Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ)

1η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 15 Νοεμβρίου 2021

Άσκηση 1. Η Alice θέλει να επικοινωνήσει με τον φίλο της τον Bob κρυφά, αλλά η κακόβουλη Eve θέλει να υποκλέψει την συνομιλία τους και να μάθει τα σχέδια τους. Η Alice με τον Bob ξέρουν ότι κάτι σχεδιάζει η Eve και γι'αυτό αποφασίζουν να κρυπτογραφούν τα μηνύματα τους με το κρυπτοσύστημα Vigenère. Μετά από μερικά μηνύματα αντιλαμβάνονται οτι η Eve είναι αρκετά έξυπνη και έχει με κάποιο τρόπο βρει το κλειδί που χρησιμοποίησαν. Έτσι, αποφασίζουν να κρυπτογραφούν και τα κλειδιά τους έτσι ώστε η Eve να μην μπορεί να τα βρει. Για το σκοπό αυτό χρησιμοποιούν το σύστημα του Καίσαρα για να τροποποιήσουν τα κλειδιά τα οποία στη συνέχεια χρησιμοποιούν για κρυπτογράφηση με το σύστημα Vigenère.

1. Με ποια τεχνική θεωρείτε ότι η Eve κατάφερε αρχικά να αποκρυπτογραφήσει χωρίς να έχει πρόσβαση στα αρχικά κλειδιά, αλλά ξέροντας μόνο τα κρυπτοκείμενα; Μπορεί τώρα η Eve να χρησιμοποιήσει την ίδια τεχνική για να αποκρυπτογραφήσει τα μηνύματα παρά την τροποποίηση των κλειδιών; Πέτυχαν κάτι η Alice και ο Bob με την τροποποίηση των κλειδιών με το σύστημα του Καίσαρα; Εξηγήστε.

2. Μπείτε στην θέση της Eve και θέλετε να αποκρυπτογραφήσετε τα μηνύματα. Ξέρετε ότι το αρχικό κλειδί πριν την τροποποίηση με Καίσαρα είναι **cryptography**. Ξέρετε ακόμη ότι τελικό κρυπτοκείμενο είναι αυτό:

   ```
   Nd Dhy. A dcmgv yk ccob xsieewa svptdwn os ptp Kqg, url gz wazwry vaffu jj t
   mgzogk tsi os xyextrm lmb hildcmzu. B plsgp plpz oq npw dci Otikigkb usklxc.
   Egi ahr lrdrd zh g rcr qg wvox zwx hglpsqzw bxrunubydo os wpextrm cgb cik?
   ```

   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 στο σύστημα του Καίσαρα; Δείξτε τον κώδικα που αναπτύξατε (άλλοι τρόποι λύσης γίνονται δεκτοί, ενδεχομένως με μειωμένη βαθμολογία, εφ'όσον τους αναφέρετε).

3. Παραπάνω η Alice έκανε μια ερώτηση. Τώρα είστε ο Bob. Απαντήστε στην ερώτηση της! Μετά γράψτε κώδικα που θα κρυπτογραφεί την απάντηση με το ίδιο σύστημα που χρησιμοποίησε η Alice

πριν και δείξτε την κρυπτογραφημένη απάντηση. Επίσης, δείξτε τον κώδικα που αναπτύξατε (άλλοι τρόποι λύσης γίνονται δεκτοί, ενδεχομένως με μειωμένη βαθμολογία, εφ'όσον τους αναφέρετε).

Άσκηση 2. 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.

Άσκηση 3. Να αποδείξετε ότι για το κρυπτοσύστημα Vigenére 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), $\mathbb{E}[_{\mathcal{L}}]$ η αναμενόμενη τιμή του δείκτη σύμπτωσης για κείμενο γλώσσας $\mathcal{L}$, και $\mathbb{E}[_r]$ η αναμενόμενη τιμή του δείκτη σύμπτωσης για εντελώς τυχαίο κείμενο με χαρακτήρες από το αλφάβητο της γλώσσας $\mathcal{L}$.

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

Άσκηση 4. 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:

```
KUDLEZSIOGOOSMWJICKIELOLOVTDOECJZYWNCHIOAAKILDVUDWQIPJVKRPVLTLIOZATLJUCSMOIWLCKVBBLN
ZBJUCSMOIWLCKVURLYLZPZPFCVNDIYJLBENHEMCYWGVPFPAWUVHSUGQWCOBTOSFEPPEKPWLTSZZAOIIVUMCET
WUPYOXGZAIONAHZCRNBIOFACMHOBIIVUJMEZPFIIEWWYMVPDAOJWFEWVWHYRQGKBIOTYZCCRWWOIUEVZZGPEY
TSWFMPUCMOCBSKGIKCEEPPOZPGUTSWFMPUCFOFULEPPEZEEPPOZCYKIPAMABOYATSMTXAPESSQWCZPFSYSZCW
YLXOSLTVENMIYBSPWQZWNYYRZEHNQDRFOFKLTVPDCIDQETWUOCEYQYEWVBKRPIXYGPETAJAEXQWOAOMMWOSFD
OEXJFZAFORNZBEUUBULTSMXRQLOFOFNZXTJPLGZMDTWULHCVELXLOYYTLZCOMTGPTSGPYBFBKAJGZAISOAHPJ
ZCAGBVMHPTIPZYBRNPTRLSOUADTTBQOQHRCWHYISOZEYBQUZURAHPICIPFBZEPAENMNKYKFXZTBIOWAEPZLBI
OPNQQYOBFKUDSMMKVECFOFETZPISZMTOSZBIKAHTALXZPGZMLGRUAXSMTLVOLISVLTJWFXJFXKIYOTTBIOHRN
PPXAIKUDMMQUZHVHDYMDYNPBLVPVLYPFVVVPAENMBBYOHBSGBGVPEDAZNMMYCEDIWYWURLBZEENIUSZSEIMRM
```

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.

Άσκηση 5.

1. Αποδείξτε ότι το κρυπτοσύστημα της διαφάνειας 21 (Lecture 1) δεν διαθέτει τέλεια μυστικότητα αν τα κλειδιά δεν είνκαι ισοπίθανα (δείξτε το με χρήση του ορισμού του Shannon, χωρίς χρήση των ισοδύναμων συνθηκών).

2. 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.

3. 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. $\forall x_1, x_2 \in \mathcal{M}, y \in \mathcal{C} : \Pr[C = y | M = x_1] = \Pr[C = y | M = x_2]$

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*.

Καλή επιτυχία!