Εργαστήριο 1

Κρυπτανάλυση του Vigeniere

Βασίλειος Κάτος
2009/10

Πολυαλφαβητική αντικατάσταση

- μετάθεση με λέξη κλειδί

απλό	α	ρ	ν	α	κ	ι	α	σ	π	ρ	ο	κ	α	ι	π	α	χ	υ
+κλειδί	λ	υ	κ	ο	ς	λ	υ	κ	ο	ς	λ	υ	κ	ο	ς	λ	υ	κ
κρυπτοκ.	μ	ν	ψ	π	δ	υ	φ	δ	η	λ	β	ζ	λ	ω	κ	μ	ς	ζ

- Το μέγεθος του κλειδιού καθορίζει τον αριθμό αλφάβητων: 5. Αυτό είναι και η *περίοδος* του κρυπταλγόριμου

Κρυπτοκείμενο

yixdepvwzpwxvzkeykrrjtyykssjlgjqguizyilieauezftvim
uimzpanzgnyeyjikexukerjjgcpznssfrzywoeexfaokl
gjhkmszvhsfvkzrbvwzzkgksxjxuklkjggdetumyxizk
mtxiicectlgekkuxurpzvvzyicrcbrxojtgzhlfvmfsjjwatl
gjqusmrvtnfrkjetugudtakixtlogwcymiyexvqujxuwx
keyyvhlfvzyilieauggisajirwvglhoezuczkjmsgsxkmtx
zgkjxvimfsjjjxfqgeszyixvgifytkvejircmtxxnvqueaok
lbrxguhkuetuxnvrjzwggtkrvoekhvjuiivrcoekndviklk
mezdsxvgudtrvblieaumtmsrmiyvbvfvzzrmfviceod
mtxxuvbvfvzxsuuwoesxuixksiceodzgkfgtolissklkiib
vravslkitklkjesvkufhyrvktmxtpkumtrrjfyzjibvvgcxo
diy

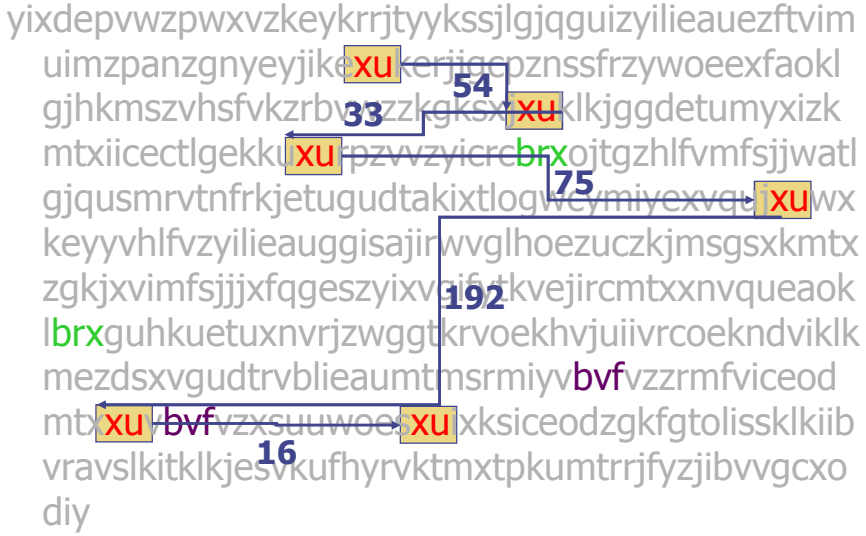
Κρυπτανάλυση του Vigenère

- 1ος Στόχος
  - Εύρεση του μήκους του κλειδιού
- 2ος Στόχος
  - Διαμερισμός του προβλήματος σε μονοαλφαβητικές αντικαταστάσεις

Ο έλεγχος του Kasiski

- Εύρεση επαναλαμβανομένων μοτίβων στο κρυπτοκείμενο
- Καταγραφή αποστάσεων
- Το μήκος του κλειδιού θα πρέπει να είναι κοινός παράγοντας
  - Εύρεση ΜΚΔ.

Κρυπτοκείμενο



Υποψήφια μήκη κλειδιών

- gcd(54,33)=gcd(33,75)=gcd(75,192)
  =gcd(33,192)=3
- gcd(192,16)=16
- gcd(16,54)=2