Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

# Υπολογιστική Κρυπτογραφία
# 1η Σειρά Ασκήσεων

*Προθεσμία παράδοσης: 24/10/2016*

8 Οκτωβρίου 2016

## 1η Άσκηση

Δίνεται το παρακάτω ciphertext, το οποίο γνωρίζουμε ότι έχει κρυπτογραφηθεί με το κρυπτοσύστημα Vigenère. Αποκρυπτογραφήστε το με χρήση δείκτη σύμπτωσης αναπτύσσοντας πρόγραμμα σε γλώσσα προγραμματισμού της επιλογής σας (άλλοι τρόποι λύσης γίνονται δεκτοί, ενδεχομένως με μειωμένη βαθμολογία). Εξηγήστε σύντομα τη μέθοδο που ακολουθήσατε.

TLXMYJPNHHGTPJMALVGCXDXYLNFHRBTHWPWJZNKHKZNUESCSZOGKXF
EBXZXRCFXZWDTXGPKYEIYYETTMFHRUHUKALRENALFITAAAHRJVKLEBZ
ZILETPUGKFIZNALVYZIWJEEYYOLVSPWHTIRCYTSMKJCULPZPPXALREOGH
VDPXMYYKSUGKYENIGKMKTIGHPCZPXDMCWBTCIKSYYPRRWQHYH

## 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 με χαρακτήρες από το αλφάβητο της γλώσσας $\mathcal{L}$.

Ποια είναι η τιμή του $\mathbb{E}[I_r]$ αν η γλώσσα $\mathcal{L}$ έχει $t$ χαρακτήρες;

## 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

Έστω $n$ ένας θετικός ακέραιος. Ένα *Λατινικό τετράγωνο* τάξης $n$ είναι ένα $n \times n$ μητρώο $L = (l_{i,j})_{1 \leq i,j \leq n}$ με στοιχεία $l_{i,j} \in \{1, ..., n\}$, τέτοια ώστε κάθε στοιχείο του συνόλου $\{1, ..., n\}$ να εμφανίζεται ακριβώς μία φορά σε κάθε γραμμή και κάθε στήλη του $L$. Κάθε Λατινικό τετράγωνο ορίζει ένα κρυπτοσύστημα στον κειμενοχώρο $\mathcal{M} = \{1, ..., n\}$ και τον κλειδοχώρο $\mathcal{K} = \{1, ..., n\}$, όπου η κρυπτογράφηση ενός plaintext $m \in \mathcal{M}$ χρησιμοποιώντας ένα κλειδί $k \in \mathcal{K}$ ορίζεται ως $y = C_k(m) = l_{k,m}$.

1. Βρείτε ένα Λατινικό τετράγωνο τάξης 5. Χρησιμοποιώντας αυτό το μητρώο, κρυπτογραφήστε: α) το plaintext $m = 3$ με όλα τα κλειδιά, β) όλα τα plaintext με το κλειδί $k = 4$.

2. Αποδείξτε ότι ένα Λατινικό τετράγωνο ορίζει κρυπτοσύστημα που επιτυγχάνει τέλεια μυστικότητα αν το κλειδί είναι ομοιόμορφα κατανεμημένο.

   *Σημείωση: Να μην γίνει κατευθείαν χρήση του Θεωρήματος που αποδεικνύει τέλεια μυστικότητα υπό προϋποθέσεις, στην περίπτωση που οι χώροι $\mathcal{M}, \mathcal{C}, \mathcal{K}$ είναι ισοπληθικοί.*

## 5η 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: Για οποιουσδήποτε $a, b \in \mathbb{Z}$, $n \in \mathbb{N}^+$, ισχύει $ab \bmod n = (a \bmod n)(b \bmod n) \bmod n$.*