10 . ΠΑΡΑΡΤΗΜΑ

ΚΡΥΠΤΟΓΡΑΦΙΑ – ΕΝΔΕΙΚΤΙΚΟ ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ 1

Όνομα μαθητή/τριας: _____

Όνομα ομάδας: _____ Ημερομηνία: _____

Η κρυπτογραφία είναι η πρακτική της χρήσης τεχνικών για ασφαλή επικοινωνία στο Διαδίκτυο, όταν προσπαθείτε να ανταλλάξετε ιδιωτικά μηνύματα. Με την κρυπτογραφία μπορείτε να κρυπτογραφήσετε τα μηνύματά σας για να αποφύγετε την πρόσβαση τρίτων σε αυτά. Ο δέκτης θα πρέπει να αποκρυπτογραφήσει το μήνυμά σας για να το διαβάσει.

1. Σκεφτείτε ένα **μήνυμα** που θέλετε να στείλετε σε έναν φίλο σας και γράψτε το:

_____

2. Τι νομίζετε ότι πρέπει να κάνετε για να **κρυπτογραφήσετε** το μήνυμά σας, έτσι ώστε κανείς άλλος να μην το καταλαβαίνει; Γράψτε το **κρυπτογραφημένο** μήνυμά σας:

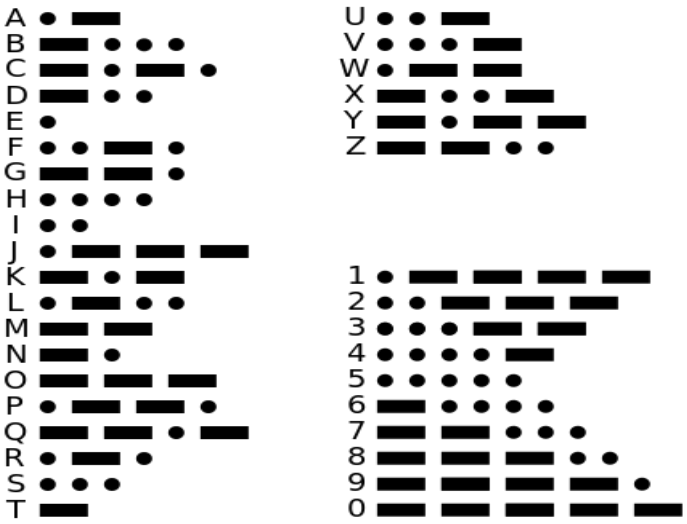
_____

3. Τι πρέπει να γνωρίζει ο φίλος σας για να αποκρυπτογραφήσει το μήνυμά σας;

_____

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού,
Εκπαίδευση και Διά Βίου Μάθηση
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2014-2020

Το 1832, πριν από την εφεύρεση των τηλεφώνων, ο Αμερικανός Samuel Morse εφηύρε μια συσκευή που ονομάζεται τηλεγραφητής **Morse** (Μορς), η οποία χρησιμοποιήθηκε για τη μετάδοση μηνυμάτων σε μεγάλες αποστάσεις. Ένα δίκτυο καλωδίων δημιουργήθηκε σταδιακά σε όλη τη χώρα. Τα καλώδια δε μετέδιδαν ήχο αλλά ηλεκτρικούς παλμούς μεγάλης ή μικρής διάρκειας, σύμφωνα με τον παρακάτω πίνακα.



Μεταξύ των γραμμάτων υπήρχε μια σύντομη παύση και μεταξύ των λέξεων μεγαλύτερη. Τα φωτεινά σήματα θα μπορούσαν επίσης να χρησιμοποιηθούν για τη μετάδοση κώδικα Morse.

1. Με βάση τον παραπάνω πίνακα, μπορείτε να καταλάβετε το ακόλουθο μήνυμα;

-.-. --- -- .--. ..- - . .-.

