

## ΕΡΓΑΣΤΗΡΙΑ ΔΕΞΙΟΤΗΤΩΝ

*Πρόγραμμα Καλλιέργειας Δεξιοτήτων  
Πράξη: «Επιμόρφωση των εκπαιδευτικών στις δεξιότητες  
μέσω εργαστηρίων» (MIS 5092064)*



ΣΤΟ ΠΛΑΙΣΙΟ ΤΟΥ ΕΠΙΧΕΙΡΗΣΙΑΚΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ «ΑΝΑΠΤΥΞΗ ΑΝΘΡΩΠΙΝΟΥ ΔΥΝΑΜΙΚΟΥ  
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ 2014-2020» που συγχρηματοδοτείται από την Ελλάδα και  
την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο)



Επιχειρησιακό Πρόγραμμα  
Ανάπτυξη Ανθρώπινου Δυναμικού,  
Εκπαίδευση και Διά Βίου Μάθηση  
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



## ΕΡΓΑΣΤΗΡΙΑ ΔΕΞΙΟΤΗΤΩΝ

ΘΕΜΑΤΙΚΗ ΕΝΟΤΗΤΑ: ΔΗΜΙΟΥΡΓΩ ΚΑΙ ΚΑΙΝΟΤΟΜΩ –  
ΔΗΜΙΟΥΡΓΙΚΗ ΣΚΕΨΗ & ΠΡΩΤΟΒΟΥΛΙΑ  
1. STEM/STEAM

Το παιχνίδι των κρυφών μηνυμάτων



Νικόλαος Νταούλας



## Φιλοσοφία –Σκοπιμότητα προγράμματος

Είναι πλέον ευρέως αποδεκτό πως οι δεξιότητες ζωής αποτελούν ένα πλαίσιο αποτελεσμάτων που πρέπει να στοχεύουν όλα τα προγράμματα που αναπτύσσονται για τους νέους (Duerden, Witt, Fernandez, Bryant, & Theriault, 2012). Ο τρόπος καλλιέργειας των δεξιοτήτων που πρέπει να αποκτήσει ο αυριανός ενεργός πολίτης, η αποσαφήνιση και η στόχευση ξεχωριστών δεξιοτήτων αλλά και η αξιολόγησή τους αποτελεί μια πρόκληση για τον εκπαιδευτικό και ακόμη και στις μέρες μας πεδίο έρευνας.

Το πρόγραμμα που ακολουθεί στοχεύει σε μια σειρά από δεξιότητες περισσότερο ή λιγότερο σε διαφορετικούς τομείς. Μια σειρά δραστηριοτήτων αναπτύσσεται στα πλαίσια ενός παιχνιδιού όπου οι μαθητές έρχονται αντιμέτωποι με μαθηματικά και οδηγούνται σε υπολογιστική σκέψη, έρχονται σε επαφή και προβληματίζονται για θέματα ασφάλειας και ιδιωτικότητας στον σημερινό ψηφιακό κόσμο. Γενικότερα, ένα παιγνιδοποιημένο πλαίσιο όπως παρουσιάζεται είναι δυνατό να βοηθήσει σημαντικά στην ενεργοποίηση των μαθητών και των μαθητριών και μπορεί να συμβάλει αποφασιστικά στην μαθησιακή διαδικασία. Οι μαθήτριες και οι μαθητές εργάζονται ομαδικά γύρω από έναν πολύ συγκεκριμένο στόχο, να κερδίσουν στο παιχνίδι που αναμένεται να τις/τους οδηγήσει σε υψηλή προσήλωση και παραγωγικότητα. Η παιγνιδοποίηση είναι η διαδικασία δημιουργίας δραστηριοτήτων μάθησης που μοιάζουν με παιχνίδια και επικεντρώνονται στο κρίσιμο σημείο μεταξύ των στοιχείων που αποτελούν το παιχνίδι και την ολιστική εμπειρία της παικτικότητας (gamefulness) (Werbach, 2014). Έτσι, οι δραστηριότητες αναπτύσσονται με πολύ συγκεκριμένους μαθησιακούς στόχους αλλά κρατάνε ζωντανή την αίσθηση του παιχνιδιού και της ψυχαγωγίας.

