Homework 2

Ασημάκης Κύδρος
ΑΕΜ: 3881
asimakis@csd.auth.gr

Μάρτιος 2023

1 Θεωρείστε ένα προβλέψιμο νόμισμα. Βρείτε ένα πείραμα ώστε το προβλέψιμο νόμισμα να μετατραπεί σε τυχαίο, δηλαδή η πιθανότητα για γράμμα ή κορώνα να είναι ίδιες.

Ρίχνουμε το νόμισμα σε δυάδες. Τα πιθανά αποτελέσματα είναι

- ΚΚ, $Pr[KK] = Pr^2[K]$
- ΓΓ, $Pr[\Gamma\Gamma] = Pr^2[\Gamma]$
- ΚΓ, $Pr[K\Gamma] = Pr[K]Pr[\Gamma]$
- ΓΚ, $Pr[\Gamma K] = Pr[K]Pr[\Gamma]$

Παρατηρούμε πως τα γεγονότα ΚΓ και ΓΚ είναι ισοπίθανα. Επομένως, μπορούμε να θέσουμε ως ΄κορώνα΄ το ΚΓ και ως ΄γράμματα΄ το ΓΚ και θα έχουμε ένα καινούριο τυχαίο νόμισμα. Τα άλλα 2 γεγονότα τα αγνοούμε, και αν προκύψουν τότε επαναλαμβάνουμε το πείραμα.

2 Υπό ποιές προϋποθέσεις θα μπορούσε το σύστημα του Καίσαρα να έχει τέλεια ασφάλεια;

Θεωρούμε κλειδιά ισομήκη του μηνύματος που κρυπτογραφείται και τυχαίως παραγόμενα από το $\mathcal{K}$.
Τότε, κρυπτογραφόντας το μήνυμα letter-by-letter με κάθε αντίστοιχο νούμερο του κλειδιού προκύπτει ένα τελείως ασφαλές σύστημα.

3 Έστω το σύστημα $\mathcal{M} = \mathcal{C} = \{0, 1, 2, ..., 100\}$, $\mathcal{K} = \{odd\ \ primes < 100\}$ με $c = m^2\ \ mod\ \ p$ όπου p το κλειδί. Εξετάστε αν το σύστημα αυτό είναι σημασιολογικά ασφαλές.

Η predicate

$$f : \mathcal{M} \to \{0, 1\}$$

$$f(m) = \begin{cases} 1, & m^2 = np + c, n \in \mathbb{N} + \{0\} \\ 0, & otherwise \end{cases}$$

αποκαλύπτει πληροφορία για το m μέσω του c καθώς δείχνει σε ποιά modulo ομάδα του p ανήκει το m^2. Συγκεκριμένα, το $m^2 \in [c]_p$, δηλαδή ισχύει $m^2 = c$ ή $m^2 = np + c$ με θετικό ακέραιο n.
Επομένως το σύστημα δεν είναι σημασιολογικά ασφαλές.