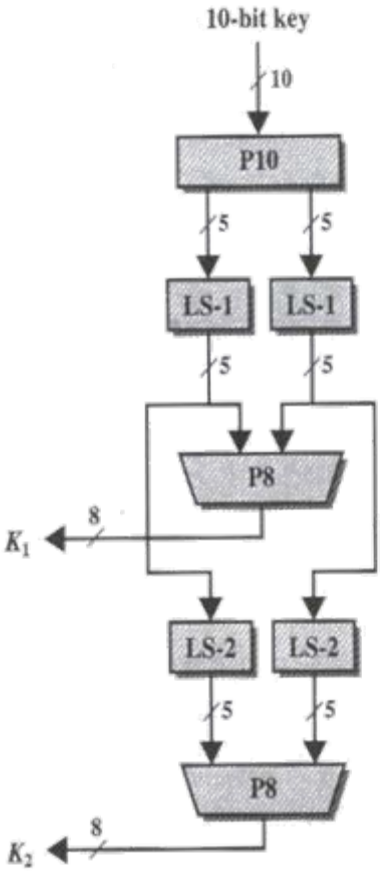
- Αφού σχηματιστεί το υποκλειδί K_1 τα δύο μέρη των 5-bit (πριν την εφαρμογή της μετατόπισης P_8) υφίστανται ξεχωριστά ολίσθηση με βάση τη συνάρτηση LS-2.

S-DES → Παραγωγή υποκλειδιών (9)

University of Cyprus

- Παράδειγμα:
  - Τα δύο μέρη πριν την μετατόπιση της LS-2:
    - Μέρος1: 00001
    - Μέρος2: 11000
  - Τα δύο μέρη μετά την μετατόπιση της LS-2:
    - Μέρος1: 00100
    - Μέρος2: 00011

Παραγωγή υποκλειδιών



S-DES → Παραγωγή υποκλειδιών (10)

University of Cyprus

- Μετά την ολίσθηση LS-2 τα δύο μέρη των 5-bit υφίστανται αντιμετάθεση σύμφωνα με την συνάρτηση P_8.
- Στη συνάρτηση P_8 εισάγονται δύο μέρη των 5-bit και εξάγεται το υποκλειδί K_2 που έχει εύρος 8-bit.

S-DES → Παραγωγή υποκλειδιών (11)

University of Cyprus

- Παράδειγμα:
  - Τα δύο μέρη πριν την αντιμετάθεση P_8:
    - Μέρος1: 00100
    - Μέρος2: 00011
  - Το υποκλειδί K_2 μετά την αντιμετάθεση P_8 :
    - Υποκλειδί K_2: 01000011

S-DES → Παραγωγή υποκλειδιών (12)

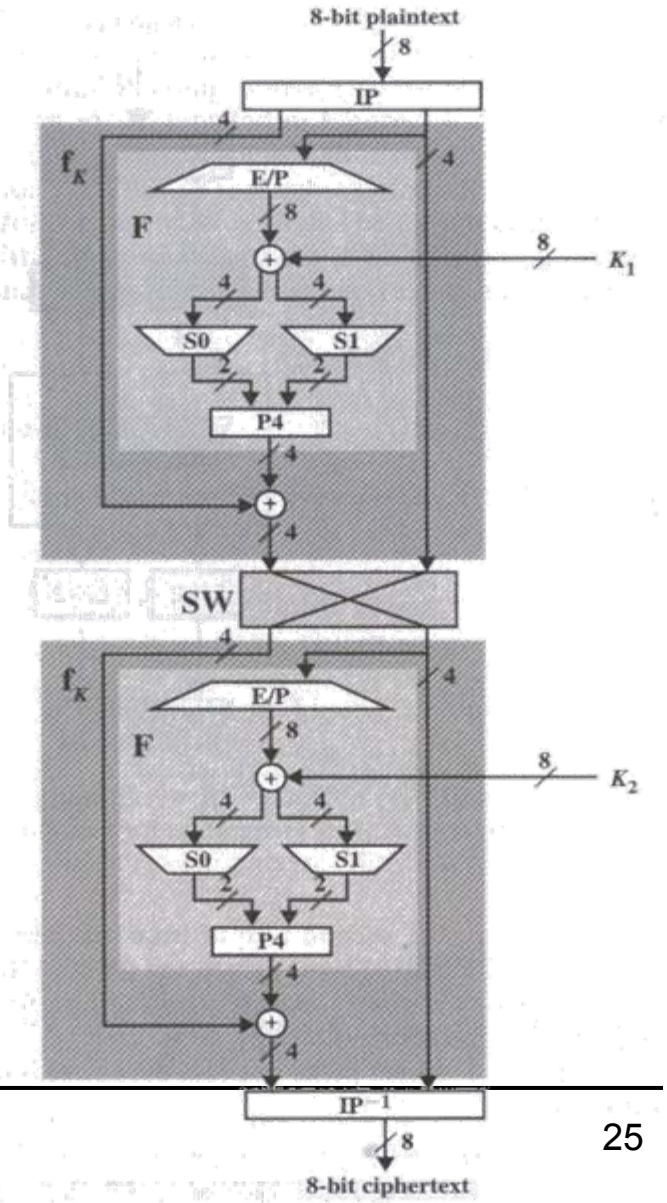
University of Cyprus

- Παράδειγμα παραγωγής των υποκλειδιών K_1 και K_2 από το ενιαίο κλειδί K:
  - Το 10-bit κλειδί K:
    - 1010000010
  - Το 8-bit υποκλειδί K_1:
    - 10100100
  - Το 8-bit υποκλειδί K_2:
    - 01000011

S-DES → Κρυπτογράφηση (1)

University of Cyprus

- Σχηματικά η διαδικασία κρυπτογράφησης:



S-DES → Κρυπτογράφηση (2)

University of Cyprus

- Η κρυπτογράφηση του S-DES αποτελείται από δύο συνεχόμενα βήματα όπου γίνεται διπλή εφαρμογή της συνάρτησης f_K, πρώτα με είσοδο το υποκλειδί K_1 και μετά με είσοδο το υποκλειδί K_2.
- Η συνάρτηση f_K μπορεί να περιγραφεί:
  - $f_K(L,R) = (L \text{ XOR } F(R,SK),R)$
    - Όπου:
      - L: το αριστερό 4-bit μέρος του απλού μηνύματος.
      - R: το δεξί 4-bit μέρος του απλού μηνύματος.
      - F: η ενδιάμεση διαδικασία αντιμετάθεσης και μετατόπισης (εισάγονται 4-bit και εξάγονται 4-bit).
      - SK: το υποκλειδί.

S-DES → Κρυπτογράφηση (3)

University of Cyprus

- Αρχικά το απλό μήνυμα των 8-bit εισάγεται για κρυπτογράφηση. Το αρχικό απλό μήνυμα αντιμετατίθεται σύμφωνα με τη συνάρτηση IP.

