“ΚΡΥΠΤΟΓΡΑΦΙΑ”

Άσκηση :

Το plaintext ειναι το παρακάτω :
ΕΡΧΟΜΑΣΤΕ ΑΠΟ ΜΙΑ ΣΚΟΤΕΙΝΗ ΑΒΥΣΣΟ ΚΑΤΑΛΗΓΟΥΜΕ ΣΕ ΜΙΑ ΣΚΟΤΕΙΝΗ ΑΒΥΣΣΟΣΟ ΜΕΤΑΞΥ ΦΩΤΕΙΝΟ ΔΙΑΣΤΗΜΑ ΤΟ ΛΕΜΕ ΖΩΗ ΕΥΘΥΣ ΩΣ ΓΕΝΝΗΘΟΥΜ ΕΑΡΧΙΖΕΙ ΚΑΙ Η ΕΠΙΣΤΡΟΦΗ ΤΑΥΤΟΧΡΟΝΑ ΤΟ ΞΕΚΙΝΗΜΑ ΚΑΙ Ο ΓΥΡΙΣΜΟΣ ΚΑΘΕ ΣΤΙΓΜΗ ΠΕΘΑΙΝΟΥΜΕ ΓΙΑΥΤΟ ΠΟΛΛΟΙ ΔΙΑΛΑΛΗΣΑΝ ΣΚΟΠΟΣ ΤΗΣ ΖΩΗΣ ΕΙΝΑΙ Ο ΘΑΝΑΤΟΣ ΜΑ ΚΑΙ ΕΥΘΥΣΩΣ ΓΕΝΝΗΘΟΥΜΕ ΑΡΧΙΖΕΙ ΚΑΙ Η ΠΡΟΣΠΑΘΕΙΑ ΝΑ ΔΗΜΙΟΥΡΓΗΣΟΥΜΕ ΝΑ ΣΥΝΘΕΣΟΥΜΕ ΝΑ ΚΑΝΟΥΜΕ ΖΩΗ ΤΗΝ ΥΛΗ ΓΙΑΥΤΟ ΠΟΛΛΟΙ ΔΙΑΛΑΛΗΣΑΝ ΣΚΟΠΟΣ ΤΗΣ ΕΦΗΜΕΡΗΣ ΖΩΗΣ ΕΙΝΑΙ Η ΑΘΑΝΑΣΙΑ

Η μεθοδολογία που ακολουθήσαμε είναι η εξής :

Αρχικά έχουμε στόχο να εντοπίζουμε το μήκος του κλειδιού , αυτό θα το πετύχουμε βρίσκοντας patterns μέσα στο κείμενο μας , Εμεις στη συγκεκριμένη περίπτωση ελέγξαμε 3πλετες γραμμάτων . Για κάθε τέτοια τριπλέτα βλέπουμε μετά απο πόσες θέσεις ξαναεμφανίζεται και υποθέτουμε οτι όλες αυτες οι αποστάσεις (ή οι περισσότερες) ειναι πολλαπλάσια του κλειδιού μας Το αποτέλεσμα είναι το παρακάτω

```
Χ Ω Τ  12 30
Ω Τ Η  13 30
Τ Η Τ  14 30
Η Τ Α  15 30
Τ Α Κ  16 30
Α Κ Ψ  17 30
Κ Ψ Χ  18 30
Ψ Χ Χ  19 30
Χ Χ Ρ  20 30
Χ Ρ Π  21 30
Ρ Π Υ  22 30
Π Υ Ι  23 30
Υ Ι Γ  24 30
Ι Γ Δ  25 30
Γ Δ Ζ  26 30
Ω Ζ Γ  36 140
Ω Ζ Γ  36 210
Ζ Γ Ψ  37 140
Ζ Γ Ψ  37 210
Σ Σ Ψ  70 145
Σ Σ Ψ  70 290
Χ Χ Κ  74 255
Δ Κ Α  77 130
Φ Ο Φ  86 220
Ο Φ Σ  87 220
Φ Σ Υ  88 220
Ι Ι Φ  104 200
Ι Φ Ο  105 200
Ψ Κ Τ  115 115
Τ Ι Δ  129 190
Ι Δ Α  130 190
Κ Σ Υ  161 105
Σ Υ Μ  162 130
Ω Ζ Γ  176 70
Ζ Γ Ψ  177 70
Α Η Ο  209 145
Η Ο Κ  210 145
Ο Κ Χ  211 145
Κ Χ Μ  212 145
Χ Μ Σ  213 145
Μ Σ Σ  214 145
Σ Σ Ψ  215 145
Σ Ψ Π  216 145
```