Η κρυπτογράφηση και η στεγανογραφία, παρότι έννοιες που δεν χρησιμοποιούνται ευρέως στην καθημερινότητα, περιέχουν τεχνικές και μεθόδους που κεντρίζουν το ενδιαφέρον των παιδιών. Το πρόγραμμα των επτά εργαστηρίων που περιγράφονται μέσα από τις δραστηριότητες και την έρευνα που καλούνται να κάνουν οι μαθητές και οι μαθήτριες εμπεριέχει βιωματική και ρεαλιστική εφαρμογή μαθηματικών, καλλιεργούν τις ψηφιακές δεξιότητες όχι ως στείρα αναπαραγωγή οδηγιών αλλά ως ένα εργαλείο επίλυσης προβλημάτων. Η ταχύτητα επίλυσης του κάθε προβλήματος και τα μέσα που μπορούν να αξιοποιηθούν είναι τα εφόδια που θα οδηγήσουν στον άμεσο στόχο της νίκης στο παιχνίδι αλλά θα επιφέρουν μια σειρά από μαθησιακούς στόχους και καλλιέργεια ήπιων δεξιοτήτων κρίσιμων για την ανάπτυξη των νέων. Σημαντικός παράγοντας στην επιτυχία του προγράμματος είναι η συνεργασία των μαθητών, οι διακριτοί ρόλοι και η άσκηση κοινωνικών δεξιοτήτων. Η συνεργατική μάθηση απαιτεί ορθή χρήση διαπροσωπικών δεξιοτήτων και ομαδικότητα. Έρευνες έχουν δείξει πως βάζοντας τους μαθητές και τις μαθήτριες να συνεργαστούν πετυχαίνουν καλύτερα αποτελέσματα, συγκρατούν



μεγαλύτερο μέρος της ύλης, και αισθάνονται θετικά τόσο μεταξύ τους όσο και με το αντικείμενο με το οποίο έρχονται αντιμέτωποι σε σύγκριση με την ατομική εργασία (Johnson & Johnson, 2008). Δίνεται χρόνος στους/στις μαθητές/τριες να προσαρμοστούν στις ανάγκες και τη δυναμική της ομάδας τους, να συζητήσουν, να εκφραστούν και να προτείνουν τις λύσεις που θα υιοθετήσει η ομάδα.

### **Πληροφορίες υλοποίησης: προαπαιτούμενες γνώσεις, προετοιμασία υλικού**

Θεωρούμε πως οι μαθητές/τριες έχουν μια υποτυπώδη εξοικείωση με τον προγραμματισμό και βασικές ψηφιακές δεξιότητες (προγραμματισμό σε μικρόκοσμους, εφαρμογές σχεδίασης/ζωγραφικής, χρήση υπολογιστή κτλ.). Χρειάζονται ηλεκτρονικοί υπολογιστές, εφαρμογές γραφείου και σύνδεση στο διαδίκτυο. Προτείνεται οι μαθητές και οι μαθήτριες να επιλέγουν εφαρμογές διαδικτύου που δίνουν τη δυνατότητα και απομακρυσμένης συνεργασίας ώστε να μπορούν να εργαστούν κι εκτός εργαστηρίου αν επιθυμούν. Για την υλοποίηση των δύο πρώτων εργαστηρίων δεν απαιτούνται ηλεκτρονικές συσκευές αλλά προτείνεται να υπάρχει η δυνατότητα πρόσβασης.