S-DES → Κρυπτογράφηση (4)

University of Cyprus

- Εάν θεωρήσουμε ότι το 8-bit απλό μήνυμα έχει την ακόλουθη μορφή:
  - $(m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8)$
- Μετά την αντιμετάθεση της συνάρτησης IP σχηματίζεται το μήνυμα:
  - $(m_2, m_6, m_3, m_1, m_4, m_8, m_5, m_7)$
  - Αφού η αντιμετάθεση της συνάρτησης IP έχει ως εξής:

IP

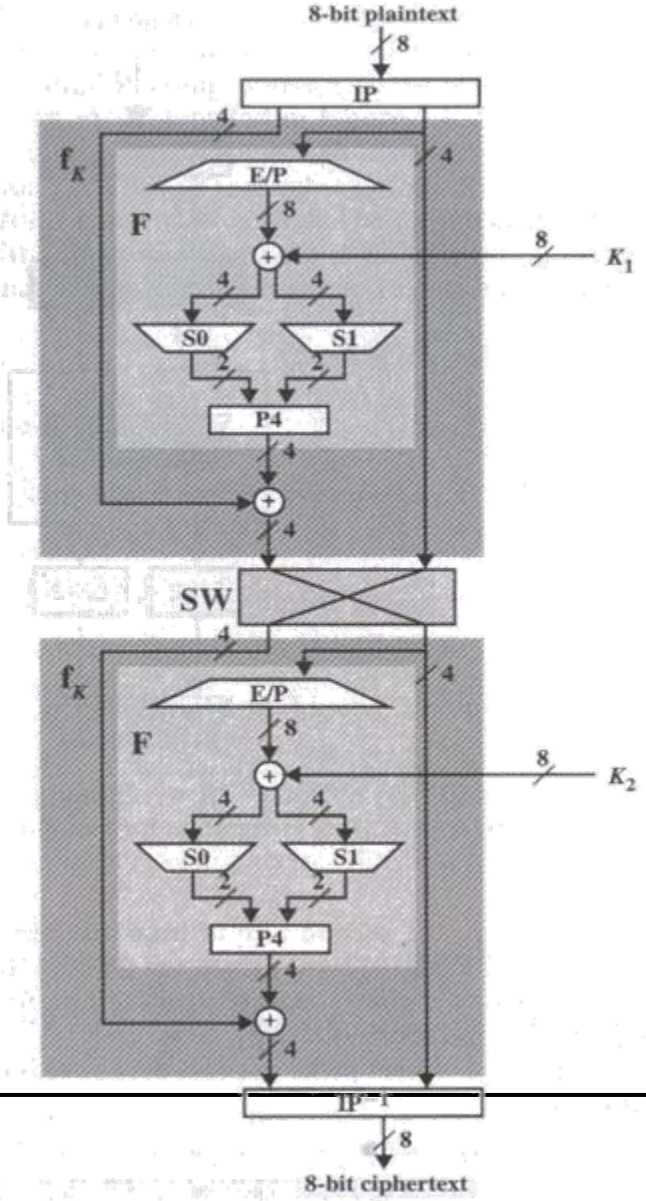
2 6 3 1 4 8 5 7

S-DES → Κρυπτογράφηση (5)

University of Cyprus

- Παράδειγμα:
  - Το μήνυμα m πριν την εφαρμογή της IP:
    - 11110011
  - Το μήνυμα m μετά την εφαρμογή της IP:
    - 10111101

S-DES → Κρυπτογράφηση



S-DES → Κρυπτογράφηση (6)

University of Cyprus

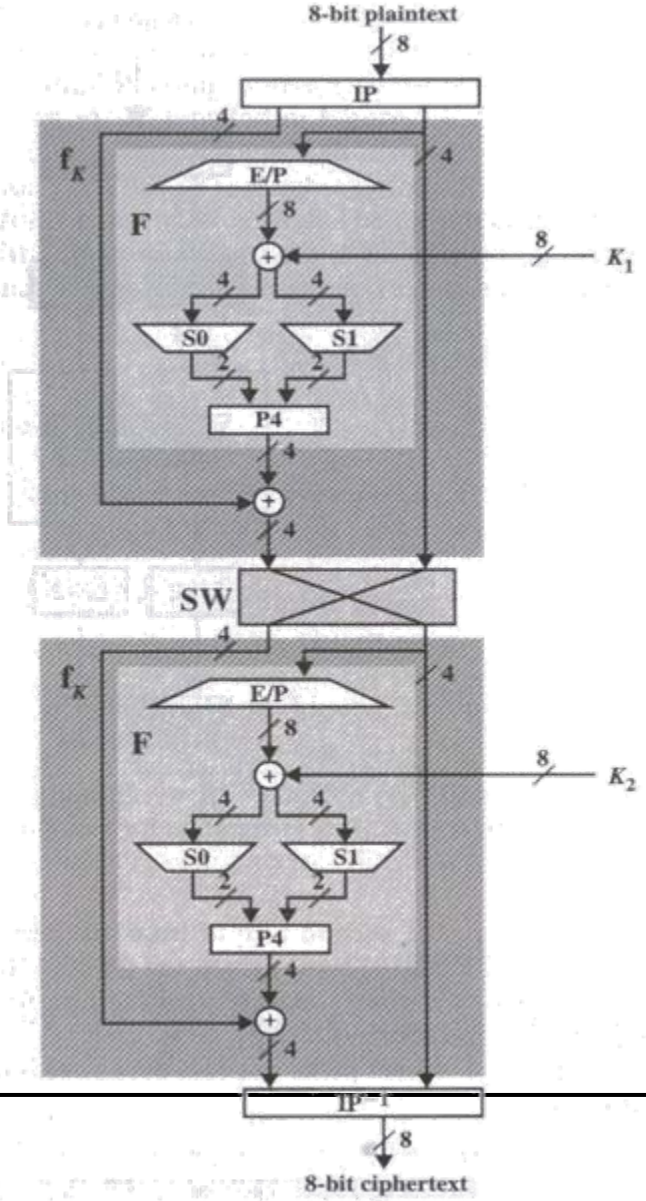
- Μετά την αντιμετάθεση της συνάρτησης IP το μήνυμα χωρίζεται στο αριστερό (L) και στο δεξί (R) μέρος του.

S-DES → Κρυπτογράφηση (7)

University of Cyprus

- Παράδειγμα:
  - Το μήνυμα m (10111101) χωρίζεται:
    - Στο αριστερό μέρος L: 1011
    - Και στο δεξί μέρος R: 1101

S-DES → Κρυπτογράφηση



S-DES → Κρυπτογράφηση (8)

University of Cyprus

- Στη συνέχεια το δεξιό μέρος R εισάγεται στη συνάρτηση E/P. Η συνάρτηση E/P λαμβάνει 4-bit είσοδο και παράγει 8-bit έξοδο.

