Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία
2η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 3/11/2017

25 Οκτωβρίου 2017

1η Άσκηση

Θεωρήστε την παραλλαγή του DES-X, με 2 κλειδιά k_1, k_2, όπου η κρυπτογράφηση ενός απλού κειμένου M γίνεται ως εξής :

$$Enc_{k_1,k_2}(M) = E_{k_1}(M \oplus k_2),$$

όπου E η συνάρτηση κρυπτογράφησης του DES.

Έχουμε περισσότερη ασφάλεια από τον κλασσικό DES στο παραπάνω σύστημα; Θεωρήστε ότι ο αντίπαλος έχει δυνατότητα KPA (διαθέτει μερικά ζεύγη απλού κειμένου - κρυπτοκειμένου).

2η Άσκηση

Εξετάστε τη γεννήτρια ψευδοτυχαιότητας RC4. Αποδείξτε ότι το δεύτερο byte (κλειδί) εξόδου είναι ίσο με 0 με πιθανότητα περίπου ίση με 2^{-7}. Δείξτε πρώτα ότι αν μετά τη φάση δημιουργίας κλειδιών (KSA) ισχύει για την μετάθεση P ότι $P[2] = 0$ και $P[1] \neq 2$ τότε το δεύτερο byte εξόδου είναι ίσο 0 με πιθανότητα 1.

3η Άσκηση

Αν ένα LFSR έχει περίοδο μήκους $2^\ell - 1$, να δείξετε ότι το πολυώνυμο $t(x) = 1 + \sum_{j=1}^{\ell} c_j x^j$ είναι ανάγωγο[1].

4η Άσκηση

Πως μπορείτε να ξεχωρίσετε ένα κρυπτοκείμενο Feistel από μια τυχαία συνάρτηση αν έχει μόνο: (i) ένα γύρο, (ii) δύο γύρους.

[1] Ένα πολυώνυμο είναι ανάγωγο (*irreducible*) όταν δεν υπάρχουν μη σταθερά πολυώνυμα που να το διαιρούν.