_____

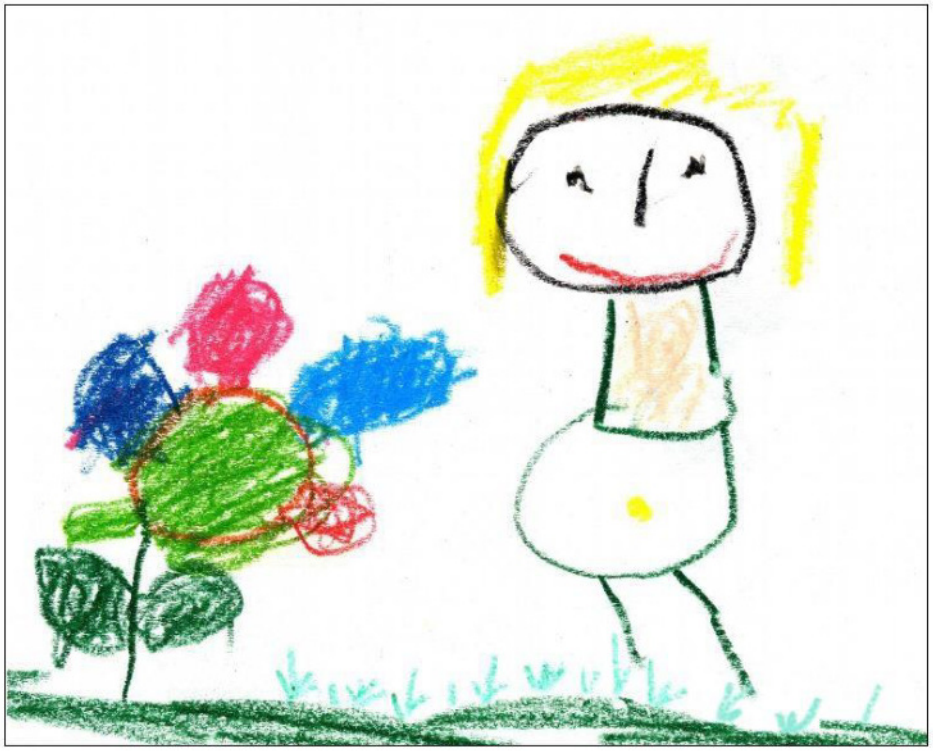
2. Ποιο είναι το σήμα Morse για SOS; (Αυτό είναι το διεθνές σήμα βοήθειας)

_____

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού,
Εκπαίδευση και Διά Βίου Μάθηση
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

3. Σε ομάδες των δύο, προσπαθήστε να στείλετε ένα μήνυμα σε μια άλλη ομάδα συμμαθητών σας, αναβοσβήνοντας έναν φακό για να αντιπροσωπεύσετε τα σήματα Morse.

4. Ένας άλλος τρόπος μετάδοσης μηνυμάτων είναι να τα κρύψετε στα μέσα ενημέρωσης, π.χ. σε μηνύματα. Αυτή η μέθοδος ονομάζεται **στεγανογραφία**. Εάν κοιτάξετε την παρακάτω εικόνα, ενδέχεται να μην παρατηρήσετε ότι υπάρχει ένα κρυμμένο μήνυμα σε αυτό. Αλλά η εικόνα περιέχει ένα μήνυμα στον κώδικα Morse (Μορς). Τα μακριά και κοντά χορτάρια του γρασιδιού είναι οι παύλες και οι τελείες αντίστοιχα, ενώ κάθε τούφα - φούντα είναι ένα γράμμα.



5. Μπορείτε να βρείτε το μυστικό μήνυμα;

6. Πώς θα σχεδιάζατε μια εικόνα για να κρυπτογραφήσετε ένα μήνυμα στον φίλο σας;

Μπράβο. Συγχαρητήρια

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού, Εκπαίδευση και Διά Βίου Μάθηση
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

ΚΡΥΠΤΟΓΡΑΦΙΑ – ΕΝΔΕΙΚΤΙΚΟ ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ 2

Όνομα μαθητή/τριας: _____

Όνομα ομάδας: _____ Ημερομηνία: _____

BRAILLE CODE (ΚΩΔΙΚΑΣ ΜΠΡΑΙΓ)

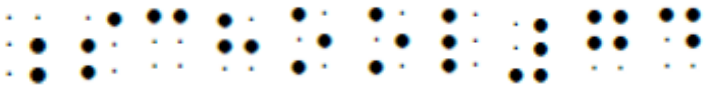
Ο Louis Braille γεννήθηκε στη Γαλλία το 1808 και τυφλώθηκε μετά από ατύχημα σε ηλικία 3 ετών. Σε ηλικία 14 ετών ανέπτυξε μια γραμματοσειρά την οποία οι τυφλοί μπορούν να διαβάσουν. Η γραμματοσειρά αποτελείται από υψωμένα σημεία που κάποιος μπορεί να νιώσει με τα δάχτυλα. Τα σημάδια Braille (μπράιγ) φαίνονται στον παρακάτω πίνακα.

Πίνακας 1: Σήματα Braille(Μπράιγ)

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	0			

Οι λέξεις και οι αριθμοί διακρίνονται χρησιμοποιώντας διαφορετικά σημάδια πριν από αυτά. Με αυτά τα σημάδια ο αναγνώστης ξέρει αν αυτό που ακολουθεί είναι μια λέξη ή ένας αριθμός:

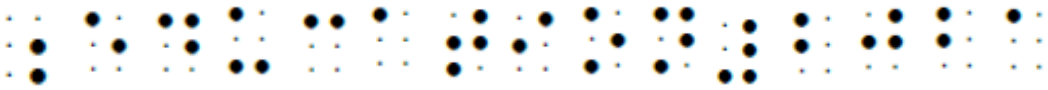
 όταν ακολουθεί **λέξη**, ή  όταν ακολουθεί **αριθμός**