S-DES → Κρυπτογράφηση (9)

University of Cyprus

- Εάν θεωρήσουμε ότι το δεξί 4-bit μέρος έχει την ακόλουθη μορφή:
  - (r_1, r_2, r_3, r_4)
- Μετά την αντιμετάθεση/επέκταση της συνάρτησης E/P σχηματίζεται η 8-bit μορφή:
  - $(r_4, r_1, r_2, r_3, r_2, r_3, r_4, r_1)$
- Αφού η αντιμετάθεση/επέκταση της συνάρτησης E/P έχει ως εξής:

E/P

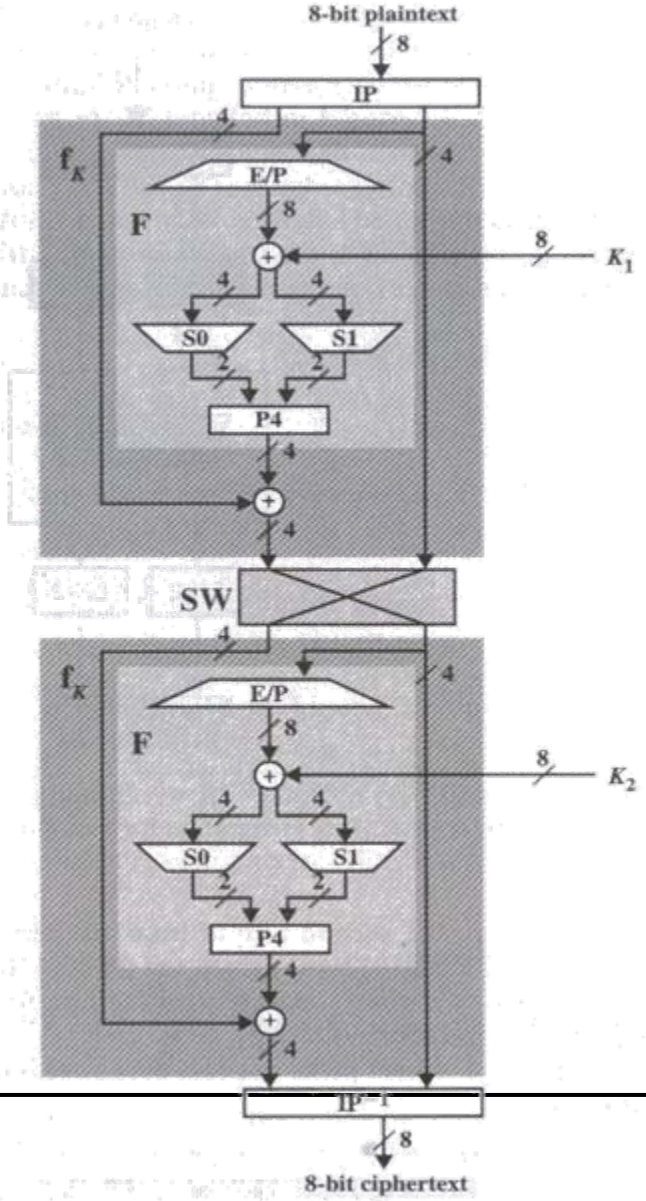
4 1 2 3 2 3 4 1

S-DES → Κρυπτογράφηση (10)

University of Cyprus

- Παράδειγμα:
  - Το δεξί μέρος r πριν από την είσοδο στη συνάρτηση E/P:
    - r = 1101
  - Μετά την έξοδο από τη συνάρτηση E/P:
    - 11101011

S-DES → Κρυπτογράφηση

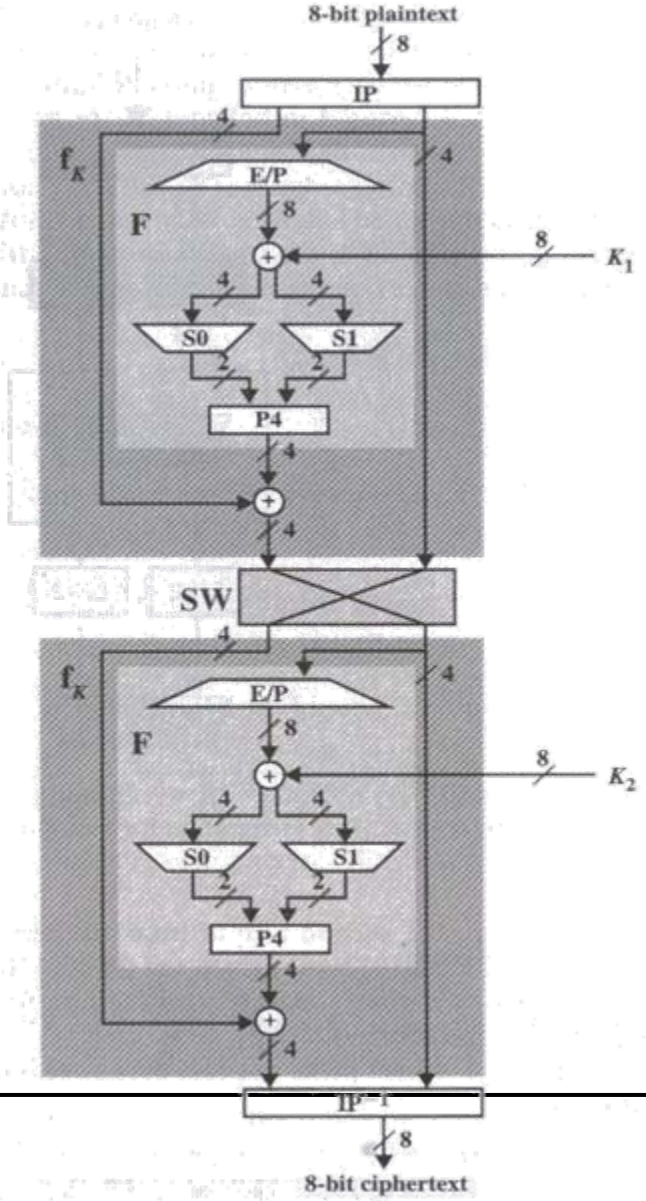


S-DES → Κρυπτογράφηση (11)

University of Cyprus

- Η 8-bit έξοδος από τη συνάρτηση E/P συνδυάζεται με το 8-bit υποκλειδί K_1 με πράξη XOR.
  - Η 8-bit έξοδος από την συνάρτηση E/P είναι:
    - 11101011
  - Το 8-bit υποκλειδί K_1 είναι:
    - 10100100
  - Το 8-bit αποτέλεσμα έχει τη μορφή:
    - 01001111

S-DES → Κρυπτογράφηση



S-DES → Κρυπτογράφηση (12)

University of Cyprus

- Το πρώτο (αριστερό) μέρος εισάγεται στο κουτί-S_0 και το δεύτερο (δεξιό) εισάγεται στο κουτί-S_1.
- Τα κουτιά S_0 και S_1 δέχονται 4-bit εισόδους και παράγουν 2-bit εξόδους. Τα κουτιά αποτελούν διδιάστατους πίνακες 4X4 που περιέχουν δεκαδικούς αριθμούς από 0 έως και 3.
- Η 4-bit είσοδος «σπάει» στη μέση και το πρώτο μέρος δηλώνει το δεκαδικό αριθμό σειράς και το δεύτερο μέρος δηλώνει το δεκαδικό αριθμό στήλης.