Περιγραφή επτά Εργαστηρίων: Στοχοθεσία των εργαστηρίων, προτεινόμενες δράσεις και υλικό αφόρμησης, επέκτασης, γενίκευσης. Κάθε εργαστήριο θα αναπτύσσεται σε ένα φύλλο Α4 με βάση τη ρουμπρίκα του Παραρτήματος (1 σελίδα ανά εργαστήριο = 7 σελίδες)

ΕΡΓΑΣΤΗΡΙΟ ΚΑΛΛΙΕΡΓΕΙΑΣ ΔΕΞΙΟΤΗΤΩΝ			
ΣΧΟΛΕΙΟ		ΤΜΗΜΑ.....	ΣΧΟΛ. ΕΤΟΣ:
Θεματική	Δημιουργώ και Καινοτομώ– Δημιουργική Σκέψη και Πρωτοβουλία	Υποθεματική	STEM/STEAM
ΒΑΘΜΙΔΑ/ΤΑΞΕΙΣ (που προτείνονται)		Α' - Β' Γυμνασίου	
Τίτλος		Το παιχνίδι των κρυφών μηνυμάτων	
Δεξιότητες στόχευσης του εργαστηρίου		<p><b>1. Δεξιότητες Μάθησης</b>                      Δημιουργικότητα                      Συνεργασία                      Επικοινωνία                      Κριτική σκέψη</p> <p><b>Δεξιότητες Ζωής</b>                      Κοινωνικές Δεξιότητες                      Υπευθυνότητα                      Διαχείριση άγχους                      Πρωτοβουλία                      Παραγωγικότητα</p> <p><b>MIT: Δεξιότητες της τεχνολογίας και της επιστήμης</b>                      Ψηφιακός γραμματισμός                      Δεξιότητες δημιουργίας και διαμοιρασμού ψηφιακών δημιουργημάτων                      Δεξιότητες ψηφιακής τεχνολογίας, επικοινωνίας και συνεργασίας,                      Δεξιότητες διεπιστημονικής και διαθεματικής χρήσης των νέων τεχνολογιών</p> <p><b>Δεξιότητες του νου</b>                      Στρατηγική σκέψη                      Επίλυση προβλημάτων</p>	
Σύνδεση με τη Βασική Θεματική		STEM/STEAM	



Προσδοκώμενα μαθησιακά αποτελέσματα	Εργαστήριο/τίτλος	Δραστηριότητες – (ενδεικτικές)
<p>Οι μαθητές και οι μαθήτριες θα μπορούν να</p> <ul style="list-style-type: none"> <li>• αναγνωρίζουν τη σημασία της ασφάλειας και της ιδιωτικότητας στην εποχή μας</li> <li>• αναπτύσσουν μεταγνωστικές ικανότητες (συζητούν, προβληματίζονται και αναστοχάζονται μέσα από παραδείγματα της καθημερινότητας και θα οδηγηθούν στο σχηματισμό εμπειρίας/γνώσης)</li> <li>• εναρμονίζονται με κανόνες απαραίτητους για την πραγματοποίηση ενός παιχνιδιού.</li> <li>• αποκτούν ρόλους σε μια νεοσύστατη ομάδα και να χτίζουν την αρχή μιας συνεργασίας</li> </ul>	<p><b>1ο εργαστήριο:</b> <b>Η ομάδα μου μαθαίνει τους κανόνες του παιχνιδιού</b></p>	<p><b>ΦΑΣΗ Α:</b> Ο/Η Εκπαιδευτικός καλωσορίζει τους μαθητές και τις μαθήτριες και ξεκινά μια συζήτηση για την ασφάλεια των δεδομένων και των επικοινωνιών και πως φαντάζονται οι μαθητές πως αυτό συμβαίνει στις μέρες μας. Η συζήτηση δεν χρειάζεται να είναι σε βάθος και με τεχνικές λεπτομέρειες και προτείνεται να επεκταθεί στη σημασία της ασφάλειας και της ιδιωτικότητας στη καθημερινή μας ζωή και στην αλληλεπίδραση μας με υπηρεσίες που πηγάζουν από τους υπολογιστές και το διαδίκτυο.</p> <p><b>ΦΑΣΗ Β:</b> Ο/Η εκπαιδευτικός ενημερώνει τους μαθητές και τις μαθήτριες για τους κανόνες του παιχνιδιού που θα παίξουν στα εργαστήρια που ακολουθούν. Χωρίζονται σε ομάδες (3-6 ατόμων). Η κάθε ομάδα εκλέγει εκπρόσωπο που θα είναι μέλος και της επιτροπής των κριτών για θέματα κανόνων που μπορεί να ανακύψουν στη διάρκεια του παιχνιδιού. Στην περίπτωση άρτιου πλήθους ομάδων στην επιτροπή συμμετέχει και ο/η εκπαιδευτικός. Οι ομάδες θα έρθουν αντιμέτωπες με μια σειρά προκλήσεων όπως περιγράφονται στις δραστηριότητες των φύλλων εργασίας. Η πρώτη ομάδα που απαντά πρώτη σε κάθε ερώτημα των δραστηριοτήτων κερδίζει 10 πόντους, η δεύτερη 8 πόντους η τρίτη 6 πόντους μέχρι το 0 που παίρνουν οι ομάδες που απαντούν τελευταίες ή καθόλου σε κάποιο ερώτημα. Προτείνεται οι απαντήσεις να δίνονται σε κάποια διαδικτυακή πλατφόρμα (π.χ. η- τάξη στα πλαίσια άσκησης ή εργασίας) ώστε να καταγράφεται ο χρόνος της κάθε ομάδας. Για κάθε 20 βαθμούς που συγκεντρώνει η κάθε ομάδα κερδίζει ένα μετάλλιο (αρχάριοι-&gt; κρυπτολόγοι-&gt; επαγγελματίες-&gt; ειδικοί-&gt; γκουρού).</p>





