Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία
1η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 18/10/2017

6 Οκτωβρίου 2017

1η Άσκηση

Δίνεται το παρακάτω ciphertext, το οποίο γνωρίζουμε ότι έχει κρυπτογραφηθεί με το κρυπτοσύστημα Vigenère. Αποκρυπτογραφήστε το και εξηγήστε τη μέθοδο που ακολουθήσατε.

ΣΒΘΖΖΞΓΕΥΤΕΩΧΩΤΗΤΑΚΨΧΧΡΠΥΙΓΔΖΔΞΔΛΒΑΠΩΖΓΨΗΞΧΩΤΗΤΑΚΨΧΧΡΠΥ
ΙΓΔΖΜΔΦΟΚΤΓΕΗΟΝΣΣΨΖΧΧΚΔΚΑΑΚΕΖΕΣΦΟΦΣΥΞΖΨΞΗΙΔΣΨΒΧΡΨΙΦΟΠΛΛ
ΣΠΥΓΨΚΤΧΨΕΣΔΚΛΔΖΡΚΤΙΔΑΝΛΔΧΛΚΙΓΞΥΩΗΥΦΛΑΤΧΩΝΛΛΧΓΧΖΜΨΚΣΥΜΘ
ΣΝΓΑΕΞΣΠΓΒΩΖΓΨΠΣΛΛΝΔΑΑΒΕΔΣΞΩΤΩΚΦΧΜΞΜΔΑΙΕΩΔΚΑΗΟΚΧΜΣΣΨΠΓΔ
ΡΛΔΤΘΩΔΓΤΨΚΤΥΞΦΕΔΟΜΠΞΨΔΑΦΩΖΓΨΞΒΘΩΩΣΣΥΠΓΥΑΓΖΜΕΚΣΥΓΞΧΛΥΑΑ
ΣΑΛΛΠΠΔΖΞΑΞΨΠΜΙΧΣΥΜΔΕΧΥΗΞΤΛΔΠΦΟΦΣΥΔΡΔΞΩΠΝΩΤΙΔΑΗΙΩΥΑΩΧΧΚ
ΦΠΕΥΓΛΔΜΨΩΒΖΜΘΠΔΥΟΥΦΟΘΑΗΟΚΧΜΣΣΨΠΓΥΚΣΠΗΞΓΤΠ

2η Άσκηση

Να αποδείξετε ότι ισχύει η σχέση $\mathbb{E}[I_{C_k}] - \mathbb{E}[I_r] = \frac{1}{k}(\mathbb{E}[I_{\mathcal{L}}] - \mathbb{E}[I_r])$, όπου $\mathbb{E}[I_{C_k}]$ είναι η αναμενόμενη τιμή του δείκτη σύμπτωσης κρυπτοκειμένου που έχει προκύψει από κλειδί μήκους k (με όλα τα γράμματα διαφορετικά), $\mathbb{E}[I_{\mathcal{L}}]$ η αναμενόμενη τιμή του δείκτη σύμπτωσης για κείμενο γλώσσας $\mathcal{L}$, και $\mathbb{E}[I_r]$ η αναμενόμενη τιμή του δείκτη σύμπτωσης για εντελώς τυχαίο κείμενο.

3η Άσκηση

1. Σε ένα κρυπτοσύστημα που διαθέτει τέλεια μυστικότητα, είναι αναγκαίο κάθε κλειδί να επιλέγεται με την ίδια πιθανότητα; Αποδείξτε τον ισχυρισμό σας.
2. Να αποδείξετε ότι οι παρακάτω προτάσεις είναι ισοδύναμες με τη συνθήκη τέλειας μυστικότητας του Shannon:
   i. $\forall x \in \mathcal{M}, y \in \mathcal{C} : \Pr[C = y] = \Pr[C = y | M = x]$
   ii. $\forall x_1, x_2 \in \mathcal{M}, y \in \mathcal{C} : \Pr[C = y | M = x_1] = \Pr[C = y | M = x_2]$

4η Άσκηση

Η αναπαράσταση του αριθμού 2^{29} στο δεκαδικό σύστημα αποτελείται από ακριβώς εννιά διακριτά ψηφία. Χωρίς να υπολογίσετε τον αριθμό, βρείτε το ψηφίο $\{0, ..., 9\}$ που λείπει.

Υπόδειξη 1: $\forall\ a, b \in \mathbb{Z}$, $n \in \mathbb{N}^+$, *ισχύει* $ab \bmod n = (a \bmod n)(b \bmod n) \bmod n$.
Υπόδειξη 2: Προσπαθήστε να λύσετε την άσκηση χωρίς να χρησιμοποιήσετε την Υπόδειξη 2.[1]

[1] Αν με $S(x)$ συμβολίσουμε το άθροισμα των ψηφίων του αριθμού x στο δεκαδικό σύστημα, τότε $\forall x : x \equiv S(x) \pmod 9$.