Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ)

1η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 14 Οκτωβρίου 2019

Άσκηση 1. Η Alice θέλει να επικοινώνησει 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. Έτσι, χρησιμοποιούν το σύστημα του Καίσαρα για να κρυπτογραφήσουν 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 κρυπτογράφηση των κλειδιών? Πέτυχαν κάτι η Alice και ο Bob με την κρυπτογράφηση των κλειδιών με Vigenère? Εξηγήστε.

2. Μπείτε στην θέση της Eve και θέλετε να αποκρυπτογραφήσετε τα μηνύματα. Ξέρετε ότι το αρχικό κλειδί πριν την κρυπτογράφηση 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. 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.

```
VVTWZARYOORLVUGHRBPQFCFDDYWGFLSELQEVOEBTARTFTWLBVUUOLFXBPBSXDJHVAHTAIFUPNV
ZNTTLESEPRDPTIPZAGZSDQURPDHDQMNTAHTHILQMHJXIARYOVCMFUAHTSIGGVFBPVJKSLELAFC
UDSTKGCAOGDLVGHNSEPRRVWTCBUGFTDZSSTVMISMCGVPAPEVNSRTECEPAOISMCGVPAPIAFZOAZ
VTCZMTYLVGSIQPZGADIAWVRXLREPZVUO
```

Άσκηση 3. 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.