Εθνικο Μετσοβιο Πολυτεχνειο

Σχολη Ηλεκτρολογων Μηχανικων & Μηχανικων Υπολογιστων

Σημειώσεις Διαλέξεων

Ασκήσεις

Επιμέλεια σημειώσεων:
Ελένη Λιτσα
Νίκος Μελισσαρης

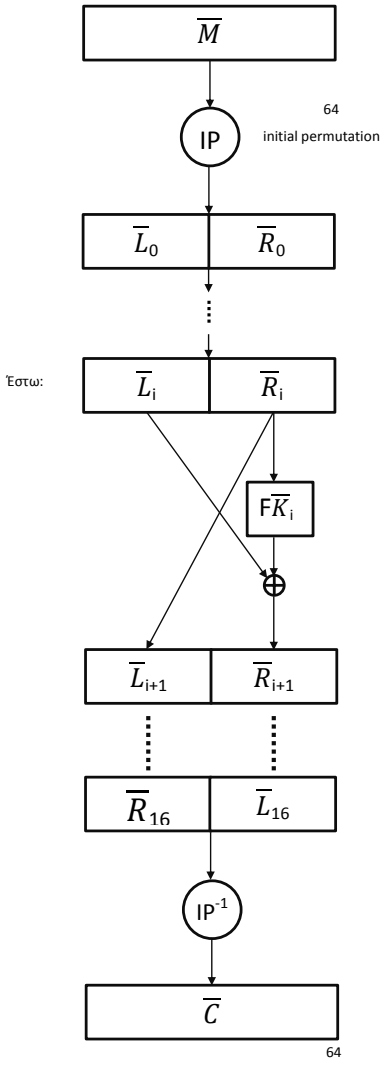
Διδάσκοντες:
Στάθης Ζαχος
Άρης Παγουρτζης

25 Νοεμβρίου 2011

1. i Αποδείξτε ότι το DES έχει την ιδιότητα της συμπληρωματικότητας, δηλαδή ότι ισχύει $E_k(M) = C \Leftrightarrow E_{\overline{k}}(\overline{M}) = \overline{C}$

   ii Μπορεί αυτή η ιδιότητα να βοηθήσει την κρυπτανάλυση και πόσο;

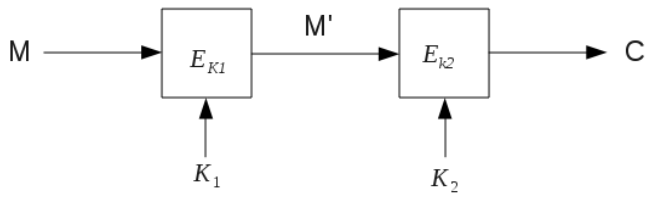
Απάντηση:



i

ii Brute Force Attack: Δοκιμάζουμε όλα τα κλειδιά: 2^{56} δοκιμές
Έστω ότι έχουμε M, C τέτοια ώστε $E_k(M) = C$.
Αν το κλειδί k δεν δουλεύει εξετάζουμε το $\overline{k}$ δηλαδή ελέγχουμε αν $E_{\overline{k}}(M) = C \Leftrightarrow E_k(\overline{M}) = \overline{C}$
Δοκιμάζουμε: $E_k(M||\overline{M}) = C'C''$
Ελέγχουμε αν $C' = C$ και $C'' = \overline{C}$
Το κέρδος από την ιδιότητα της συμπληρωματικότητας έγκειται στο γεγονός πως δεν χρειάζεται να φτιάξουμε και το συμπληρωματικό κλειδί άρα αρκεί να ελέγξουμε τα μισά κλειδιά. Βέβαια και πάλι το κέρδος αυτό δεν δίνει κάποιο ιδιαίτερο πλεονέκτημα στην κρυπτανάλυση.

2. Διπλό DES: $DES_{k_1,k_2}(M) = DES_{k_2}(DES_{k_1}(M))$
Naive brute force: 2^{112} δοκιμές



Σχήμα 1: meet in the middle attack

Τα M, C είναι γνωστά.
Αν χρησιμοποιήσω 2^{56} κλειδιά για το K_1 παράγονται $2^{56}M'$ τα οποία αποθηκεύονται στη μνήμη. Στη συνέχεια δεν εφαρμόζω 2^{56} κλειδιά για το K_2 γιατί θα έχω συνολικά $2^{56} \times 2^{56}$ περιπτώσεις. Αντίθετα, αφού το C είναι γνωστό ζητώ να ισχύει $E_{k_1}(M) = M' = D_{k_2}(C)$.
Για καλύτερη απόδοση αποθηκεύω σε μια λίστα ότι παράγεται με την εφαρμογή του κλειδιού k_1. Ότι παράγεται με την εφαρμογή του κλειδιού k_2 το συγκρίνω με τα περιεχόμενα της λίστας.
Στο σύνολο χρειάζονται 112×2^{56} δοκιμές.
Επομένως, η χρήση του διπλού DES δεν μας δίνει κάποιο πλεονέκτημα αφού σπάει σχεδόν το ίδιο εύκολα με το απλό DES .