Εθνικο Μετσοβιο Πολυτεχνειο

Σχολη Ηλεκτρολογων Μηχανικων & Μηχανικων Υπολογιστων

Σημειώσεις Διαλέξεων

Σύστημα **DES**

Επιμέλεια σημειώσεων:
Ελένη Λιτσα
Νίκος Μελισσαρης

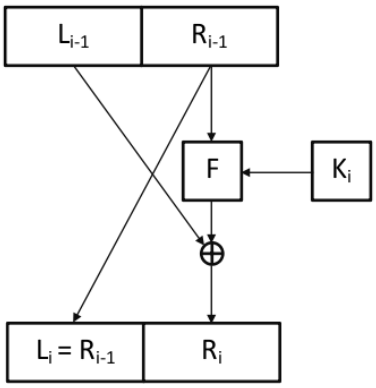
Διδάσκοντες:
Στάθης Ζαχος
Άρης Παγουρτζης

21 Νοεμβρίου 2011

Το Σύστημα DES ανήκει στα δίκτυα FEISTEL.

Δίκτυα FEISTEL: [H.Feistel 1973]
Η συμβολοσειρά χωρίζεται σε δύο μέρη: $L_0||R_0$

Κρυπτογράφηση:



Δίκτυο FEISTEL k γύρων:

Συνάρτηση: F
Είσοδος: $L_0||R_0$
$L_i = R_{i-1}$
$R_i = F_{k_{i-1}}(R_{i-1}) \oplus L_{i-1}$ για $i = 1, 2, ..., k$
Έξοδος: $R_k||L_k$

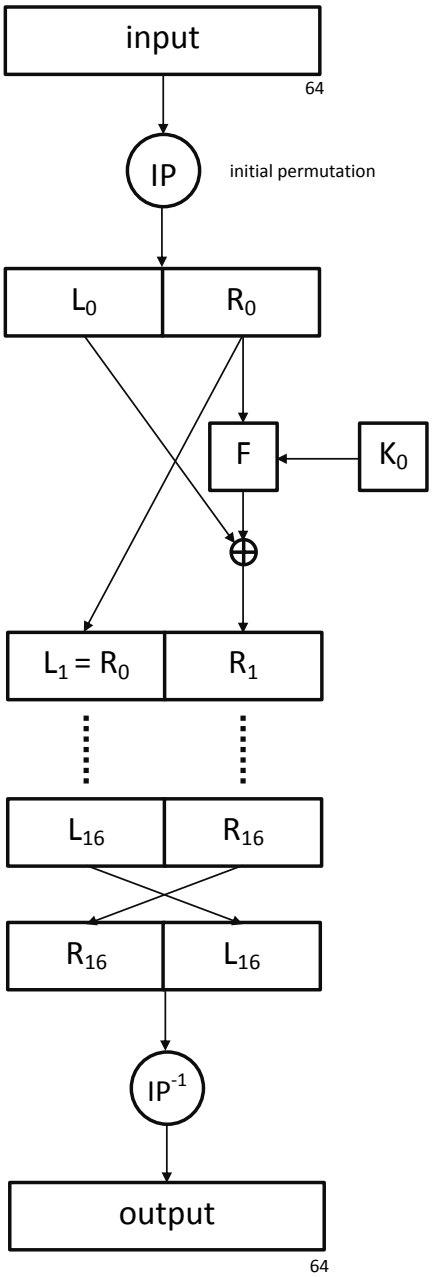
Στο τέλος γίνεται αντιμετάθεση της εξόδου $R_k||L_k$ όποτε παίρνουμε $L_k||R_k$.
Το αποτέλεσμα που προκύπτει εξαρτάται μόνο από την είσοδο και τα κλειδιά.
Η συνάρτηση F εδώ κάνει διάχυση δηλαδή κάθε bit της εισόδου μπορεί να επηρεάσει πολλά bits της εξόδου.
Η συνάρτηση F προκαλεί είτε:

- διάχυση (diffusion)
- Σύγχυση (confusion)

