Εθνικο Μετσοβιο Πολυτεχνειο

Σχολη Ηλεκτρολογων Μηχανικων & Μηχανικων Υπολογιστων

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Ελένη Λιτσα

Διδάσκοντες:
Στάθης Ζαχος
Άρης Παγουρτζης

18 Νοεμβρίου 2011

1. Ένα κρυπτοσύστημα είναι **τέλεια ασφαλές** αν ισχύει:

$$\forall m \in M \, \forall c \in C : P_r[M = m | C = c] = P_r[M = m]$$

Ερώτηση: Αν για κάθε δύο χαρακτήρες χρησιμοποιούμε το ίδιο ομοιόμορφα επιλεγμένο κλειδί έχουμε τέλεια ασφάλεια;
Απάντηση:Έστω ότι θέλουμε να κρυπτογραφήσουμε το επόμενο κείμενο:

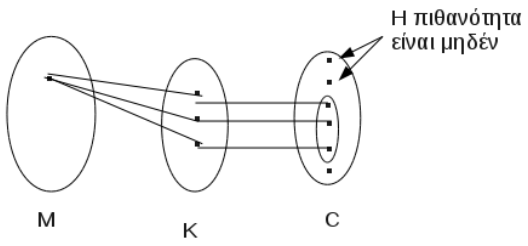
ABBA IS A GREAT GROUP

τότε $P_r[M = AB | C = QQ] = 0$ αλλά $P_r[M = AB] \neq 0$

2. Αν M χώρος αρχικού κειμένου, K χώρος κλειδιών και C χώρος κρυπτοκειμένων τότε πρέπει $|M| = |K| = |C|$ για να έχουμε τέλεια ασφάλεια.

Απόδειξη:

- Αν $|M| > |C|$ τότε κάποια μηνύματα με συγκεκριμένο κλειδί θα κρυπτογραφούνται στο ίδιο κρυπτοκείμενο, γεγονός που δεν είναι επιθυμητό.
- Αν $|M| < |C|$ τότε κάποια κρυπτοκείμενα δεν θα εμφανιστούν, άρα μπορούμε να τα αφαιρέσουμε από το C.
- Έστω $|M| = |C|$:
  Αν $|C| > |K|$ τότε για κάποιο αρχικό μήνυμα, ορισμένα κρυπτοκείμενα δεν θα εμφανιστούν ποτέ:

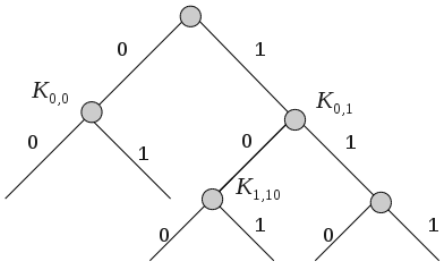


Όμως από τη σχέση $P_r[M = m | C = c] = P_r[M = m]$ προκύπτει ότι $P_r[C = c | M = m] = P_r[C = c]$ από όπου προκύπτει πως για όλα

τα c πρέπει να έχουμε την ίδια πιθανότητα, ανεξαρτήτως m. Αλλά από τα παραπών έχουμε για κάποια c η πιθανότητα να είναι μηδέν. Άτοπο.

Τέλος, αν $|C| < |K|$ τότε για κάθε δεδομένο μήνυμα, κάποια κλειδιά θα δίνουν το ίδιο κρυπτοκείμενο, γεγονός που δεν είναι επιθυμητό.

3. Εταιρεία DVD έχει $l = 2^n$ πελάτες όπου κάθε πελάτης έχει ένα DVD player.Έστω ο κάθε πελάτης c_i αντιστοιχίζεται στην ακολουθία $b_0b_1...b_{n-1}$.
Η εταιρεία δίνει κλειδιά στον κάθε πελάτη.
Έστω $keys(C_i) = \{K_{0,b_0}, K_{1,b_0b_1}, K_{2,b_0b_1b_2}, ..., K_{n-1,b_0b_1...b_{n-1}}\}$



Κάθε πελάτης αντιστοιχεί σε έναν κόμβο του δέντρου και παίρνει το αντίστοιχο κλειδί.
Η εταιρεία στέλνει στον πελάτη c_i το $E_{K_1}(K)||E_{K_3}(K)||...||E_K(M)$ (M:movie)

Ερώτηση: Τι πρέπει να στείλει η εταιρεία όταν θέλει όλοι να δουν την ταινία εκτός από έναν πελάτη c_i;

Αν θέλουμε να αποκλείσουμε τον c_i τότε δεν στέλνουμε τα κλειδιά του. Στέλνουμε τα υπόλοιπα $n = \lceil logl \rceil$ κλειδιά. Για κάθε κλειδί που δεν στέλνουμε παίρνουμε τον αδερφό του στο δέντρο.