S-DES → Κρυπτογράφηση (13)

University of Cyprus

- Στο κουτί S_0 εισάγεται το 4-bit μέρος 0100 και στο κουτί S_1 εισάγεται το 4-bit μέρος 1111.
  - Για το κουτί S_0:
    - Το πρώτο και το τέταρτο bit μετατρέπονται σε δεκαδικό αριθμό και δηλώνουν την γραμμή στο κουτί S_0:
      - Δηλαδή: $00_{(2)}$ → $0_{(10)}$ → σειρά 0
    - Το δεύτερο και το τρίτο bit μετατρέπονται σε δεκαδικό αριθμό και δηλώνουν την στήλη στο κουτί S_0:
      - Δηλαδή: $10_{(2)}$ → $2_{(10)}$ → στήλη 2
  - Για το κουτί S_1:
    - Το πρώτο και το τέταρτο bit μετατρέπονται σε δεκαδικό αριθμό και δηλώνουν την γραμμή στο κουτί S_1:
      - Δηλαδή: $11_{(2)}$ → $3_{(10)}$ → σειρά 3
    - Το δεύτερο και το τρίτο bit μετατρέπονται σε δεκαδικό αριθμό και δηλώνουν την στήλη στο κουτί S_1:
      - Δηλαδή: $11_{(2)}$ → $3_{(10)}$ → στήλη 3

S-DES → Κρυπτογράφηση (14)

University of Cyprus

- Τα κουτιά S_0 και S_1 περιέχουν συγκεκριμένες τιμές:

S_0

1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	2

S_1

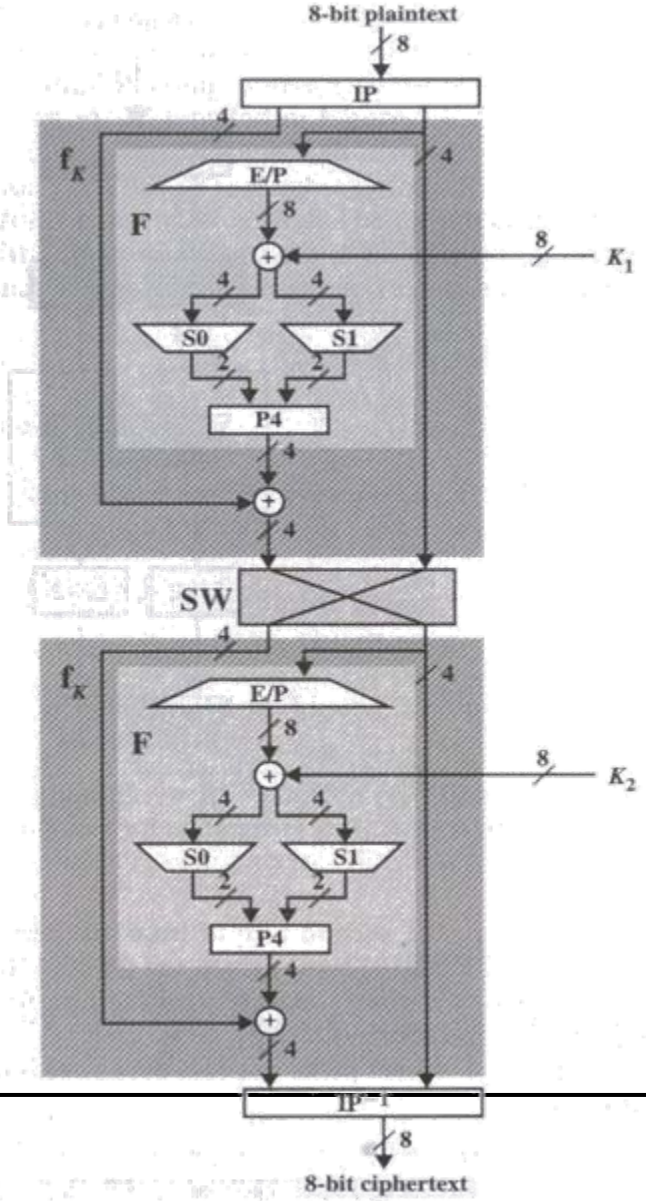
0	1	2	3
2	0	1	3
3	0	1	0
2	1	0	3

S-DES → Κρυπτογράφηση (15)

University of Cyprus

- Επομένως το τμήμα που εξάγεται από το κουτί S_0 δείχνει στη δεκαδική τιμή 3 → 11 και το τμήμα που εξάγεται από το κουτί S_1 δείχνει στη δεκαδική τιμή 3 → 11.
  - Με αυτόν τον τρόπο από το κουτί S_0 εξάγεται το τμήμα 11 και από το κουτί S_1 εξάγεται το τμήμα 11.

S-DES → Κρυπτογράφηση



S-DES → Κρυπτογράφηση (16)

University of Cyprus

- Τα δύο τμήματα εισάγονται ενοποιημένα στην συνάρτηση αντιμετάθεσης P_4. Η συνάρτηση P_4 δέχεται δύο τμήματα των 2-bit και εξάγει ένα 4-bit τμήμα.

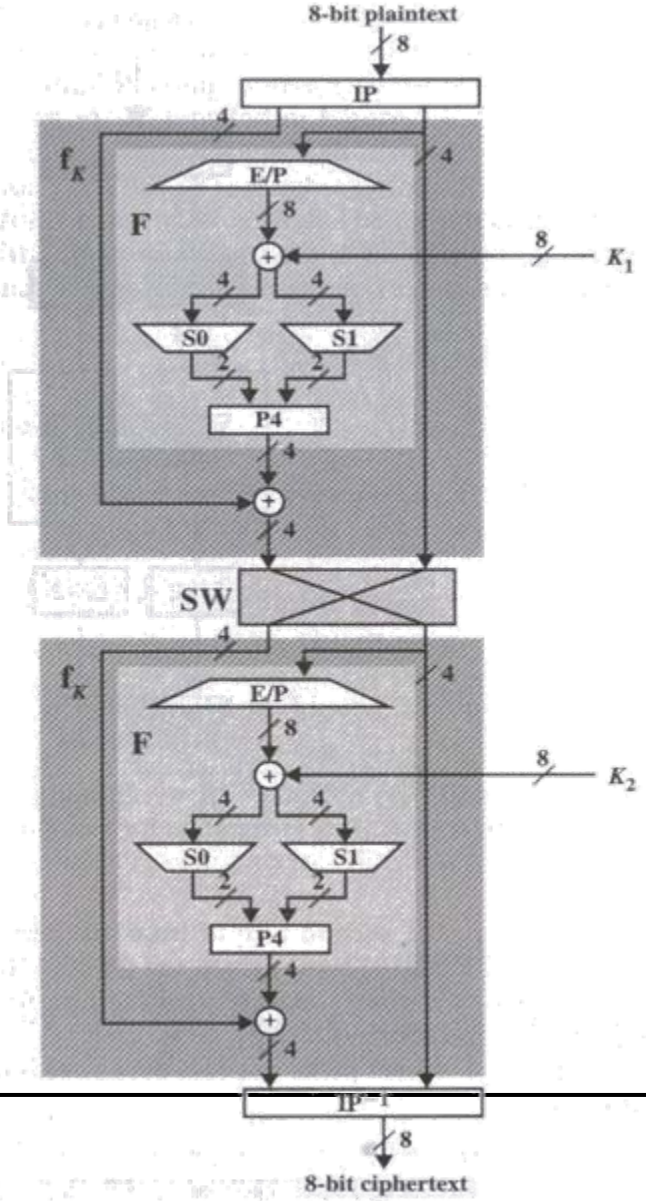
S-DES → Κρυπτογράφηση (17)