Προσδοκώμενα μαθησιακά αποτελέσματα	Εργαστήριο/τίλος	Δραστηριότητες – (ενδεικτικές)
<p>Οι μαθητές και οι μαθήτριες θα</p> <ul style="list-style-type: none"> <li>• κατανοήσουν τον ρόλο της κρυπτογράφησης ιστορικά</li> <li>• αντιληφθούν την εξέλιξη και τη συμβολή των υπολογιστών στην επίλυση προβλημάτων</li> <li>• κατανοήσουν τις έννοιες κρυπτογράφησης/αποκρυπτογράφησης</li> <li>• κάνουν απλές κρυπτογραφήσεις και αποκρυπτογραφήσεις</li> <li>• αναγνωρίζουν αποτελεσματικές τεχνικές κρυπτογράφησης</li> <li>• κατανοήσουν την έννοια συχνότητα και τη σημασία της στην επίλυση προβλημάτων</li> </ul>	<p><b>2ο εργαστήριο:</b> <b>Κώδικας</b> <b>Καίσαρα – το παιχνίδι ξεκινά</b></p>	<p><b>ΦΑΣΗ Α:</b> Ο/Η εκπαιδευτικός μπορεί να προχωρήσει σε μια σύντομη περιγραφή του κώδικα του Καίσαρα ή να αξιοποιήσει κάποιο πολυμέσο αφόρμησης για να ενεργοποιήσει το ενδιαφέρον των μαθητών και των μαθητριών. Ποικιλία υλικού μπορεί να αντλήσει από το διαδίκτυο όπως για παράδειγμα βίντεο από αποθετήρια κοινωνικής δικτύωσης (όπως το Youtube). Δεν προτείνεται κάποιο συγκεκριμένο καθότι μπορεί να προσαρμόζεται στην αισθητική και τη δυναμική τόσο του/της εκπαιδευτικού όσο και των μαθητών και μαθητριών. Το φύλλο εργασίας θεωρείται αρκετό για την κατανόηση και την αντιμετώπιση των δραστηριοτήτων αλλά κάποιοι μαθητές και μαθήτριες προτιμούν την εξήγηση των όρων. Αυτή η φάση μπορεί να συνδυαστεί με το πρώτο μέρος του φύλλου εργασίας που περιέχει το θεωρητικό μέρος.</p> <p><b>ΦΑΣΗ Β:</b> Οι μαθητές και οι μαθήτριες περνούν γρήγορα στη δράση με την εκκίνηση του παιχνιδιού που έρχεται με το μοίρασμα του πρώτου φύλλου εργασίας και κατόπιν των απαντήσεων του θεωρητικού μέρους που θα οδηγήσει σε σύντομη συζήτηση στην ολομέλεια. Κάθε απάντηση στις δραστηριότητες ανεβαίνει σε ηλεκτρονική πλατφόρμα όπως προαναφέρθηκε και η επιτροπή των κριτών διατηρεί και αναπαριστά με τρόπο της επιλογής της τη βαθμολογία και τα μετάλλια των ομάδων.</p>



