Εισαγωγή στην Κρυπτολογία
Φυλλάδιο ασκήσεων #1

Θεόδουλος Γαρεφαλάκης

13 Φεβρουαρίου 2015

Η Αλίκη επικοινωνεί με το Βασίλη χρησιμοποιόντας ένα σύστημα κρυπτογράφησης τύπου Feistel. Ειδικότερα, κάθε block έχει μήκος 128 bits, ο αλγόριθμος έχει 4 γύρους και το κοινό, κρυφό κλειδί της Αλίκης και του Βασίλη είναι το (k_1, k_2, k_3, k_4), όπου $k_i \in \mathbb{F}_2^{64}$, $i = 1, \ldots, 4$ είναι το κλειδί του i γύρου. Το αρχικό (καθαρό) μήνυμα χωρίζεται σε δύο μέρη των 64 bits έκαστο (το αριστερό και το δεξιό) L_0 και R_0. Στη συνέχεια ο αλγόριθμος κρυπτογράφησης υπολογίζει τα

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} + F(k_i, R_{i-1}), \end{aligned}$$

για $i = 1, 2, 3, 4$. Η απεικόνιση $F : \mathbb{F}_2^{64} \times \mathbb{F}_2^{64} \longrightarrow \mathbb{F}_2^{64}$ είναι η $F(k, R) = R + k$. (Στους παραπάνω ορισμούς, η πράξη "+" είναι πρόσθεση στο $\mathbb{F}_2^{64}$.) Το κρυπτογραφημένο μήνυμα είναι το (L_4, R_4). Ας υποθέσουμε ότι η Αλίκη, για να σας "επιδείξει" τον αλγόριθμο της, δέχεται να κρυπτογραφήσει ένα τυχαίο μήνυμα, ας πούμε το (L_0', R_0'). Δείξτε πώς μπορείτε, με δεδομένο το (L_4, R_4) και το ζεύγάρι καθαρού μηνύματος (L_0', R_0') και κρυπτογραφήματος (L_4', R_4'), να υπολογίσετε το καθαρό μήνυμα (L_0, R_0).

Αφού καταφέρατε να παραβιάσετε την ασφάλεια του συστήματος τους, η Αλίκη και ο Βασίλης αποφασίζουν να το βελτιώσουν με τον εξής τρόπο: επιλέγουν μία απεικόνιση $\sigma : \mathbb{F}_2^{64} \longrightarrow \mathbb{F}_2^{64}$ και τροποποιούν την απεικόνιση F, να είναι $F(k, R) = \sigma(R) + k$. Η απεικόνιση σ είναι γνωστή σε όλους (δεν είναι μέρος του κλειδιού). Για "ευκολία", επιλέγουν τη σ να είναι $\mathbb{F}_2$-γραμμική απεικόνιση. Προσπαθήστε να πραγματοποιήσετε μία επίθεση όπως η προηγούμενη.