University of Cyprus

- Εάν θεωρήσουμε ότι τα δύο τμήματα των 2-bit έχουν την ακόλουθη μορφή:
  - $(t_1, t_2), (t_3, t_4)$
- Μετά την αντιμετάθεση της συνάρτησης P_4 σχηματίζεται η 4-bit μορφή:
  - (t_2, t_4, t_3, t_1)
    - Αφού η αντιμετάθεση της συνάρτησης P_4 έχει ως εξής:

$$P_4$$
$$2\ 4\ 3\ 1$$

S-DES → Κρυπτογράφηση



S-DES → Κρυπτογράφηση (18)

- Για το συγκεκριμένο παράδειγμα η έξοδος από τη συνάρτηση P_4 θα είναι:
  - 1111
- Έπειτα το 4-bit μέρος συνδυάζεται με πράξη XOR με το αρχικό τμήμα L:
  - 1111 XOR L = 1111 XOR 1011 = 0100
- Το τμήμα αυτό εισάγεται στη συνάρτηση SW σαν αριστερό μέλος, ενώ το δεξιό μέλος είναι το τμήμα R = 1101.
- Η συνάρτηση SW αντιστρέφει το αριστερό και δεξί μέλος και τα δύο τμήματα επαναεισάγονται στη συνάρτηση f_K με όμοιο τρόπο. Η μόνη αλλαγή στη νέα εκτέλεση της f_K είναι ότι χρησιμοποιείται το υποκλειδί K_2.

S-DES → Ισχύς

University of Cyprus

- Ισχύς του S-DES.
  - Μία «βίαιη επίθεση» είναι εφικτό να παραβιάσει τον S-DES, αφού με ένα 10-bit κλειδί υπάρχουν μόνο $2^{10} = 1024$ πιθανότητες.

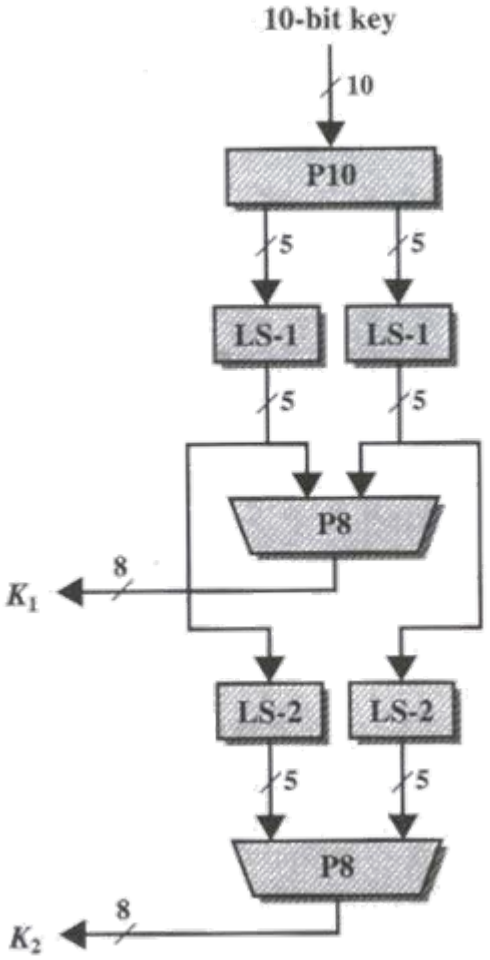
S-DES → Σχέση με DES

University of Cyprus

- Ο S-DES αποτελεί μία μικρογραφία του DES (χρησιμοποιείται για εκπαιδευτικούς σκοπούς).
  - Ο S-DES δέχεται 8-bit απλό κείμενο, ενώ ο DES 64-bit απλό κείμενο.
  - Ο S-DES δέχεται 10-bit κλειδί, ενώ ο DES 64-bit (το οποίο μετατρέπεται σε 56-bit).
  - Ο S-DES χρησιμοποιεί 2 υποκλειδιά, ενώ ο DES 16.

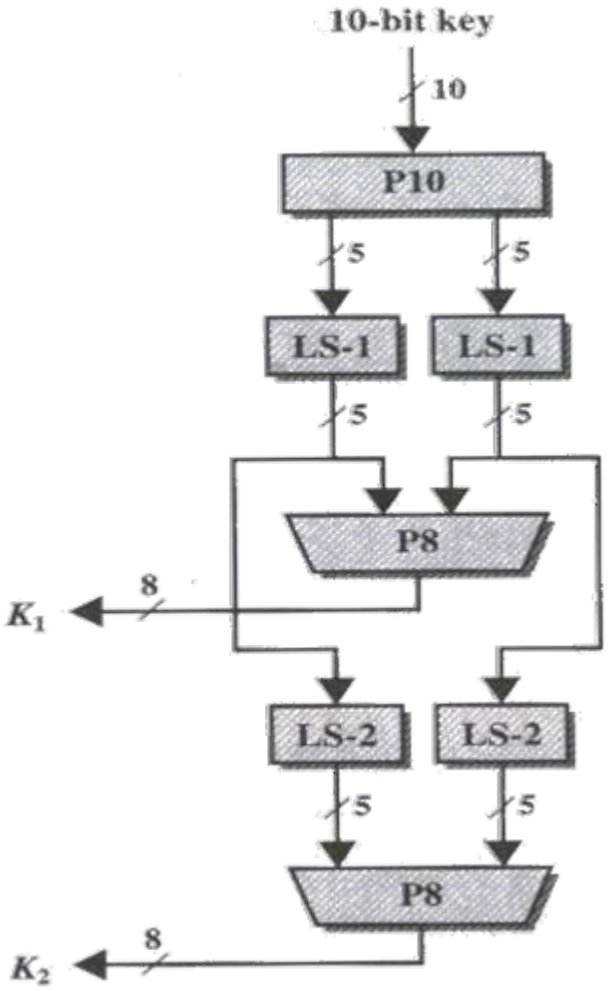
Παράδειγμα (1)

- K = 1010101010
- P10 = 3 5 2 7 4 10 1 9 8 6
- P10(K) = 1101001100
- KL = 11010
- KR = 01100
- LS-1(KL) = 10101
- LS-1(KR) = 11000
- K`= LS-1(KL) LS-1(KR)
  =1010111000



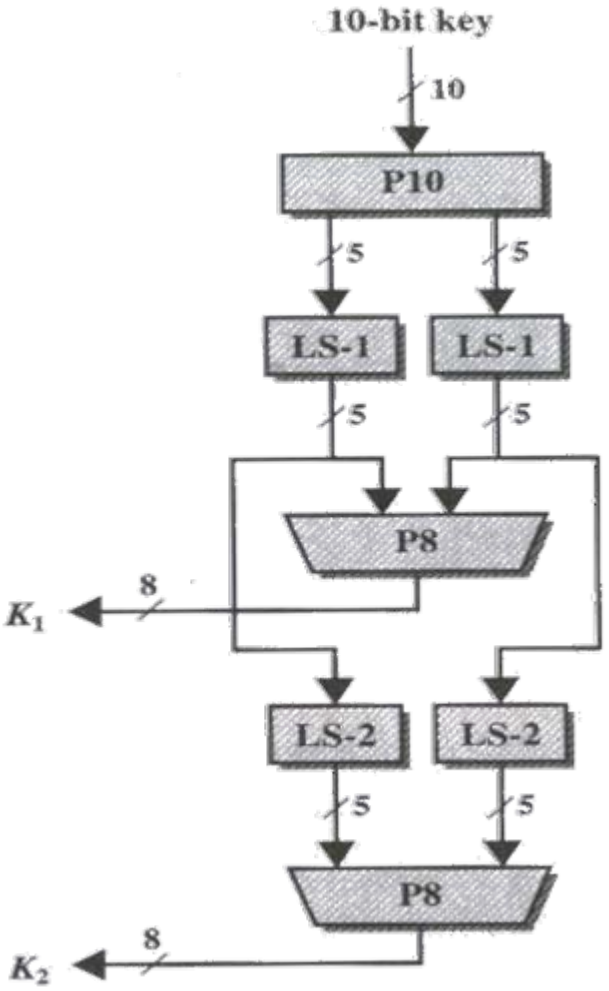
Παράδειγμα (2)

- K`= 1010111000
- P8 = 6 3 7 4 8 5 10 9
- P8(K`) = 11100100
- K1 = 11100100
- LS-2(LS-1(KL))=LS-2(10101)
  = 10110
- LS-2(LS-1(KR))= LS-2(11000)
  = 00011



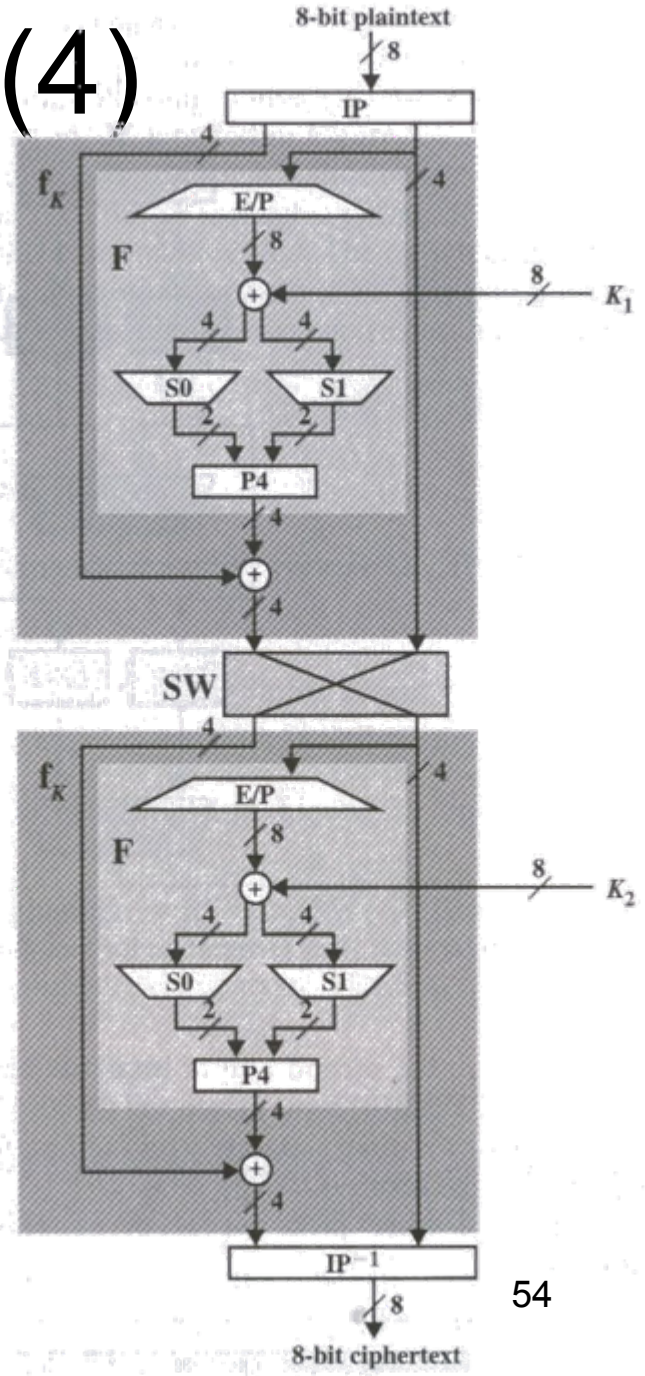
Παράδειγμα (3)

- K`` = LS-2(LS-1(KL)) LS-2(LS-1(KR))
  = 1011000011
- P8 = 6 3 7 4 8 5 10 9
- P8(K``) = 01010011= K2



Παράδειγμα (4)

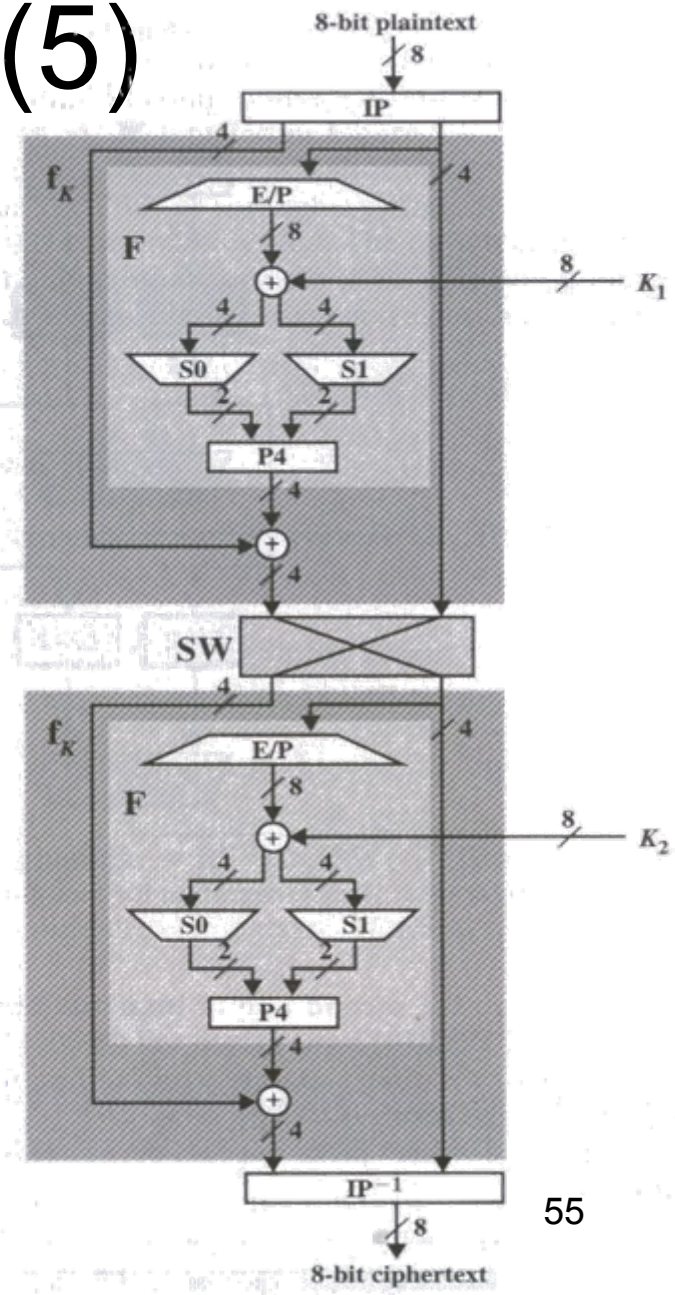
- K1 = 11100100
- K2 = 01010011
- Plaintext m = 11110000
- IP = 2 6 3 1 4 8 5 7
- IP(m) = 10111000
- mL = 1011
- mR = 1000



