Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ, ΜΠ)

1η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 3 Νοεμβρίου 2022

Άσκηση 1. Παρακάτω δίνεται ένα κρυπτοκείμενο της Αγγλικής κρυπτογραφημένο με τη μέθοδο της αντικατάστασης (substitution cipher).

```
ODQSOCL OW GIU BOEE QRROHOCS QV GIUR KIA QF Q DQCQSLR WIR ICL IW CQFQF EIYQE YIDJUVLR
FGFVLDF GIU SLV OCVI GIUR IWWOYL IC VXQV DICPQG DIRCOCS VI WOCP VXL JXICLF ROCSOCS
LHLRG YQEELR OF Q POFVRQUSXV YICWUFLP CQFQ BIRMLR QCP LHLRG YQEELR QFFURLF GIU VXQV
XOF IR XLR WOEL IR QYYIUCVOCS RLYIRP IR RLFLQRYX JRIKLYV LHLRG ICL IW BXOYX OF DOFFOCS
WRID VXL YIDJUVLR FGFVLD OF QAFIEUVLEG HOVQE
```

Γράψτε κώδικα σε Python, C, C++, Java, ή Haskell που θα σας βοηθήσει να σπάσετε τον κρυπτοκείμενο. Ποιο είναι το αρχικό κείμενο, και ποιο το κλειδί που χρησιμοποιήθηκε; Δείξτε τον κώδικα που αναπτύξατε (άλλοι τρόποι λύσης γίνονται δεκτοί, ενδεχομένως με μειωμένη βαθμολογία, εφ'όσον τους αναφέρετε).

Άσκηση 2. Τα παρακάτω κείμενα είναι κρυπτοκείμενα που προκύπτουν από τη χρήση affine cipher, με αλφάβητο το λατινκό. Ζητείται, χρησιμοποιώντας τις αντιστοιχίσεις μεταξύ γραμμάτων του κρυπτοκειμένου και του αρχικού κειμένου, να βρείτε τη συνάρτηση κρυπτογράφησης και αποκρυπτογράφησης.

(a) Το κρυπτοκείμενο είναι LNUWN CZCZY CWWQM HI, και τα γράμματα του κρυπτοκειμένου C και N αντιστοιχούν στο I και H, αντίστοιχα, στο αρχικό κείμενο.

(b) Το κρυπτοκείμενο είναι COGCZ JSSNO FYGCZ, και τα γράμματα του κρυπτοκειμένου S και Z αντιστοιχούν στο E και T, αντίστοιχα, στο αρχικό κείμενο.

(c) Το κρυπτοκείμενο είναι YLNNY ELQXP HSNSY N, και τα γράμματα του κρυπτοκειμένου L και N αντιστοιχούν στο N και D, αντίστοιχα, στο αρχικό κείμενο.

(d) Το κρυπτοκείμενο είναι TSDRG DOFES RGBDF MXMEX, και τα γράμματα του κρυπτοκειμένου S και G αντιστοιχούν στο U και O, αντίστοιχα, στο αρχικό κείμενο.

Άσκηση 3.

1. Σε ένα κρυπτοσύστημα που διαθέτει τέλεια μυστικότητα, είναι αναγκαίο κάθε κλειδί να επιλέγεται με την ίδια πιθανότητα; Έχει σημασία αν οι χώροι είναι ισοπληθικοί; Αποδείξτε τους ισχυρισμούς 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. $\forall x_1, x_2 \in \mathcal{M}, y \in \mathcal{C} : \Pr[C = y | M = x_1] = \Pr[C = y | M = x_2]$

Άσκηση 4.

1. Δύο φίλοι προσπαθούν να αυξήσουν την ασφάλεια του κρυπτοσυστήματος Vigenère. Σκέφτονται να επαυξήσουν το κλειδί με έναν ακέραιο αριθμό k, και σε κάθε νέα περίοδο να χρησιμοποιούν ένα νέο κλειδί, που προκύπτει ολισθαίνοντας το προηγούμενο κλειδί κατά k.

   (α) Είναι καλή η ιδέα τους; Επιχειρηματολογήστε. Υπάρχουν καλύτερες και χειρότερες επιλογές για το k;

   (β) Προτείνετε μια όσο το δυνατόν πιο αποδοτική επίθεση στο σύστημα αυτό, υποθέτοντας ότι γνωρίζετε την μέθοδο που ακολουθούν και ότι αγνοείτε μόνο το επαυξημένο κλειδί, δηλαδή την κωδική λέξη και το k.