Για παράδειγμα: 

είναι ο κωδικός για το SCHOOL **74**.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού, Εκπαίδευση και Διά Βίου Μάθηση
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2014-2020

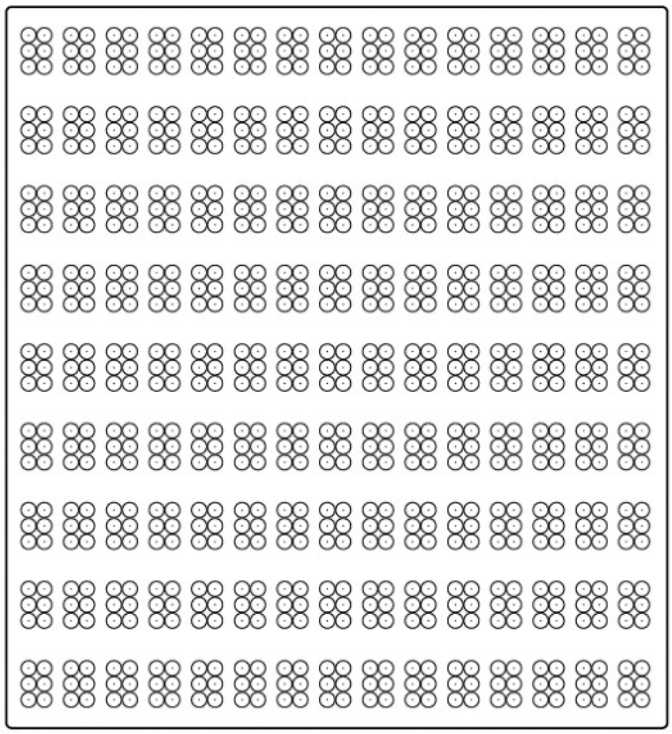
1. Μπορείτε να αποκρυπτογραφήσετε το ακόλουθο μήνυμα;



_____

2. Χρησιμοποιώντας την άκρη του μολυβιού σας, προσπαθήστε να κωδικοποιήσετε το όνομα και την ηλικία σας τρυπώντας την παρακάτω φόρμα.

Χρησιμοποιήστε τον πίνακα των σημείων Braille (Μπράιγ) για να δείτε ποιο σύμβολο αντιστοιχεί σε κάθε γράμμα.



Ζητήστε από τον συμμαθητή σας να διαβάσει αυτό που γράψατε με τα μάτια του κλειστά, αγγίζοντας.

ΣΥΓΧΑΡΗΤΗΡΙΑ!

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού, Εκπαίδευση και Διά Βίου Μάθηση
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

ΚΡΥΠΤΟΓΡΑΦΙΑ – ΕΝΔΕΙΚΤΙΚΟ ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ 3

Όνομα μαθητή/τριας:_____

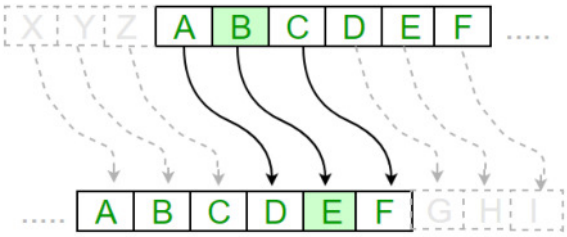
Όνομα ομάδας: _____Ημερομηνία: _____

Ο ΚΩΔΙΚΑΣ ΤΟΥ ΚΑΙΣΑΡΑ (CAESAR cipher)

Το Caesar cipher (ή κωδικός Caesar) είναι ένα από τα πιο διάσημα και εύκολα συστήματα κρυπτογράφησης, που χρησιμοποιήθηκε από τον Ιούλιο Καίσαρα (100-44 π.Χ.) για τα προσωπικά του μηνύματα. Σύμφωνα με αυτήν τη μέθοδο, κάθε γράμμα ενός μηνύματος αντικαθίσταται από ένα άλλο γράμμα σε κάποιο σταθερό αριθμό θέσεων πιο κάτω στο αλφάβητο. Ο αριθμός των θέσεων καθορίζεται από το πλήκτρο, ή Caesar shift, π.χ. αριστερή μετατόπιση 3 ή δεξιά μετατόπιση 4 κ.λπ.

Μέθοδος:

Πρώτον, θα πρέπει να επιλέξετε έναν αριθμό από το 1 έως το 26, τον οποίο θα πρέπει να μοιραστείτε με τον δέκτη. Αυτό ονομάζεται κλειδί και ο δέκτης θα το χρησιμοποιήσει για να αποκρυπτογραφήσει το μήνυμά σας.



