Εργασία 1

Κωσταντίνος Σαΐτας - Ζαρκιάς - 2406
Οδυσσεύς Κρυσταλάκος - 2362

14 Μαρτίου 2016

Θέμα 3

Αρχικά έγινε προσπάθεια εύρεσης του μήκους του κλειδιού που χρησιμοποιήθηκε για την κρυπτογράφηση. Χρησιμοποιώντας τον δείκτη σύμπτωσης (Index of Coincidence) που υλοποιήθηκε σε Python και έτσι βρέθηκε με μεγάλη βεβαιότητα ότι το μήκος του κλειδιού είναι 7 χαρακτήρες (IC = 0.06722).
Έτσι το κείμενο διασπάστηκε σε 7 στήλες έτσι ώστε να ισχύει η ίδια μετατόπιση σε κάθε στήλη. Κάνοντας ανάλυση συχνοτήτων των χαρακτήρων κάθε στήλης, βρέθηκαν οι πιο συχνοί χαρακτήρες κάθε στήλης. Αυτοί είναι:

- I
- Q
- T
- I
- V
- S
- V

Αν θεωρηθεί ότι αυτοί οι χαρακτήρες αντιστοιχούν στο E (που είναι το γράμμα με την υψηλότερη συχνότητα εμφάνισης), τα κλειδιά που προκύπτουν σε κάθε στήλη είναι:

- Μετατόπιση 4 άρα κλειδί E
- Μετατόπιση 12 άρα κλειδί M
- Μετατόπιση 15 άρα κλειδί P
- Μετατόπιση 4 άρα κλειδί E

- Μετατόπιση 17 άρα κλειδί R
- Μετατόπιση 14 άρα κλειδί O
- Μετατόπιση 17 άρα κλειδί R

Παρατηρείται ότι σχηματίζουν τη λέξη EMPEROR και έτσι φαίνεται πως βρέθηκε το σωστό κλειδί. Με αποκρυπτογράφηση του μηνύματος με αυτό το κλειδί, προκύπτει το σωστό κείμενο

Αν το κλειδί που προέκυπτε από την παραπάνω ανάλυση ήταν λάθος, θα δοκιμάζονταν άλλοι συνδιασμοί βρίσκοντας τα δεύτερα πιο συχνά εμφανιζόμενα γράμματα κλπ.

Θέμα 4

Εφόσον χρησιμοποιείται το σύστημα μετατόπισης, τα πιθανά κλειδιά είναι μόλις 23. Επομένως, με επίθεση ωμής βίας μπορούν να δοκιμαστούν όλα τα πιθανά κλειδιά. Βλέποντας τα αποτελέσματα, παρατηρείται ότι το κείμενο που προκύπτει χρησιμοποιώντας το κλειδί 3 είναι:
ΜΗΔΕΙΣΑΓΕΩΜΕΤΡΗΤΟΣΕΙΣΙΤΩΜΟΥΤΗΝΣΤΕΓΗΝ.
Αντίθετως, το κείμενα που προκύπτουν από τα υπόλοιπα κλειδιά δεν έχουν κάποιο νόημα. Έτσι έχουμε βρεθεί ότι το κλειδί είναι 3 και το κείμενο ΜΗΔΕΙΣ ΑΓΕΩΜΕΤΡΗΤΟΣ ΕΙΣΙΤΩ ΜΟΥ ΤΗΝ ΣΤΕΓΗΝ.

Θέμα 7

Χρησιμοποιήθηκε επίθεση ωμής βίας, δηλαδή δοκιμάστηκαν ως κλειδιά όλες οι λέξεις που βρίσκονται στο english.txt. Μετά απο αρκετές προσπάθειες βρέθηκε το κλειδί: secret.