ΜΕΤΡΩ ΥΠΟΛΟΓΙΖΩ ΣΥΜΠΕΡΑΙΝΩ

ΠΡΟΒΛΗΜΑ 1^{ο}

Σε μια αρχαιολογική ανασκαφή σε προάστιο της Ρώμης βρέθηκε ένα νόμισμα που στην μια όψη του φέρει την κεφαλή ενός άνδρα και γράφει «Ιούλιος Καίσαρ 42 π.Χ.». Να ερευνήσετε αν το νόμισμα είναι γνήσιο ή κίβδηλο.

ΔΙΕΡΕΥΝΗΣΗ:

~~Ο Καίσαρας~~

Στα χρόνια του Καίσαρα, δεν μετρούσανε χρονολογίες από την γέννηση του Χριστού καθώς ~~οι ρωμαίοι έζησαν~~
Ο Καίσαρας έζησε και πέθανε το 44 π.Χ.

Την εποχή που αναφέρει το νόμισμα, δεν υπήρχε η δυνατότητα υπολογισμού και πρόβλεψης για τη γέννηση του Χριστού.

ΣΥΜΠΕΡΑΣΜΑΤΑ: είναι κίβδηλο

ΕΡΓΑΣΤΗΡΙΑΚΕΣ ΑΣΚΗΣΕΙΣ

ΣΥΝΤΑΞΗ ΚΑΙ ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ ΜΗΝΥΜΑΤΟΣ

Συντάξτε ένα μήνυμα ,5-10 γραμμών, με κεφαλαία ελληνικά γράμματα και στη συνέχεια κωδικοποιήστε το με έναν κώδικα υποκατάστασης, δημιουργώντας έτσι ένα κρυπτόγραμμα τύπου "Καίσαρα".
Στην συνέχεια να το στείλετε στην ομάδα που φαίνεται στον παρακάτω πίνακα για αποκρυπτογράφηση.

Μήνυμα:

ΚΠ ΟΧΧΥΞΚΠ ΟΜΣΟΚΕΜ ΗΖΚΜ ΙΜΥΕΝΟΖΠΟΚ ΟΚΗΝΚ ΥΠΜΟΠ
ΦΣΝΠΚΕΘΧΣΝΟΖΟ ΖΚΕ ΡΥΚΕ ΟΩΠ ΣΘΡΟΝ ΗΖΣΝ ΕΙΟΘΛΣ
ΕΘΠΜ ΟΙΚ ΖΚΜ ΕΞΠΟΚ ΟΚΗΝΚ ΔΗ ΙΜΥΕΝΟΖΟ ΥΠΜΟΠ
ΟΗΑΝΟΖΚΠ ΟΩΠ ΟΥΠΟΠΜΣΖΚΠ ΟΞΞΣ ΚΓΠ ΙΟΜΣΟΓΚΕ
ΙΟΘΚΜΖΥΗ ΗΥ ΦΕΜΟΝΣ ΟΩΠ ΧΝΑΗΣ ΥΠΜΟΠ ΟΜΑΖΥΘΚΗ
ΟΙΚ ΖΚΜ ΟΜΡΘΑΙΚ ΟΩΠ ΟΟΖΑΖΥΘΚΠ ΟΙΚ ΖΚ ΡΥΚ
ΙΚΕ ΖΚΕΗ ΓΟΘΠΗΥ ΖΟ ΕΙΥΘΔΕΗΠΟΟ ΙΘΚΗΚΜΖΟ
ΖΚΕΗ ΟΩΠ ΖΣΜ ΟΡΟΜΟΙΠΟ ΖΚΕΗ

Ομάδα σύνταξης	Ομάδα αποκρυπτογράφησης
1	2
2	3
(3)	4
4	1

ΕΡΓΑΣΤΗΡΙΑΚΕΣ ΑΣΚΗΣΕΙΣ

ΟΙ ΑΓΓΕΛΟΙ ΑΝΗΚΟΥΝ ΣΤΟΝ ΠΝΕΥΜΑΤΙΚΟ ΚΟΣΜΟ ΕΙΝΑΙ ΔΗΜΙΟΥΡΓΗΜΑΤΑ ΤΟΥ ΘΕΟΥ ΚΑΙ ΗΡΘΑΝ ΣΤΗΝ ΥΠΑΡΞΗ ΠΡΙΝ ΑΠΟ ΤΟΝ ΥΛΙΚΟ ΚΟΣΜΟ ΩΣ ΠΝΕΥΜΑΤΑ ΕΙΝΑΙ ΑΣΩΜΑΤΟΙ ΚΑΙ ΑΚΙΝΗΤΟΙ ΑΛΛΗ ΟΧΙ ΠΑΝΤΑΧΟΥ ΠΑΡΟΝΤΕΣ ΣΕ ΔΥΝΑΜΗ ΚΑΙ ΓΝΩΣΗ ΕΙΝΑΙ ΑΝΩΤΕΡΟΣ ΑΠΟ ΤΟΝ ΑΝΘΡΩΠΟ ΚΑΙ ΚΑΤΩΤΕΡΟΙ ΑΠΟ ΤΟ ΘΕΟ ΠΟΥ ΤΟΥΣ ΧΑΡΙΣΕ ΥΠΕΡΦΥΣΙΚΑ ΠΡΟΣΟΝΤΑ ΤΟΥΣ ΚΑΙ ΤΗΝ ΑΘΑΝΑΣΙΑ ΤΟΥΣ