2. Ποιο είναι το αποτέλεσμα σύνθεσης δύο κρυπτοσυστημάτων Vigenère με κλειδιά διαφορετικού μήκους;

Σημείωση: Το ερώτημα 1 και το ερώτημα 2 δεν έχουν καμία σχέση μεταξύ τους, πέραν του ότι πραγματεύονται το κρυπτοσύστημα Vigenère.

Άσκηση 5. Να γράψετε πρόγραμμα σε γλώσσα Python, C/C++, ή άλλη γλώσσα της επιλογής σας, με τις συνήθεις βιβλιοθήκες, που να δέχεται ως είσοδο κρυπτοκείμενα κρυπτογραφημένα με Vigenère και να εξάγει το πολύ 10 πιθανά plaintexts και τα αντίστοιχα κλειδιά (ένα από αυτά θα πρέπει να αντιστοιχεί ακριβώς στο σωστό, με όλα τα γράμματα σωστά). Το πρόγραμμά σας θα πρέπει να εξάγει και τον δείκτη σύμπτωσης καθενός plaintext.
Να εξηγήσετε τις βασικές ιδέες που χρησιμοποιήσατε στον κώδικά σας.

Κρυπτοκείμενο εισόδου:

```
Mlrec dwrl xur ngfg; mlr ickgre thsdk vrk wnvj: Lvrki tymga gai qnpc, peheq fcsg.
Zr qnegfsel, Wbhjk hutx untw hbbp'q, nlv kehytur, sbq mlbhezh jbxu zc- Lvnm iirp
owga e semdwp piypmes ghsx Gfw hunrqrp sbq mlr fsfgubrr, nlv ccisfrb Xfrx lrnplg,
skir smjsuxeqf-wgi ngh V npw cyw; Syq yys utxu lcl vvl lbammf ngh uvq lcve; Hrnrz
qyhwrf ydz: onx fbkwhubrt rpw hux iaq, Qgar psex mx bbupr amls, ztc lrr ts qhrr,
Aml iauipbkabt fia gfsh fmvbic owga Kbqq. Lvr emturk przma gm lkvgoyr djcz mlr emuyf:
Mlr ymfu qtc jnlwg: gai fymo abhr pygepf: mlr qcwd Zheaf pgiaw avgf eoar zbvawg.
Phqr, zw xfvxrqf, 'R ag ahx gbm dogx xb fcwy n gijrp oceeh. Chqz csy, eaq qahgbrt
jcdz vg seqcj gzbxr Gfw gbnrqvly thkvbjq; xce fc chphcfx lbybk Hb levy zwmbgh guc
kialig, nlv hux fngfk Cs tpy gfw krlxrel khnkw, haraz V wmr. Vr eol ui guyl hux khydk
kvep jnqz if wsja: Gl anr fr jc kvnep gbsuv gai Unnhm Vlprf, Yfr fxi guc yfrtx Npfazyxw,
jume kr drrj. Rzc' zngu vq loxxr, zhaz oobhrf; yfr gas' Jr yjs ahx abu lvnm wgecfuga
```

`auvaz wa hpq qyqg Zhzrq csfga eaq fwoixr, guyl kubgu jc sfr, pi nec; Gbr xuhnj lsziie bd zsehmp ucsfgl, Qnqc osnd fl gges ngh snrw, phm wgemfu vg avyj Lc fmvvic, lc fxix, gm xwaw, eaq lgh gh cvrjv.`

Η μορφή της εξόδου του προγράμματος θα πρέπει να είναι η εξής:
KEY1 PLAINTEXT1 IC1
KEY2 PLAINTEXT2 IC2
KEY3 PLAINTEXT3 IC3
KEY4 PLAINTEXT4 IC4
... (κ.ο.κ. συνολικά 10 το πολύ γραμμές αυτής της μορφής)

Σημείωση: άλλοι τρόποι λύσης γίνονται δεκτοί, ενδεχομένως με μειωμένη βαθμολογία, εφ'όσον τους αναφέρετε. Για παράδειγμα, η χρήση του online calculator του δείκτη σύμπτωσης που θα βρείτε εδώ: `https://www.dcode.fr/index-coincidence`. Η χρήση Vigenére solver δεν επιτρέπεται.

Σύντομες οδηγίες: (α) προσπαθήστε μόνοι σας, (β) συζητήστε με συμφοιτητ(ρι)ές σας, (γ) αναζητήστε ιδέες στο διαδίκτυο – με αυτή τη σειρά και αφού αφιερώσετε αρκετό χρόνο σε κάθε στάδιο! Σε κάθε περίπτωση οι απαντήσεις πρέπει να είναι *αυστηρά ατομικές*. Ενδεχομένως να σας ζητηθεί να παρουσιάσετε σύντομα κάποιες από τις λύσεις σας.

Καλή επιτυχία!