Στη συνέχεια γράφετε το αλφάβητο σε δύο γραμμές: πρώτα τα γράμματα από το Α έως το Ζ και έπειτα κάθε γράμμα αντικαθίσταται, ξεκινώντας από το γράμμα στη θέση αμέσως μετά το κλειδί.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού, Εκπαίδευση και Διά Βίου Μάθηση
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2014-2020

Για παράδειγμα, στην περίπτωση που το κλειδί είναι 4, το γράμμα Α θα αντικατασταθεί από το Ε (το γράμμα μετά το 4ο), το γράμμα Β θα αντικατασταθεί από το F και ούτω καθεξής. Τα τέσσερα πρώτα γράμματα (ABCD) ακολουθούν αμέσως μετά το Z.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Αντικατάσταση από:	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

1. Με βάση τα παραπάνω, εάν χρησιμοποιείτε το κλειδί Caesar cipher 4, η λέξη ΑΝΝΑ θα κρυπτογραφηθεί στο ERRE. Μπορείτε να κρυπτογραφήσετε το ακόλουθο μήνυμα χρησιμοποιώντας την παραπάνω μέθοδο (Caesar cipher key 4);

CRYPTOGRAPHY IS FANTASTIC: _____

2. Με βάση τα παραπάνω, μπορείτε να αποκρυπτογραφήσετε το ακόλουθο μήνυμα;

GSQTYXIVW VSGO: _____

Μία παραλλαγή:

Η μέθοδος που παρουσιάζεται μπορεί εύκολα να σπάσει, οπότε βρέθηκε μια παραλλαγή. Ο αποστολέας και ο παραλήπτης θα πρέπει να συμφωνήσουν σε μια λέξη κλειδί, για παράδειγμα τη λέξη **DODEKANISOS** (ένα νησιωτικό συγκρότημα στην Ελλάδα). Η λέξη κλειδί γράφεται στην αρχή του αλφαβήτου (τα ίδια γράμματα δεν επαναλαμβάνονται). Στη συνέχεια, αντικαθιστάτε κάθε ένα από τα άλλα γράμματα με τα υπόλοιπα γράμματα του αλφαβήτου, ξεκινώντας από το τελευταίο γράμμα της λέξης κλειδιού. Δείτε το παρακάτω:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Αντικατάσταση από	**D**	**O**	**E**	**K**	**A**	**N**	**I**	**S**	T	U	V	W	X	Y	Z	B	C	F	G	H	J	L	M	P	Q	R

Αυτός ο πίνακας θα χρησιμοποιηθεί για κωδικοποίηση και αποκωδικοποίηση.

3. Με βάση την παραπάνω παραλλαγή, εάν χρησιμοποιείτε το κλειδί κρυπτογράφησης Caesar cipher **DODEKANISOS**, μπορείτε τώρα να κρυπτογραφήσετε το ακόλουθο μήνυμα;

CRYPTOGRAPHY IS FANTASTIC: _____

4. Με βάση τα παραπάνω, μπορείτε τώρα να αποκρυπτογραφήσετε το ακόλουθο μήνυμα;

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού, Εκπαίδευση και Διά Βίου Μάθηση
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

GSQTYXIVW VSGO: _____

5. Μπορείτε να δείτε τη διαφορά;

ΔΡΑΣΤΗΡΙΟΤΗΤΑ:

Σε ομάδες των δύο, συμφωνήστε σε μια λέξη - κλειδί και δημιουργήστε τον αντίστοιχο πίνακα παρακάτω:

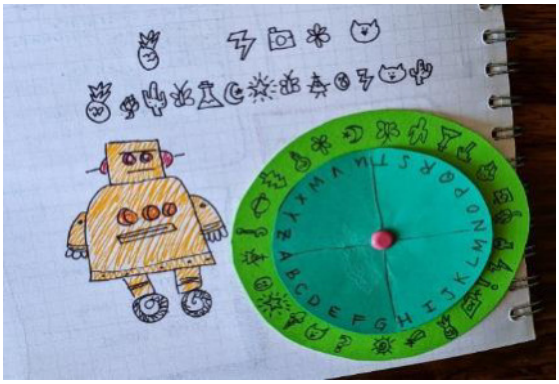
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Αντικατάσταση από																										

Στείλτε ένα κρυπτογραφημένο μήνυμα ο ένας στον άλλο. Αποκρυπτογραφήσατε σωστά το μήνυμα που λάβατε;

Τώρα μπορείτε να κρυπτογραφήσετε και να αποκρυπτογραφήσετε μηνύματα χρησιμοποιώντας τη μέθοδο Caesar cipher (Κώδικας του Καίσαρα)!

Άσκηση για το σπίτι: Γιατί να μην προσπαθήσετε να φτιάξετε τον δικό σας δίσκο κρυπτογράφησης;

Συγχαρητήρια



Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού, Εκπαίδευση και Διά Βίου Μάθηση
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη