Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Εργαστήριο 1 – Κρυπτανάλυση του Vigeniere

Προετοιμασία

1. Αποσυμπιέστε τα αρχεία στο compsec_pract1.zip σε ένα φάκελο της επιλογής σας (Το αρχείο αυτό βρίσκεται στην προσωπική σελίδα του διδάσκοντα).
2. Ξεκινήστε ένα τερματικό εντολών και μπείτε στον φάκελο με τα παραπάνω αποσυμπιεσμένα αρχεία
3. Ελέγξτε το περιεχόμενο του αρχείου plaintext.txt.

Ασκήσεις κρυπτανάλυσης

1. Εξερευνήστε τις δυνατότητες του *simplesub* [*-d*]

   - ποιο είναι το αλφάβητο του απλού κειμένου που δέχεται ο κρυπταλγόριθμος;

2. Αποκρυπτογραφήσετε το κρυπτοκείμενο που προέκυψε από μονοαλφαβητική αντικατάσταση:

   kiljkeffev

   Συμμετρικό κλειδί:
   Απλό κείμενο:

3. Υπολογίστε το ιστόγραμμα του **plaintext.txt** χρησιμοποιώντας το αρχείο αλφάβητου **alphabet.txt**
   (βοήθεια: εκτελέστε ./*hist* για να δείτε τη σύνταξη της εντολής)

   - ποιο είναι το πιο συχνό γράμμα;

4. Εκτελέστε πολυαλφαβητική αντικατάσταση με τον Vigeniere.
   (για κρυπτογράφηση δώστε ./*vigenere*, για αποκρυπτογράφηση, ./*vigenere -d*)

   - σημειώστε ότι η κρυπτογράφηση παράγει αρχείο **.vig**

5. Εκτελέστε κρυπτανάλυση στο κρυπτοκείμενο **ae.txt.vig**
   (βοήθεια: πρέπει να βρείτε πρώτα το μήκος του κλειδιού και μετά να "σπάσετε" το κρυπτοκείμενο σε μονοαλφαβητικά δοχεία)

   Βοηθητικά scripts:

kasiski	– Έλεγχος Kasiski
gcd	– Υπολογισμός του ΜΚΔ δυο αριθμών
polysplit	– διαμερισμός του κρυπτοκειμένου σε αριθμό μονοαλφαβητικών κρυπτοκειμένων
hist	– υπολογισμός ιστογράμματος