Εθνικο Μετσοβιο Πολυτεχνειο

Σχολη Ηλεκτρολογων Μηχανικων & Μηχανικων Υπολογιστων

Σημειώσεις Διαλέξεων

Ασκήσεις

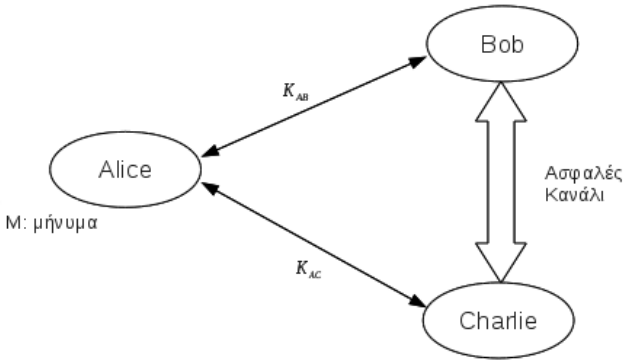
Επιμέλεια σημειώσεων:
Ελένη Λιτσα
Νίκος Μελισσαρης

Διδάσκοντες:
Στάθης Ζαχος
Άρης Παγουρτζης

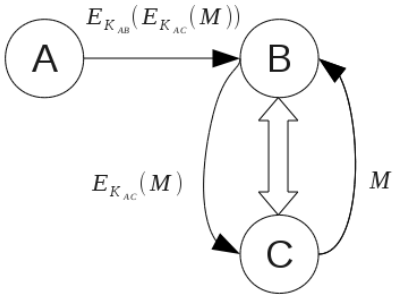
11 Νοεμβρίου 2011

1. **Απλή μοιρασιά μυστικού (Simple secret sharing)**

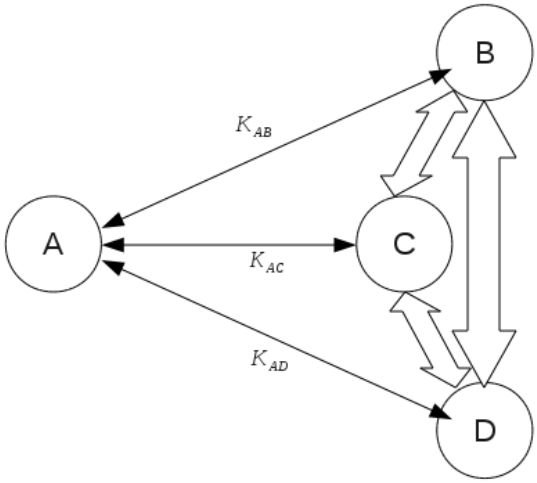
Στόχος η διανομή μυστικής πληροφορίας σε n παίκτες έτσι ώστε οποιοιδήποτε k από αυτούς να την ανακαλύψουν αλλά όχι k-1.



- Η Alice θέλει να στείλει το μυστικό και στους δύο έτσι ώστε μόνο και οι δύο μαζί να μπορούν να το διαβάσουν



- Αν n=3 παίκτες και ο στόχος είναι οι δύο να το διαβάσουν και ο ένας όχι



H Alice στέλνει σε όλους :
$E_{K_{AB}}(E_{K_{AC}}(K^R))||E_{K_{AB}}(E_{K_{AD}}(K^R))||E_{K_{AC}}(E_{K_{AD}}(K^R))||E_{K^R}(M)$
R: Random key

- Στη γενική περίπτωση έχουμε n παίκτες και ο στόχος είναι οι k από αυτούς να ανακαλύψουν την πληροφορία.Τότε χρειαζόμαστε
$\binom{n}{k}$ συνδυασμούς από κρυπτογραφήματα κλειδιών.

2. **Κρυπτοσύστημα XOR**

Κλειδί m χαρακτήρων: $K_0K_1...K_{m-1}$ όπου κάθε K_i είναι ένας ASCII χαρακτήρας, δηλαδή $K_i \in \{0,1\}^8$

plaintext: $M = M_0M_1...M_{r-1} \qquad \forall\, i \;\; M_i \in \{A, B, ..., Z\}$

cryptotext: $C = C_0C_1...C_{r-1} \qquad \forall\, i \;\; C_i = M_i \oplus K_i \; (mod\, m)$

Δείκτης Σύμπτωσης: η πιθανότητα δύο τυχαίες θέσεις ενός κειμένου να έχουν το ίδιο γράμμα

$CI_{random\, english\, text} \approx 26 \left(\frac{1}{26}\right)^2 = \frac{1}{26} \approx 0.038$

$CI_{normal\, english\, text} \approx \sum_{i=0}^{25} p_i^2 \approx 0.065$

$C_0 = M_0 \oplus K_0 \qquad C_m = M_m \oplus K_0 \qquad C_{2m} = M_{2m} \oplus K_0$

$C_0 \oplus C_m = M_0 \oplus M_m$
$C_i \oplus C_{m+i} = M_i \oplus M_{m+i}$ όταν στη θέση i και στη θέση m+i εντοπίζεται ο ίδιος χαρακτήρας τότε παίρνω μηδέν ως αποτέλεσμα.
Το ποσοστό των μηδενικών πρέπει να είναι ίσο με τον δείκτη σύμπτωσης.