Βλέπουμε οτι έχουμε 30,140,210,220,145 κλπ όλα ειναι πολλαπλάσια του 5 και είναι το πρώτο μήκος που θα δοκιμάσουμε (και θα είμαστε τυχεροί) αν δεν βρισκαμε αποτέλεσμα θα δοκιμαζαμε για keylenght=6,10 …

Βρίσκοντας απο site τις συχνότητες εμφάνισης των γραμμάτων της ελληνικής αλφαβήτου τις αποθηκεύουμε και πάμε να βρούμε τις συχνότητες των γραμμάτων του ciphertext όμως το μελετάμε σαν στήλες , δηλαδή θεωρουμε κειμενο με γράμματα μόνο απο την 1η , 6η , 11η κτλ σειρά στη συνέχεια μόνο απο την 2η,7η,12η κτλ σειρά.

Κρατάμε τις συχνοτητες κάθε γράμματος κάθε στήλης και απο την 1η στήλη πάμε να βρούμε τη μετατόπιση Κ1 του κλειδιού μας . Πολλαπλασιαζουμε κάθε συχνότητα με την συχνότητα του ελληνικού αλφαβήτου και υστερα προσθέτουμε , το κάνουμε αυτό για όλες τις μετατοπίσεις 0-23 και κρατάμε το μέγιστο , το οποίο είναι και το ζητούμενο

Ακολουθούμε ακριβώς την ίδια τακτική για τα υπόλοιπα 4 στοιχεία του κλειδιού μας και σαν πρώτο αποτέλεσμα έχουμε αυτό `13 9 13 15 18` και μας δίνει σαν plaintext το εξής

ΕΡΤΟΜΑΣΠΕΑΠΟΙΙΑΣΚΜΤΕΙΝΔΑΒΥΣΟΟΚΑΤΧΛΗΓΟΡΜΕΣΕΙΙΑΣΚΜΤΕΙΝΔΑΒΥΣΟΟΣΟΜΒ
ΤΑΞΥΣΩΤΕΙΚΟΔΙΑΟΤΗΜΑΠΟΛΕΜΒΖΩΗΕΡΘΥΣΩΟΓΕΝΝΔΘΟΥΜΒΑΡΧΙΓΕΙΚΑΖΗΕΠΙΟΤΡ
ΟΦΔΤΑΥΤΜΧΡΟΝΧΤΟΞΕΗΙΝΗΜΧΚΑΙΟΩΥΡΙΣΙΟΣΚΑΕΕΣΤΙΩΜΗΠΕΕΑΙΝΟΡΜΕΓΙΧΥΤΟΠ
ΜΛΛΟΙΑΙΑΛΑΘΗΣΑΓΟΚΟΠΟΟΤΗΣΖΦΗΣΕΙΚΑΙΟΘΧΝΑΤΟΟΜΑΚΑΖΕΥΘΥΟΩΣΓΕΚΝΗΘΟΡ
ΜΕΑΡΤΙΖΕΙΗΑΙΗΠΞΟΣΠΑΕΕΙΑΝΧΕΗΜΙΜΥΡΓΗΟΟΥΜΕΚΑΣΥΝΕΕΣΟΥΙΕΝΑΚΧΝΟΥΜΒΖΩ
ΗΤΔΝΥΛΗΩΙΑΥΤΜΠΟΛΛΜΙΔΙΑΘΑΛΗΣΧΝΣΚΟΝΟΣΤΗΟΕΦΗΜΒΡΗΣΖΦΗΣΕΙΚΑΙΗΑΕΑΝΑΣ
ΖΑ .

Αυτο το αποτέλεσμα μας θυμίζει αρκετα ελληνικές λέξεις και παρατηρούμε οτι η πρώτη λέξη θα μπορούσε να είναι ερχομαστε οποτε αλλαζουμε το Κ3 απο 13 σε 10 και καταλήγουμε στο ζητούμενο μας !!