Homework 1 από Εισαγωγή

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

Μάρτιος 2023

Εκφώνηση

Έστω το ελληνικό αλφάβητο {α,β,γ,....,ω}
το οποίο έχουμε αριθμήσει διαδοχικά ως εξής:

$$\alpha \to 0$$
$$\beta \to 1$$
$$\gamma \to 2$$
$$.$$
$$.$$
$$.$$
$$\omega \to 23$$

Έστω το κρυπτοσύστημα (K, M, C) με:

$$K = [0, 24) \cap \mathbb{Z}$$
$$M = C = \{\alpha, \beta, \gamma, ..., \omega\}$$
$$E(k, m) = (index_m + k)\ mod\ 24$$
$$D(k, c) = (index_c - k)\ mod\ 24$$

Η κρυπτογράφηση λέξεων γίνεται letter-wise.

1 Με κατανομή Pr[M = $'\alpha'$] = 0.7, Pr[M = $'\omega'$] = 0.3 επί του χώρου μηνυμάτων M, υπολογίστε την Pr[C = $'\beta'$]

Είναι φανερό πως, για συγκεκριμένο k, η πιθανότητα ενός μηνύματος και της αντίστοιχης κρυπτογράφησής του συμπίπτουν, δηλαδή ισχύει

$$Pr[M =' \alpha'] = 0.7 = Pr[E(k,' \alpha')]$$
$$Pr[M =' \omega'] = 0.3 = Pr[E(k,' \omega')]$$

Επομένως πρέπει να εξετάσουμε τις περιπτώσεις όπου το k βολεύει έτσι ώστε ένα από τα δύο γράμματα να κρυπτογραφείται σε $'\beta'$.

Εύκολα φαίνεται πως για k = 1 το $'\alpha'$ κρυπτογραφείται σε $'\beta'$ και για k = 2 το $'\omega'$ κρυπτογραφείται σε $'\beta'$.

Άρα έχουμε

$$Pr[C =' \beta'] = Pr[(M =' \alpha') \cap (k = 1)] \\ +Pr[(M =' \omega') \cap (k = 2)]$$

M, K ανεξάρτητες, άρα το παραπάνω γίνεται

$$Pr[C =' \beta'] = Pr[M =' \alpha']Pr[k = 1] \\ +Pr[M =' \omega']Pr[k = 2]$$

άρα

$$Pr[C =' \beta'] = 0.7Pr[k = 1] + 0.3Pr[k = 2]$$

Στην περίπτωση όπου η κατανομή επί του χώρου των κλειδιών είναι ομοιόμορφη έχουμε

$$Pr[k] = \frac{1}{|K|} = \frac{1}{24} \Rightarrow \\ Pr[C =' \beta'] = \frac{1}{24}$$

2 Με κατανομή $\mathbf{Pr}[M =' \epsilon\nu\alpha'] = \mathbf{0.3}$, $\mathbf{Pr} = [M =' \delta\upsilon o'] = \mathbf{0.7}$ επί του χώρου μηνυμάτων, υπολογίστε την $\mathbf{Pr}[C =' \theta\pi\delta']$

Ακολουθούμε παρόμοια διαδικασία:

Υπόθεση 1) Ένα k για όλη τη λέξη.

Με το μάτι αναγνωρίζουμε πως το k = 3 κρυπτογραφεί το μήνημα $'\epsilon\nu\alpha'$ σε $'\theta\pi\delta'$, αλλά για το μήνυμα $'\delta\upsilon o'$ δεν υπάρχει k. Όντως, για να ισχύει $'\theta' = E(k,'\delta')$ πρέπει k = 4, αλλά για να ισχύει $'\pi' = E(k,'\upsilon')$ πρέπει k = 20. Αδύνατον να ισχύουν και τα δύο ταυτοχρόνως άρα δεν υπάρχει κρυπτογράφηση.

Επομένως έχουμε

$$Pr[C =' \theta\pi\delta'] = Pr[(M =' \epsilon\nu\alpha') \cap (k = 3)] \Rightarrow$$
$$Pr[C =' \theta\pi\delta'] = Pr[M =' \epsilon\nu\alpha']Pr[k = 3] \Rightarrow$$
$$Pr[C =' \theta\pi\delta'] = 0.3Pr[k = 3]$$

και αν υποθέσουμε ξανά ομοιόμορφη κατανομή στο K, τότε έχουμε

$$Pr[C =' \theta\pi\delta'] = \frac{1}{80}$$

Υπόθεση 2) Ένα k για κάθε γράμμα της λέξης.

Πρέπει για κάθε γράμμα καθεμιάς από τις 2 λέξεις να τυχαίνει το κατάλληλο κλειδί ώστε να σχηματίζεται η λέξη $'\theta\pi\delta'$. Εύκολα φαίνεται επομένως πως πρέπει να ισχύει

$$Pr[C =' \theta\pi\delta'] =$$
$$Pr[(M =' \epsilon\nu\alpha') \cap (\{k_1, k_2, k_3\} = \{3, 3, 3\})] +$$
$$Pr[(M =' \delta\upsilon o') \cap (\{k_1, k_2, k_3\} = \{4, 20, 13\})]$$

Ξέρουμε πώς τα M και K είναι ανεξάρτητα, άρα αυτό συνεπάγεται

$$Pr[C =' \theta\pi\delta'] = Pr[M =' \epsilon\nu\alpha']Pr[k = 3]^3 + \\ Pr[M =' \delta\upsilon o']Pr[k = 4]Pr[k = 20]Pr[k = 13]$$

άρα

$$Pr[C =' \theta\pi\delta'] = 0.3Pr[k = 3]^3 \\ +0.7Pr[k = 4]Pr[k = 20]Pr[k = 13]$$

Τέλος, υποθέτοντας ομοιόμορφη κατανομή στο K καταλήγουμε στο

$$Pr[C =' \theta\pi\delta'] = (\frac{1}{24})^3 = \frac{1}{13824}$$