Παράδειγμα (5)

- E/P = 4 1 2 3 3 2 4 1
- E/P(mR) = E\P(1000)
  = 01000001
- E/P(mR) xor K1 =
  01000001xor 11100100=
  10100101

- m`L = 1010
- m`R = 0101



Παράδειγμα (6)

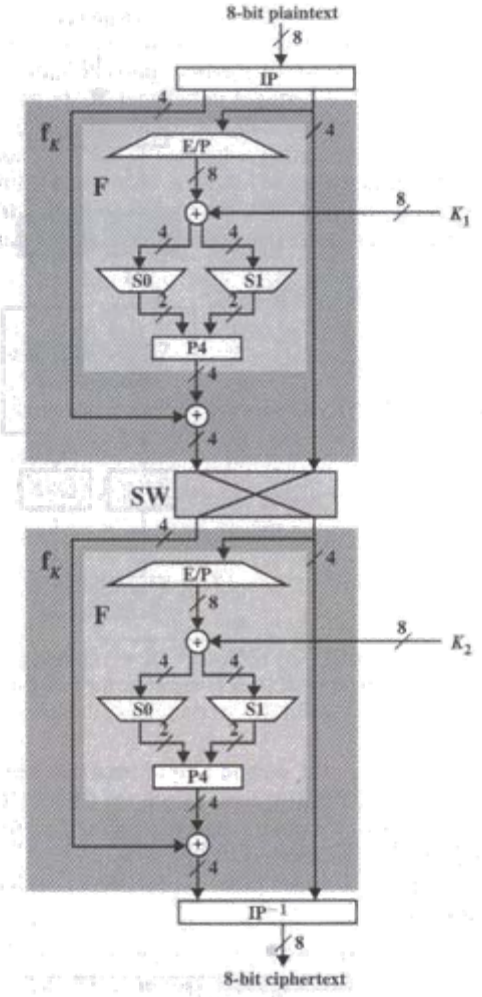
- m`L = 1010
- S_0(m`L) = 2 = 10
- m`R = 0101
- S_1(m`R) = 1 = 01
- m``= m`L m`R = 1001
- P4 = 2 4 3 1
- P4(m``) = 0101
- mL xor P4(m``) =
  1011 xor 0101=
  1110

S_0

1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	2

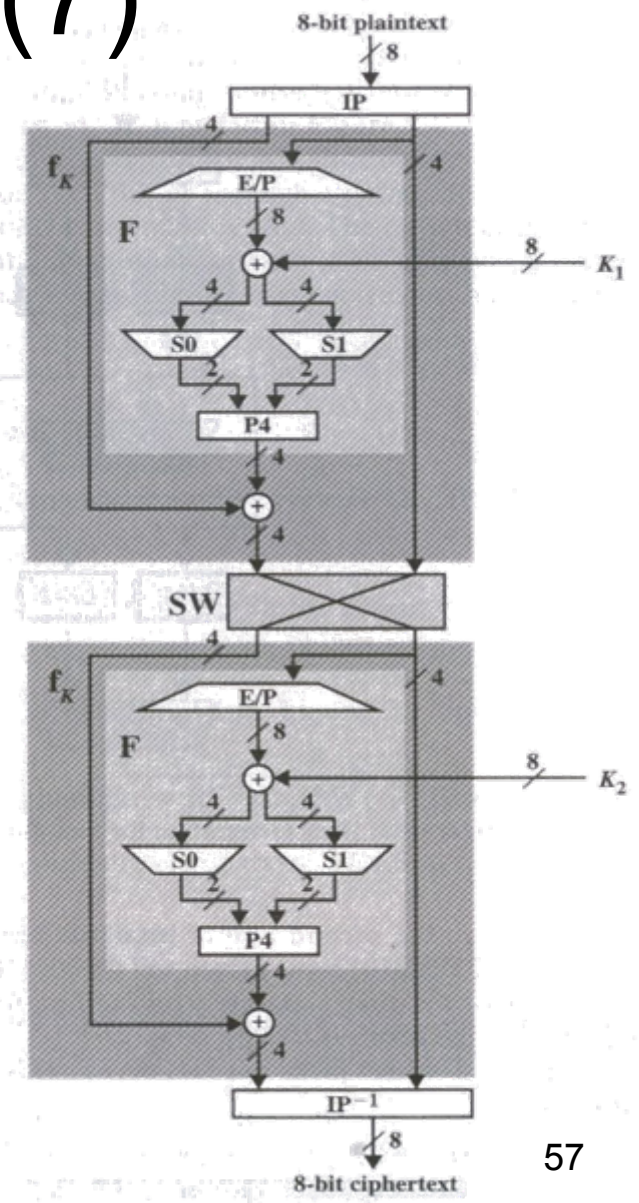
S_1

0	1	2	3
2	0	1	3
3	0	1	0
2	1	0	3



Παράδειγμα (7)

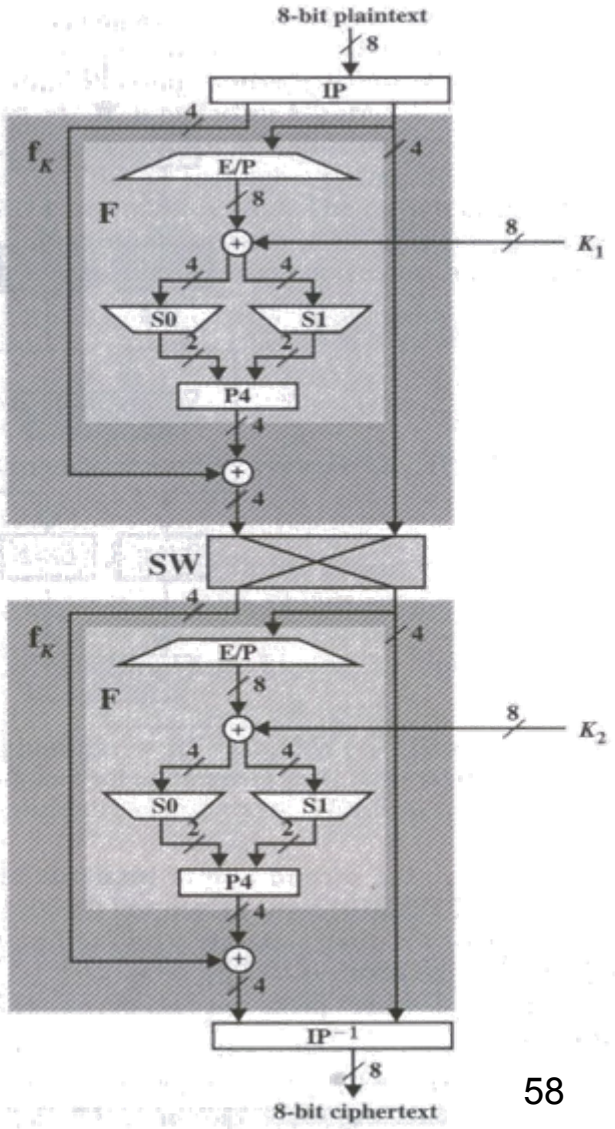
- (mL xor P4(m``)) SW mR =
  1110 SW 1000 = 10001110
- ML = 1000
- MR = 1110
- K2 = 01010011



Παράδειγμα (8)

- E/P = 4 1 2 3 2 4 1
- E/P(MR) = E/P(1110)
  = 01111101
- E/P(MR) xor K2 =
  = 01111101 xor 01010011
  = 00101110

- M`L = 0010
- M`R = 1110



Παράδειγμα (9)

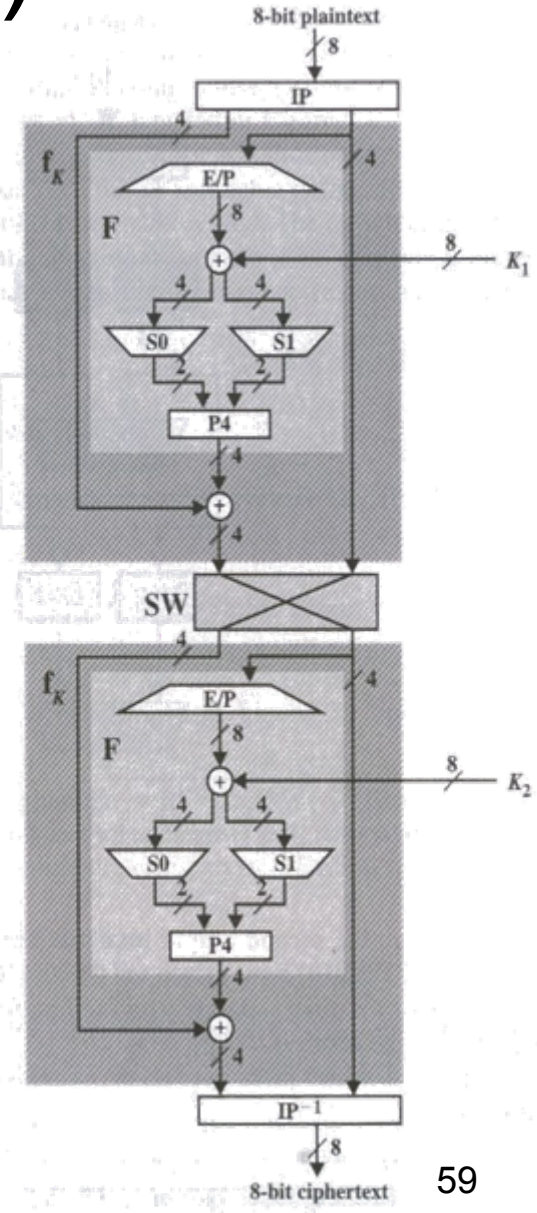
- M`L = 0010
- S_0(M`L) = 0 = 00
- M`R = 1110
- S_1(m`R) = 0 = 00
- M``= M`L  M`R = 0000
- P4 = 2 4 3 1
- P4(M``) = 0000
- ML xor P4(M``) =
  1000 xor 0000 =
  1000

S_0

1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	2

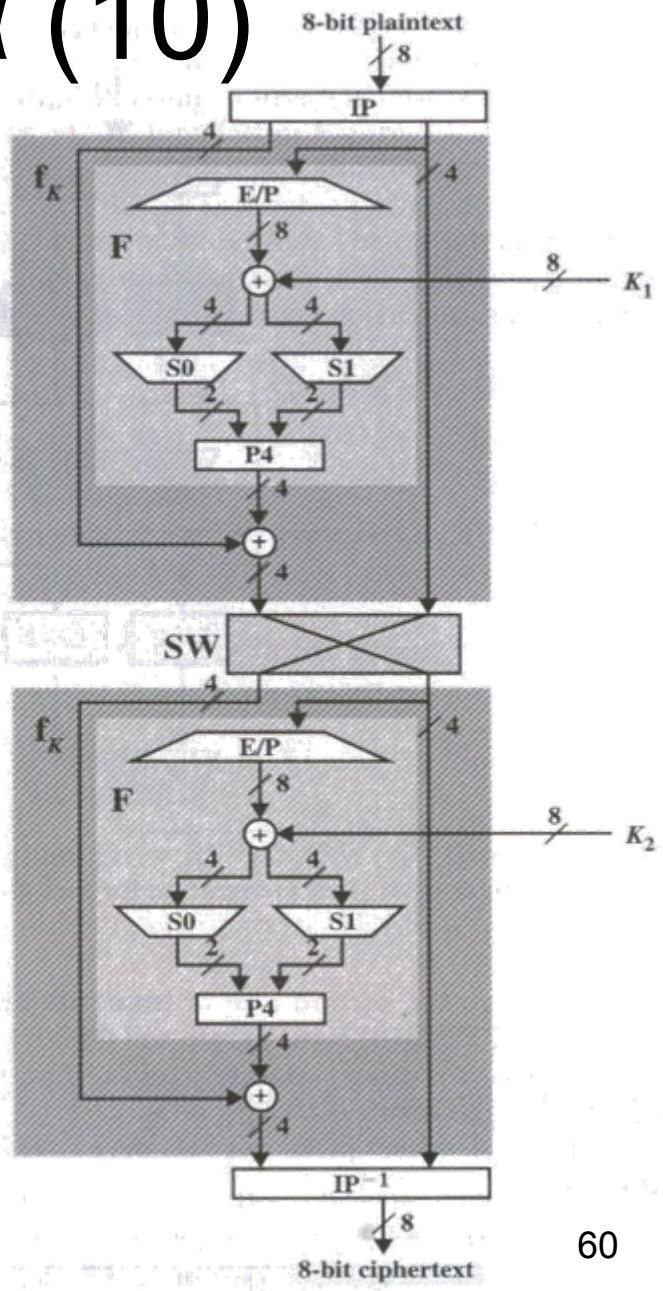
S_1

0	1	2	3
2	0	1	3
3	0	1	0
2	1	0	3



Παράδειγμα (10)

- IP = 2 6 3 1 4 8 5 7
- IP-1(ML xor P4(M``) ,MR)
  = IP-1(1000,1110)=
  = 01011001
- c = 01011001



Αποκωδικοποίηση

- IP = 2 6 3 1 4 8 5 7
- E/P = 4 1 2 3 2 3 4 1
- P4 = 2 4 3 1
- SW αντιμετάθεση left and right

S_0

1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	2

S_1

0	1	2	3
2	0	1	3
3	0	1	0
2	1	0	3