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

ΣΥΝΤΑΞΗ ΚΑΙ ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ ΜΗΝΥΜΑΤΟΣ

Συντάξτε ένα μήνυμα ,5-10 γραμμών, με κεφαλαία ελληνικά γράμματα και στη συνέχεια κωδικοποιήστε το με έναν κώδικα υποκατάστασης, δημιουργώντας έτσι ένα κρυπτόγραμμα τύπου "Καίσαρα".
Στην συνέχεια να το στείλετε στην ομάδα που φαίνεται στον παρακάτω πίνακα για αποκρυπτογράφηση.

Μήνυμα:

ΟΒΚ ΥΔΗΚ ΨΚΒ ΜΖΚΖ ΨΚΒΗΔ ΩΤΚΖ Δ ΘΚΖΙΒΠΤΩΣ ΘΔΟ
ΘΝΗΜ ΤΔΖ ΣΗΨΗΔΟΚΖΤΝ ΨΚΒ ΘΗΞΚΖΗ ΣΗ ΟΒΚ ΑΚΗΨΚ ΟΗΛΟΔ
ΣΨΒΔΟΗΟΒΙ ΖΚ ΙΜΕΚΖΜ ΟΚΓΒ ΕΜ ΤΝΖ ΟΟΤΝ ΤΔ
ΜΙΨΜΥΚΕΔΟ ΤΔΟ ΡΗΟΣΔΦΚΗΔΟ

Ομάδα σύνταξης	Ομάδα αποκρυπτογράφησης
1	2
2	3
3	④
④	1

ΜΕΤΡΩ-ΥΠΟΛΟΓΙΖΩ -ΣΥΜΠΕΡΑΙΝΩ

ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Η κρυπτογραφία δημόσιου κλειδιού είναι εφικτή κάνοντας χρήση συναρτήσεων που ενώ είναι εύκολο να υπολογιστούν οι τιμές τους (κρυπτογράφηση), είναι πολύ δύσκολο να αντιστραφούν (αποκρυπτογράφηση), εκτός κι αν κάποιος διαθέτει μια επιπλέον πληροφορία που θα του επιτρέψει να αντιστρέψει την συνάρτηση γρήγορα.

Στην εργασία που ακολουθεί κάντε χρήση της συνάρτησης φ(χ)==χ3 για να κωδικοποιήσετε ένα σύντομο μήνυμα και δώστε το για αποκωδικοποίηση σε μια άλλη ομάδα εργασίας.. Για κλειδί χρησιμοποιήστε τις αντιστοιχίες του παρακάτω πίνακα

Α	01
Β	02
Γ	03
Δ	04
Ε	05
Ζ	06
Η	07
Θ	08
Ι	09
Κ	10
Λ	11
Μ	12
Ν	13
Ξ	14
Ο	15
Π	16
Ρ	17
Σ	18
Τ	19
Υ	20
Φ	21
Χ	22
Ψ	23
Ω	24

3375'4696'01'1728'08'3375'10648'01'729'1000'3375'5832'125'729'2
197'01'729'3375'1728'6'1'64'01'4'913'01'5832'6859'3375'4696'3375'
1331'3375'01'2197'64'49'13'13824'2197'1000'1'729'27'8000'2197'01'
729'1000'13824'2197

ΟΠΑΜΒΟΧΑΙΚΟΣΕΙΝΑΙΟΜΑΔΑΡΑΣΤΟΠΟΛΟΑΝΔΡΩΝ
ΚΑΙΓΥΝΑΙΚΩΝ

Ο ΠΑΜΒΟΧΑΙΚΟΣ ΕΙΝΑΙ ΟΜΑΔΑΡΑ ΣΤΟ ΠΟΛΟ
ΑΝΔΡΩΝ ΚΑΙ ΓΥΝΑΙΚΩΝ

ΜΕΤΡΩ-ΥΠΟΛΟΓΙΖΩ -ΣΥΜΠΕΡΑΙΝΩ

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.

Λύνοντας το παρακάτω πρόβλημα θα γίνει φανερό ότι η ανταλλαγή κλειδιών, μπορεί να γίνει εξ αποστάσεως χωρίς τα δυο άτομα να συναντηθούν.

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;

Λύση

Η Μπομπ λαμβάνει το κουτί με την κλειδαριά της Αλίκης και προσθέτει ένα ακόμα λουκέτο, δικό του. Το στέλνει πίσω στην Αλίκη η οποία βγάζει το δικό της λουκέτο και το στέλνει πίσω με την κλειδαριά του Μπομπ πλέον, ο οποίος το ανοίγει, αφού έχει το κλειδί της ίδιας του κλειδαριάς.

Συμπεράσματα: