**Φύλλο/α Εργασίας Εργαστηρίου/ων**

**Φύλλο εργασίας 1: Κρυπτογράφηση – Ο κώδικας του Καίσαρα**

Η πιο απλή και γνωστή τεχνική κρυπτογράφησης ακολουθεί έναν απλό τρόπο αντικατάστασης όπου το κάθε γράμμα του απλού κειμένου αντικαθίσταται από ένα γράμμα μετά από σταθερή μετατόπιση στο αλφάβητο. Για παράδειγμα, αν το κλειδί είναι 5, το γράμμα Α αντικαθίσταται από το Ζ το Β από το Η και ούτω καθεξής. Έχει πάρει το όνομά της από τον Ιούλιο Καίσαρα, καθώς αναφορές δείχνουν πως τη χρησιμοποιούσε για την αλληλογραφία του.

Η αρίθμηση των γραμμάτων μπορεί να μας βοηθήσει να κάνουμε γρήγορα την κρυπτογράφηση και αποκρυπτογράφηση.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Α** | **Β** | **Γ** | **Δ** | **Ε** | **Ζ** | **Η** | **Θ** | **Ι** | **Κ** |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| **Λ** | **Μ** | **Ν** | **Η** | **Ο** | **Π** | **Ρ** | **Σ** | **Τ** | **Υ** |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| **Φ** | **Χ** | **Ψ** | **Ω** |  |  |  |  |  |  |
| 20 | 21 | 22 | 23 |  |  |  |  |  |  |

Έτσι με Κλειδί=3 έχουμε Α-> Δ και η νέα αρίθμηση γίνεται:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Α** | **Β** | **Γ** | **Δ** | **Ε** | **Ζ** | **Η** | **Θ** | **Ι** | **Κ** |
| 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| Λ | **Μ** | **Ν** | **Η** | **Ο** | **Π** | **Ρ** | **Σ** | **Τ** | **Υ** |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| **Φ** | **Χ** | **Ψ** | **Ω** |  |  |  |  |  |  |
| 0 | 1 | 2 | 3 |  |  |  |  |  |  |

Με ΑΚ: Απλό Κείμενο και ΚΚ: Κρυπτογραφημένο Κείμενο.

Κρυπτογράφο ονομάζουμε τον ειδικό που υλοποιεί τη διαδικασία κρυπτογράφησης δηλαδή

μετατρέπει το Απλό Κείμενο σε Κρυπτογραφημένο Κείμενο. Έτσι στο παράδειγμά μας ο Κρυπτογράφος κάνει την πράξη (ΚΚ= ΑΚ + Κλειδί) mod 24. To mod μας κάνει το υπόλοιπο της ακέραιας διαίρεσης μεταξύ 2 ακεραίων.

**Ερώτηση:** Γιατί χρειάζεται να διαιρούμε με το 24;

# Απάντηση:…………………………………………………………………………………………………………………………………

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

# …………………………………………………………………………………………………………………………………………………..

Κρυπταναλυτή/τρια ονομάζουμε τον ειδικό που υλοποιεί την αντίστροφη διαδικασία δηλαδή

μετατρέπει το Κρυπτογραφημένο Κείμενο σε Απλό Κείμενο. Έτσι. στο παράδειγμά μας ο/η Κρυπταναλυτής.τρια κάνει την πράξη (ΑΚ= ΚΚ - Κλειδί) mod 24.

Με **κλειδί** 8 κρυπτογραφούμε τη φράση όπως φαίνεται παρακάτω. ΑΚ: Θα συναντηθούμε στις δέκα

ΚΚ: ΠΙΒΔΦΙΦΓΟΠΨΔΥΝΒΓΡΒΜΝΣΙ

**Ερώτηση:** Γιατί προτιμούμε να μην έχουμε κενά στο ΚΚ;

# Απάντηση:…………………………………………………………………………………………………………………………………………

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

# ……………………………………………………………………………………………………………………………………………………………

**Ερώτηση:** Ποια η % συχνότητα εμφάνισης του κάθε γράμματος στο ΚΚ; Τι πληροφορία μας δίνει για το ΑΚ και πως μπορεί να την αξιοποιήσει ο/η Κρυπταναλυτής/τρια;

# Απάντηση:…………………………………………………………………………………………………………………………………………..

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

# ……………………………………………………………………………………………………………………………………………………………..

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

# Τώρα είστε Κρυπταναλυτές/τριες. Γνωρίζετε ότι ο Κώδικας είναι αυτός του Καίσαρα και το κλειδί που χρησιμοποιήθηκε είναι το 8. Αποκρυπτογραφήστε τις παρακάτω φράσεις και μεταφορτώστε τις απαντήσεις στην ηλεκτρονική πλατφόρμα που θα σας υποδείξει ο/η εκπαιδευτικός.

α) ΙΔΓΨΝΡΦΙΡΥΔΒΓΡΣΨ

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

β) ΩΙΑΝΓΟΤΝΕΘΦΨΙΥΝΒΘΒ

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

γ) ΜΘΒΝΓΨΛΑΙΥΥΙΒΓΨΦΦΡΣΨ

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

δ) ΥΨΔΙΑΝΒΝΡΟΣΑΔΩΓΨΛΑΙΕΟΒΟ

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

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

Τώρα είστε Κρυπτογράφοι. Χρησιμοποιήστε τον κώδικα του Καίσαρα με κλειδί 7 για να δημιουργήσετε το ΚΚ των παρακάτω φράσεων.

α) ΑΥΤΗ Η ΣΥΝΑΛΛΑΓΗ ΜΕ ΤΗΝ ΤΡΑΠΕΖΑ ΕΙΝΑΙ ΑΣΦΑΛΗΣ

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

β) ΜΠΟΡΕΙΤΕ ΤΩΡΑ ΝΑ ΣΤΕΙΛΕΤΕ ΤΟΝ ΠΡΟΣΩΠΙΚΟ ΣΑΣ ΚΩΔΙΚΟ

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

γ) ΜΟΝΟ ΕΣΕΙΣ ΘΑ ΒΛΕΠΕΤΕ ΤΗΝ ΗΜΕΡΟΜΗΝΙΑ ΓΕΝΝΗΣΗΣ

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

δ) ΤΟ ΠΡΟΪΟΝ ΠΡΟΣΤΕΘΗΚΕ ΣΤΟ ΚΑΛΑΘΙ ΣΑΣ

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