**Φύλλο/α Εργασίας Εργαστηρίου/ων**

**Φύλλο εργασίας 2: Κρυπτογράφηση – ο κώδικας του Καίσαρα (συνέχεια)**

Όπως είδαμε, 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. Έτσι, αν το κλειδί είναι 5 το γράμμα Α αντικαθίσταται από το Ζ το Β από το Η και ούτω καθεξής.

**Ερώτηση:** Ποιος είναι ο μέγιστος αριθμός κλειδιών που μπορεί κάποιος να χρησιμοποιήσει για να κρυπτογραφήσει μηνύματα;

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

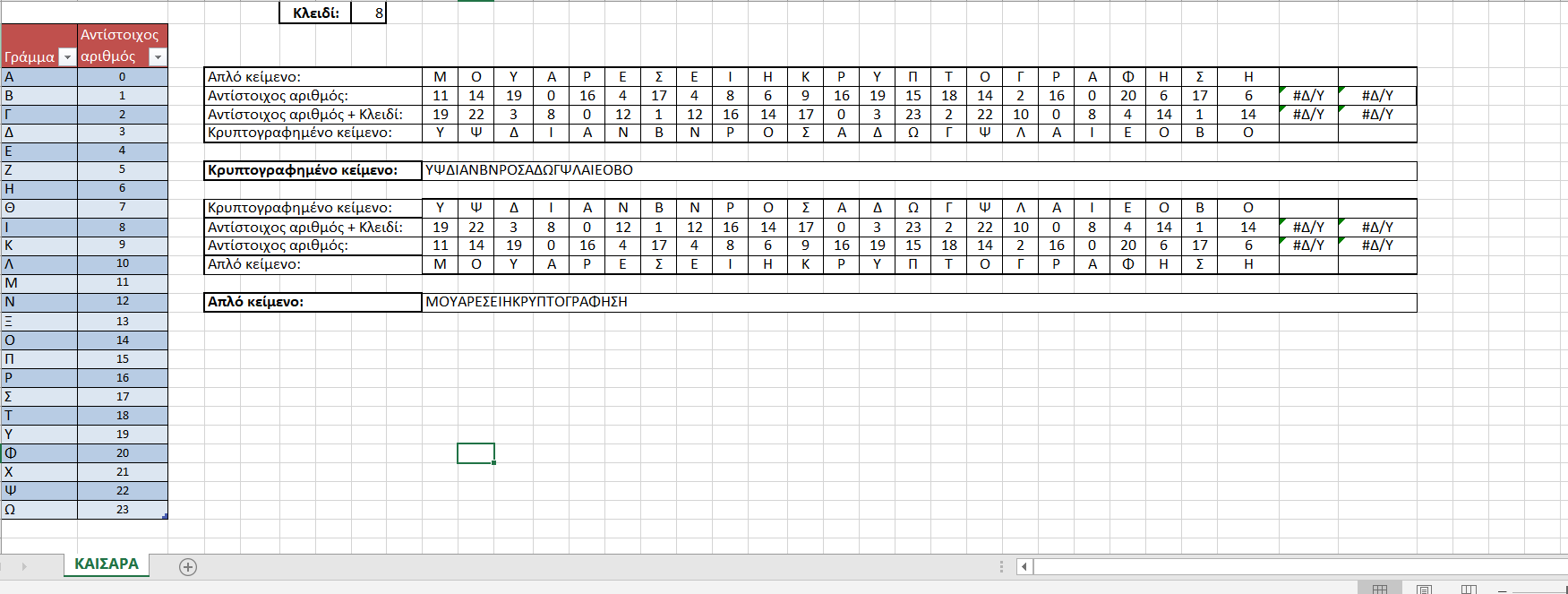
…………………………………………………………………………………………………………………………………………………………………..

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

Αυτό το πλήθος λέγεται και χώρος κλειδιού, αφού αποτελεί το σύνολο των στοιχείων που μπορεί κάποιος να χρησιμοποιήσει για τη μέθοδο κρυπτογράφησης που αξιοποιεί. Επομένως, αν κάποιος/α γνωρίζει ότι η μέθοδος είναι ο κώδικας του Καίσαρα, δεν έχει παρά να δοκιμάσει όλα αυτά τα κλειδιά μέχρι να πάρει ένα μήνυμα που βγάζει νόημα.

**1η Δραστηριότητα**

Προσπαθήστε να δημιουργήσετε ένα λογιστικό φύλλο που θα κάνει γρήγορα και εύκολα τις πράξεις που απαιτούνται για την κρυπτογράφηση και την αποκρυπτογράφηση μηνυμάτων δημιουργημένων από κώδικα του Καίσαρα. Ενδεικτικά, θα μπορούσε να είναι όπως στο σχήμα που ακολουθεί.



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

επόμενη):

Τώρα είστε Κρυπταναλυτές/τριες. Το ΚΚ (Κρυπτογραφημένο κείμενο) έχει δημιουργηθεί από το απλό κείμενο με τη σχέση ΚΚ = 2\*ΑΚ+3 (\*: η πράξη του πολλαπλασιασμού). Αποκρυπτογραφήστε τα παρακάτω ΚΚ.

α) ΒΘΣΔΜΜΞΜΥΠΧΜΣΚΠΘΘΜΔΥΠΞΠ

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

β) ΠΩΜΔΠΠΞΧΜΣΚΠΘΩΘΘΥΔΞ

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

**Ερώτηση:** Πώς θα μπορούσε να τροποποιηθεί το λογιστικό φύλλο για να βρίσκει με τον νέο τρόπο τα σωστά γράμματα; Υλοποιήστε το ή προτείνετε λύσεις εδώ.

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

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

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

**Ερώτηση:** Έχει αλλάξει ο χώρος κλειδιών; Είναι περισσότερα τώρα ή απαρτίζονται από το ίδιο πλήθος;

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

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

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