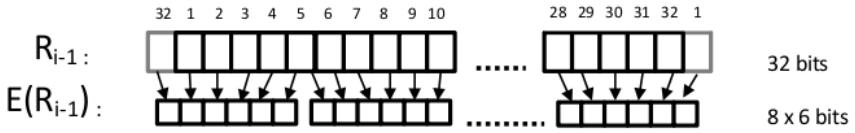
Αποκρυπτογράφηση:

$$L_{k-1} = R_k \oplus F_{k_{k-1}}(R_{k-1}) = R_n \oplus F_{k_{k-1}}(R_{k-1})$$

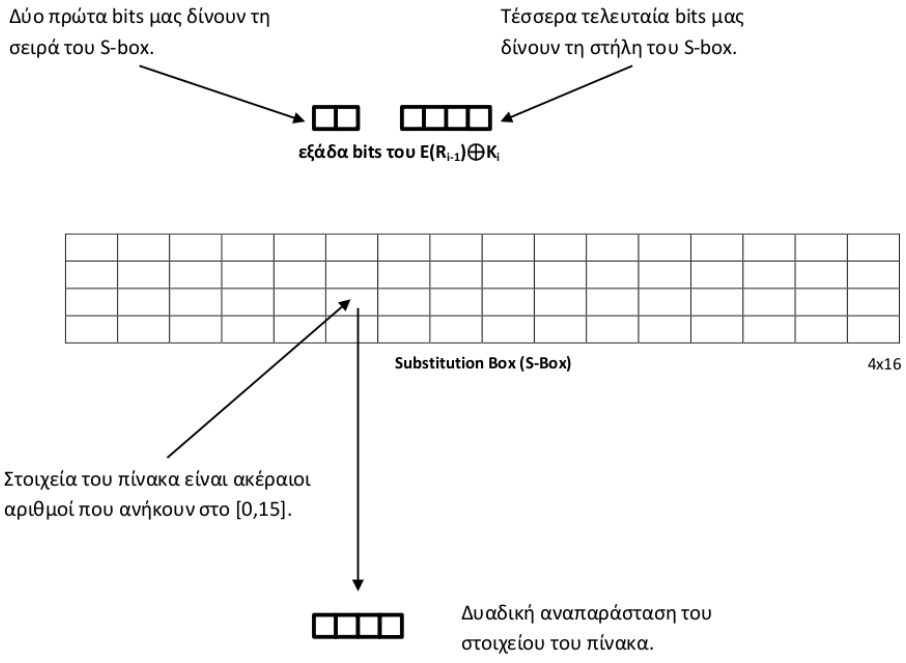
Σύστημα DES: Είναι ένα FEISTEL δίκτυο με 16 γύρους.
Η είσοδος και η έξοδος είναι blocks των 64-bits.


input
64
IP
initial permutation
L_0
R_0
F
K_0
$L_1 = R_0$
R_1
L_{16}
R_{16}
R_{16}
L_{16}
IP^{-1}
output
64

Η συνάρτηση F ενεργεί πάνω σε ένα κομμάτι 32 bits και το επεκτείνει (αναδιάταξη με επαναλήψεις).



Από την εφαρμογή της F προκύπτουν 8 εξάδες E_j. Από το αρχικό κλειδί K με αφαίρεση *bits* ισοτιμίας και διαδοχικές ολισθήσεις προκύπτουν 8 εξάδες K_j. Στη συνέχεια το αποτέλεσμα της πράξης $B_j = E_j \oplus K_j$ καταχωρείται σε 6 κουτιά-αντικατάστασης (s-boxes).


Δύο πρώτα bits μας δίνουν τη σειρά του S-box.
Τέσσερα τελευταία bits μας δίνουν τη στήλη του S-box.
εξάδα bits του $E(R_{i-1})\oplus K_i$
Substitution Box (S-Box)
4x16
Στοιχεία του πίνακα είναι ακέραιοι αριθμοί που ανήκουν στο [0,15].
Δυαδική αναπαράσταση του στοιχείου του πίνακα.

Προσπάθειες κρυπανάλυσης:

- Διαφορική Κρυπτανάλυση [Biham, Shamir 1990]
- Γραμμική κρυπτανάλυση [Matsui 1993-94]

Διαφορική Κρυπτανάλυση

Έστω E_j η j-οστή εξάδα του E_{R_i} και k_j η αντίστοιχη εξάδα στο κλειδί, τότε $B_j = E_j \oplus k_j$. Από το s-box προκύπτει το $S_j(B_j)$.
Έστω E_j^* η j-οστή εξάδα του $E_{R_i^*}$
input-xor: $B_j \oplus B_j^* = E_j \oplus E_j^*$ $\quad 2^6 = 64$ input-xors
output xor: $S_j(B_j) \oplus S_j(B_j^*) = C_j'$ $\quad 2^4 = 16$ outputs x-ors