**Φύλλο/α Εργασίας Εργαστηρίου/ων**

**Φύλλο εργασίας 3: Κρυπτογράφηση – Ο αλγόριθμος Vigenère (Βιζενέρ)**

Εδώ τα πράγματα δυσκολεύουν κάπως και το κλειδί που μας δείχνει το γράμμα που θα χρησιμοποιήσω αντί του απλού κειμένου δίνεται από μια λέξη ή μια φράση. Ο κρυπτογράφος έχει μπροστά του τον πίνακα που ακολουθεί και για κάθε γράμμα α**ντικαθιστά από τη στήλη που του υποδεικνύει η λέξη κλειδί.**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Α** | **Β** | **Γ** | **Δ** | **Ε** | **Ζ** | **Η** | **Θ** | **Ι** | **Κ** | **Λ** | **Μ** | **Ν** | **Ξ** | **Ο** | **Π** | **Ρ** | **Σ** | **Τ** | **Υ** | **Φ** | **Χ** | **Ψ** | **Ω** |
| **Α** | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω |
| **Β** | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α |
| **Γ** | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β |
| **Δ** | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ |
| **Ε** | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ |
| **Ζ** | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε |
| **Η** | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ |
| **Θ** | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η |
| **Ι** | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ |
| **Κ** | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι |
| **Λ** | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ |
| **Μ** | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ |
| **Ν** | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ |
| **Ξ** | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν |
| **Ο** | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ |
| **Π** | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο |
| **Ρ** | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π |
| **Σ** | Σ | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ |
| **Τ** | Τ | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ |
| **Υ** | Υ | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ |
| **Φ** | Φ | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ |
| **Χ** | Χ | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ |
| **Ψ** | Ψ | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ |
| **Ω** | Ω | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ |

Έτσι αν η λέξη κλειδί είναι «ΓΡΙΦΟΣ» και το ΑΚ: «ΔΕΝ ΜΟΥ ΑΡΕΣΕΙ» ο κρυπτογράφος για να αντικαταστήσει το Δ θα κοιτάξει στην στήλη του Γ και θα το αντικαταστήσει με το γράμμα που συναντά σε αυτή τη γραμμή άρα με το Ζ. Για το Ε θα κοιτάξει στη στήλη του Ρ και θα βρει το γράμμα Φ κτλ.. Όταν θα εξαντληθούν τα γράμματα της λέξης κλειδί θα συνεχίσει γυρνώντας στην αρχή κι επομένως κοιτώντας πάλι στη στήλη του Γ. Προκύπτει επομένως το ΚΚ: ΖΦΦΘΕΝΓΙΝΞΤΒ

**Ερώτηση**:Θυμηθείτε πως η συχνότητα εμφάνισης των γραμμάτων του ΚΚ μας βοηθούσε να βγάζουμε συμπεράσματα για το ΑΚ. Εδώ μπορεί να μας δώσει αντίστοιχα πληροφορία; Τι αναπαριστά το πρώτο Φ και τι το δεύτερο στο ΚΚ;

**Απάντηση**:………………………………………………………………………………………………………………………………………………….

……………………………………………………………………………………………………………………………………………………………………

……………………………………………………………………………………………………………………………………………………………………

**Ερώτηση**: Από τι εξαρτάται τώρα ο χώρος κλειδιού;

**Απάντηση**:………………………………………………………………………………………………………………………………………………….

……………………………………………………………………………………………………………………………………………………………………

……………………………………………………………………………………………………………………………………………………………………

**1η Δραστηριότητα (10 πόντους για την 1η ομάδα για κάθε απάντηση -2 για κάθε επόμενη):**

Με τη βοήθεια του αλγόριθμου Vigenère (Βιζενέρ) και με κλειδί τη λέξη «ΟΧΙ» κρυπτογραφήστε τις παρακάτω φράσεις

α) Η ΑΣΦΑΛΕΙΑ ΑΥΞΗΘΗΚΕ

...……….……………………………………………………………………… ……………………………………………………………………………………………………………………………

β) ΓΙΑ ΥΠΟΛΟΓΙΣΤΗ ΕΥΚΟΛΟ

…………………………………………………………………………………..…………………………………………………………………………………

**2η Δραστηριότητα (10 πόντους για την 1η ομάδα για κάθε απάντηση -2 για κάθε επόμενη)**

Τώρα είστε Κρυπταναλυτές/τριες. Γνωρίζετε πως το κλειδί είναι η λέξη «ΝΑΙ» και ο ίδιος αλγόριθμος. Αποκρυπτογραφήστε τη.