Κρυπτογραφία
Εργασία 2η

Κρυπτοσυστήματα ιδιωτικού κλειδιού

Ομάδα 16
Βασίλειος Κυριακόπουλος

Α.Μ.
2022201800103

Περιεχόμενα

Ερώτημα 1

Η κρυπτογράφηση βρίσκεται στο αρχείο main.py, όπου εκεί τρέχοντας τον κώδικα υλοποιούνται τα ερωτήματα 1α και 1β.

Αναλυτικά,
- Για το 1α, το αρχείο εξόδου για το υποερώτημα α.1 αντιστοιχεί στο First_File.txt, και το α.2 στο Second_File.txt, όπου υπάρχουν με τα συνοδευτικά αρχεία της άσκησης. Τα παραπάνω μπορούν να δημιουργηθούν τρέχοντας το script main.py.

- Για το 1β, τα υποκλειδιά που παράγονται από το K = a1e9 είναι:

k^1=8a67

k^2=29ad

k^3=ab46

k^4=ae19

Για το 1γ, η κρυπτογράφηση πήρε 12 ώρες και η αποκρυπτογράφηση πήρε εξίσου 12 ώρες. Screenshot δεν υπήρξε, επειδή δεν είχαμε παρατηρήσει ότι χρειάζεται και λόγω τεχνικών προβλημάτων δεν ήταν δυνατή η επαναλειτουργία του υπολογιστή που χρησιμοποιούσαμε για 12 ώρες.

Ερώτημα 2

Για την υλοποίηση του 2α, γράψαμε τον κώδικα του αρχείου cryptanalysis.py, όπου εκτυπώνει τον πίνακα γραμμικών προσεγγίσεων και τον πίνακα κατανομής διαφορών.

Στην συνέχεια για το 2β, από τους παραπάνω δύο πίνακες, με ένα μικρό script, εκτυπώσαμε τις 10 καλύτερες προσεγγίσεις σε μορφή θέσεων. Όπου, στον γραμμικό πίνακα ήταν τέσσερα 6 ή -6 στις θέσεις [3, 7], [7, 3], [11, 15], [12, 12], και έξι 4 ή -4 στις θέσεις [1, 4], [1, 10], [2, 6], [2, 13], [4, 4], [4, 13]. Στον πίνακα κατανομής διαφορών υπήρξαν επτά 6 στις θέσεις [1, 2], [2, 1], [2, 2], [3, 3], [12, 14], [13, 12], [14, 15] και τρία 4 στις θέσεις [1, 14], [3, 12], [4, 6].
Ολόκληροι οι πίνακες βρίσκονται στην παρακάτω σελίδα.

Πίνακας γραμμικών προσεγγίσεων:

```
[[ 8  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0]
 [ 0  2  2  0  4 -2  2  0  2  0 -4 -2  2  0  0  2]
 [ 0  2  0  2  0  2  4 -2  2  0  2  0 -2 -4  2  0]
 [ 0  0  2 -2  0  0  2  6  0  0  2 -2  0  0  2 -2]
 [ 0 -2  2  0 -4 -2 -2  0  2  0  0 -2  2 -4  0  2]
 [ 0  0 -4  0  0 -4  0  0  0 -4  0  0  0  0  4  0]
 [ 0  0 -2 -2  0 -4  2 -2  0  4  2 -2  0  0 -2 -2]
 [ 0 -2  0 -6  0  2  0 -2  2  0 -2  0 -2  0  2  0]
 [ 0  4  0  0 -4  0  0  0  4  0  0  0  0  4  0  0]
 [ 0  2 -2  0  0  2 -2  0 -2  4  0 -2  2  0  4  2]
 [ 0 -2  0  2  0 -2  0  2  2  4 -2  4 -2  0  2  0]
 [ 0  0 -2 -2  0  0  2  2  0  0  2  2  0  0 -2  6]
 [ 0  2  2  0  0 -2 -2  0 -2  0  0 -2 -6  0  0  2]
 [ 0  0  0  0 -4  0  4  0 -4  0 -4  0  0  0  0  0]
 [ 0  4 -2 -2  0  0 -2  2  0  0 -2  2  0 -4 -2 -2]
 [ 0 -2 -4  2  0  2  0  2  2  0 -2 -4 -2  0 -2  0]]
```

Πίνακας κατανομής διαφορών:

```
[[16  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0]
 [ 0  0  6  0  0  0  0  2  0  2  0  0  2  0  4  0]
 [ 0  6  6  0  0  0  0  0  0  2  2  0  0  0  0  0]
 [ 0  0  0  6  0  2  0  0  2  0  0  0  4  0  2  0]
 [ 0  0  0  2  0  2  4  0  0  2  2  2  0  0  2  0]
 [ 0  2  2  0  4  0  0  4  2  0  0  2  0  0  0  0]
 [ 0  0  2  0  4  0  0  2  2  0  2  2  2  0  0  0]
 [ 0  0  0  0  0  4  4  0  2  2  2  2  0  0  0  0]
 [ 0  0  0  0  0  2  0  2  4  0  0  4  0  2  0  2]
 [ 0  2  0  0  0  2  2  2  0  4  2  0  0  0  0  2]
 [ 0  0  0  0  2  2  0  0  0  4  4  0  2  2  0  0]
 [ 0  0  0  2  2  0  2  2  2  0  0  4  0  0  2  0]
 [ 0  4  0  2  0  2  0  0  2  0  0  0  0  0  6  0]
 [ 0  0  0  0  0  0  2  2  0  0  0  0  6  2  0  4]
 [ 0  2  0  4  2  0  0  0  0  0  2  0  0  0  0  6]
 [ 0  0  0  0  2  0  2  0  0  0  0  0  0 10  0  2]]
```

Ερώτημα 3

Αφού βρήκαμε τα 10 καλύτερα γραμμικά και διαφορικά χαρακτηριστικά, θα διαλέξουμε τα γραμμική χαρακτηριστικά για την υλοποίηση του 3ου ερωτήματος. Η κρυπτογράφηση έγινε με το κλειδί K = a1e9, και εμείς θέλουμε να βρούμε πιθανά κομμάτια του κλειδιού. Επομένως, μετατρέποντας τις παραπάνω θέσεις σε δεκαεξαδική μορφή, δοκιμάζουμε ανά δύο θέσεις να δημιουργήσουμε ένα κλειδί που θα μας δώσει το επιθυμητό αποτέλεσμα.