**Φύλλο Eργασίας ΙΙ**

**ΚΡΥΠΤΟΓΡΑΦΙΑ- *χρήση κλειδιού***

*Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης (cipher) και ενός κλειδιού κρυπτογράφησης (key). Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στη μυστικότητα του κλειδιού κρυπτογράφησης*

**Δραστηριότητα 1**

https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcTeUk3nIT2JdIss2bQ4wL97iX7FapoigtCwSXWrEUHneyIoa0QJfQΠαρακολουθήστε το video που αφορά τον κώδικα του Ιούλιου Καίσαρα http://www.youtube.com/watch?v=sMOZf4GN3oc#t=58

**Πώς κρυπτογραφούσε τα μηνύματα του ο Ιουλιος Καίσαρας**

Παράδειγμα:

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

Μπορείτε να αποκρυπτογραφήσετε τα παρακάτω μηνυματα?

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

*Με την πάροδο του χρόνου οι κρυπταναλυτές έβρισκαν σχετικά εύκολα τρόπους να ξεκλειδώνουν τέτοια μηνύματα κοιτάζοντας την συχνότητα εμφάνισης των γραμμάτων στα γνωστά κείμεναΈτσι δημιουργήθηκε η ανάγκη για νέες μεθόδους πιο πολύπλοκες και συνεπώς πιο δύσκολες, χρησιμοποήση ενός κλειδιού*.

**Δραστηριότητα 2**

*Ένα απο τα βασικά προβλήματα στην κρυπτογραφία είναι το πως θα γίνει με ασφάλεια η ανταλλαγή του* ***κλειδιού κρυπτογράφησης*** *μεταξύ δυο ατόμων. Έχει επικρατήσει στην βιβλιογραφία τα άτομα που θέλουν να ανταλλάξουν κρυπτογραφημένα μηνύματα να ονομάζονται Αλίκη και Μπόμπ.*

**Η Αλίκη θέλει να στείλει ένα γράμμα στο φίλο της τον Μπομπ. Επειδή δεν θέλει να παραβιαστεί το γράμμα της το κλειδώνει σε ένα κιβώτιο με ένα λουκέτο και ταχυδρομεί το κιβώτιο στον Μπομπ. Πως θα μπορέσει όμως ο Μπόμπ να ανοίξει το κιβώτιο αφού δεν έχει το κλειδί του λουκέτου της Αλίκης;**

**Δραστηριότητα 3**

Παίζουμε στην τάξη το παιχνίδι **public key encryption** από : <http://csunplugged.org/public-key-encryption> Παίζοντας το παιχνίδι θα γίνει φανερό ότι η ανταλλαγή κλειδιών, μπορεί να γίνει εξ αποστάσεως χωρίς τα δυο άτομα να συναντηθούν.



**Δραστηριότητα 4**

**Στη σύγχρονη όμως εποχή η κρυπτογράφηση αποτελεί πλέον στοιχείο της καθημερινής ζωής, από τη λειτουργία των κινητών τηλεφώνων ως τη διενέργεια τραπεζικών πράξεων μέσω του Διαδικτύου.**

Ακολουθώντας το σύνδεσμο <http://www.saferinternet.gr/index.php?objId=Category37&childobjId=Category114&parentobjId=Page2> από την ιστοσελίδα του saferinternet.gr.

Ή παρακολουθήστε το video στην ιστοσελίδα:

 https://www.globalsign.com/ssl-information-center/what-is-an-ssl-certificate.html

**Να απαντήσετε στην ερώτηση:**

**Πώς ξέρω ότι η συναλλαγή που θα κάνω στη συγκεκριμένη ιστοσελίδα είναι ασφαλή?**



**Δραστηριότητα 5**

Να κατασκευάσετε έναν εννοιολογικό χάρτη για τον όρο **«ΚΡΥΠΤΟΓΡΑΦΙΑ» ή τι είναι το SSL**

**Δραστηριότητα 6**

Να κωδικοποιήσετε το μήνυμα σας. Στη συνέχεια θα παραδόσετε στον καθηγητή σας το κωδικοπιημένο μήνυμα και θα πάρετε ένα άλλο κωδικοποιημένο μήνυμα από τον καθηγητή σας , το οποίο θα προσπαθήσετε να αποκωδικοποιήσετε.

**ΠΑΡΑΔΕΙΓΜΑ -----Μέθοδος κωδικοποίησης και αποκωδικοποίησης:**

Διαλέξτε μια λέξη για να είναι το κλειδί σας. Η λέξη πρέπει να 5 ή 6 γράμματα και να μην έχει γραμματα που επαναλαμβάνονται. Π.χ. **ΠΟΤΗΡΙ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Π** | **Ο** | **Τ** | **Η** | **Ρ** | **Ι** |
| **Θ** | **Α** | **Σ** | **Υ** | **Ν** | **Α** |
| **Ν** | **Τ** | **Η** | **Θ** | **Ο** | **Υ** |
| **Μ** | **Ε** | **Σ** | **Τ** | **Ο** | **Δ** |
| **Ε** | **Ν** | **Τ** | **Ρ** | **Ο** |  |

Αντιμεταθέτουμε τις στήλες ώστε η λέξη κλειδί να είναι τοποθετημένη αλφαβητικα

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Η** | **Ι** | **Ο** | **Π** | **Ρ** | **Τ** |
| **Υ** | **Α** | **Α** | **Θ** | **Ν** | **Σ** |
| **Θ** | **Υ** | **Τ** | **Ν** | **Ο** | **Η** |
| **Τ** | **Δ** | **Ε** | **Μ** | **Ο** | **Σ** |
| **Ρ** |  | **Ν** | **Ε** | **Ο** | **Τ** |

Άρα το κλειδί είναι **: ΗΙΟΠΡΤ** και το μήνυμά είναι: **ΥΑΑΘΝΣΘΥΤΝΟΗΤΔΕΜΟΣΡ ΝΕΟΤ**

**ΑΠΟΚΩΔΙΚΟΠΟΙΗΣΗ**

Γραφω το κλειδι αρχικα και στη συνέχεια γράφω το μηνυμα ξεκινώντας από την πρώτη στήλη και πηγαίνω προς τα κάτω

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Η** | **Ι** | **Ο** | **Π** | **Ρ** | **Τ** |
| **Υ** | **Ν** | **Τ** | **Τ** | **Ο** | **Ν** |
| **Α** | **Σ** | **Ν** | **Δ** | **Σ** | **Ε** |
| **Α** | **Θ** | **Ο** | **Ε** | **Π** | **Ο** |
| **Θ** | **Υ** | **Η** | **Μ** |  | **Τ** |

Θα πρέπει να ανακαλύψω το κλειδί και να τοποθετήσω τις στήλες με τη σωστή σειρά. Και βρηκα το μηνυμα!!

= = = = = = = = = = = = =

Γράψτε εδώ το κωδικοποιημένο κλειδί σας :

Γράψτε εδώ το κωδικοποιημένο σας μήνυμα :

**Η απαντηση:**

**Κλειδί: ---------------------------------------------**

**Μήνυμα: --------------------------------------------------------------------------------------------**