

| | |
|------------------------------------|--|
| | |
| <p>Βασίλειος Κάτος 2009/10</p> | <h1 style="text-align: center;">Εργαστήριο 1</h1> <p style="text-align: center;"><i>Κρυπτανάλυση του Vigeniere</i></p> <p style="text-align: right;">1</p> |

| | | | | | | | |
|----------|--|------|-------------------------------------|---------|-------------------------------------|----------|-------------------------------------|
| | <h2 style="text-align: center;">Πολυαλφαβητική αντικατάσταση</h2> | | | | | | |
| | <ul style="list-style-type: none"> ▪ μετάθεση με λέξη κλειδί <table border="1" style="margin-left: 40px; border-collapse: collapse;"> <tr> <td style="padding: 2px;">απλό</td> <td style="padding: 2px;">α ρ ν α κ ι α σ π ρ ο κ α ι π α χ υ</td> </tr> <tr> <td style="padding: 2px;">+κλειδί</td> <td style="padding: 2px;">λ υ κ ο ς λ υ κ ο ς λ υ κ ο ς λ υ κ</td> </tr> <tr> <td style="padding: 2px;">κρυπτοκ.</td> <td style="padding: 2px;">μ ν ψ π δ υ φ δ η λ β ζ λ ω κ μ ς ζ</td> </tr> </table> ▪ Το μέγεθος του κλειδιού καθορίζει τον αριθμό αλφάβητων: 5. Αυτό είναι και η <i>περίοδος</i> του κρυπταλγόριθμου | 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 |
| 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 | | | | | | |

| | |
|--|--|
| | <h2>Κρυπτοκείμενο</h2> |
| | <p>yixdepvwzprwxvzkeykrrjtyykssjlgjqguizyilieauezftvim uimzpanzgnyeeyjikexukerjjgcpznssfrzywoeexfaokl gjhkmszvhsfvkzrbvwzzkgksxjxuklkjggdetumyxizk mtxiiectlgekkuurpzvvzyicrcbrxojtgzhlfvmfsjjwatl gjqusmrvtnfrkjetugudtakixtlogwcymiyexvqujxuwx keyyvhlfvzyilieauggisajirwvglhoezuczkjmsgsxkmtx zgkjxvimfsjjxfqgeszyixvgifytkvejircmtxxnvqueaok lbrxguhkuetuxnvrjzwwggtkrvoekhvjuivrcoekndviklk mezdsxvgudtrvblieaumtmsrmiyvbvfvzrmfviceod mtxxuvbvfzxsuuwoesxuiixsiceodzgkfgtolissklkiib vravslkitklkjесvkufhyrvktmxtpkumtrrfyzjibvvgcxo diy</p> |

| | |
|--|---|
| | <h2>Κρυπτανάλυση του Vigenère</h2> |
| | <ul style="list-style-type: none">■ 1ος Στόχος<ul style="list-style-type: none">■ Εύρεση του μήκους του κλειδιού■ 2ος Στόχος<ul style="list-style-type: none">■ 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

yixdepvwzpwvxzkeykrrjtyykssjlgjqguizyilieauezftvim
uimzpanzgnyeeyjike **xu** kerjigcpznssfrzywoexfaokl
gjhkmszvhsvfkzrbvzzkgsx **54** **xu** klkjggdetumyxizk
mtxiicectlgckk **33** **xu** pzvvzyicere **brx** oitgzhlfvmfsjjwatl
gjqusmrvtnfrkjetugudtakixtlogwecymiyexvq **75** **xu** wx
keyyvhlfvzyilieauggisajirwvglhoezuczkjmsgsxkmtx
zgkxvimfsjjjxfqgeszyixv **192** tkvejircmtxxnvqueaok
brxguhkuetuxnvrjzwwgtkrvoekhvjuiivrcoekndvikl
mezdsxvgudtrvblicauamtmsrmiyv **bvf**vzzrmfviceod
mt **xu** **bvf**vzxsuuwoe **xu** xksiceodzgkfgtolissklkiib
vrvslkitklkjesvkufhyrvktmxtpkumtrrfyzjibvvgcxo
diy

Υποψήφια μήκη κλειδιών

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