Προσδοκώμενα μαθησιακά αποτελέσματα	Εργαστήριο/τίτλος	Δραστηριότητες – (ενδεικτικές)
<p>Οι μαθητές και οι μαθήτριες θα</p> <ul style="list-style-type: none"> <li>• κατανοήσουν τη δομή ενός υπολογιστικού φύλλου και την αναφορά σε κελιά</li> <li>• υλοποιήσουν απλές συναρτήσεις και πράξεις με κελιά</li> <li>• αναγνωρίζουν και θα αξιοποιούν λογικές πράξεις</li> <li>• υλοποιήσουν κρυπτογράφηση με αντικατάσταση με τη βοήθεια υπολογιστικών φύλλων</li> <li>• χρησιμοποιήσουν αναζητήσεις και απλές δομές προγραμματισμού (αν...τότε)</li> </ul>	<p><b>3ο εργαστήριο: Δημιουργία υπολογιστικού φύλλου για τον Κώδικα του Καίσαρα</b></p>	<p><b>ΦΑΣΗ Α:</b> Ο/Η εκπαιδευτικός κάνει μια σύνδεση με τα προηγούμενα εργαστήρια και υπενθυμίζει στους μαθητές και τις μαθήτριες τους λόγους που εξυπηρετούν τέτοιες τεχνολογίες στην εποχή μας, έρευνα που θα διενεργήσουν εξάλλου σε επόμενο εργαστήριο θα προσπαθήσουν να δημιουργήσουν τις κατάλληλες συναρτήσεις για να αυτοματοποιήσουν την κωδικοποίηση και την αποκωδικοποίηση μηνυμάτων που έχουν δημιουργηθεί με τον κώδικα του Καίσαρα.</p> <p><b>ΦΑΣΗ Β:</b> Οι μαθητές και οι μαθήτριες αντιμετωπίζουν το δεύτερο φύλλο εργασίας και κατόπιν των απαντήσεων του θεωρητικού μέρους που θα οδηγήσει σε σύντομη συζήτηση στην ολομέλεια συνεχίζουν με τη πρώτη δραστηριότητα. Λόγω των δυσκολιών που πιθανώς θα αντιμετωπίσουν εδώ προτείνεται να μη προσθέτει η αφαιρεί πόντους από το παιχνίδι τους. Οι συναρτήσεις που μπορούν να προταθούν είναι η αναζήτηση σε μορφή που θα επιλέξουν (π.χ. VLOOKUP) για την εύρεση του αντίστοιχου αριθμού για κάθε γράμμα. Μια κυκλική πράξη πρόσθεση, αφαίρεση ή ακέραια διαίρεση θα χρειαστεί για να γίνεται σωστά ο υπολογισμός όταν ο αντίστοιχος αριθμός γίνεται μεγαλύτερος από 23. Έπειτα συνεχίζεται το παιχνίδι με τη δεύτερη δραστηριότητα. Η επιτροπή των κριτών υπενθυμίζει τους κανόνες του παιχνιδιού και προβάλλει την βαθμολογία των ομάδων μέχρι τώρα.</p>





Προσδοκώμενα μαθησιακά αποτελέσματα	Εργαστήριο/τίτλος	Δραστηριότητες – (ενδεικτικές)
<p>Οι μαθητές και οι μαθήτριες θα</p> <ul style="list-style-type: none"> <li>• κατανοήσουν σε μεγαλύτερο βάθος τον ρόλο της κρυπτογράφησης και την εξέλιξη της</li> <li>• αντιληφθούν την εξέλιξη και τη συμβολή των υπολογιστών στην επίλυση προβλημάτων</li> <li>• κατανοήσουν τις έννοιες κρυπτογράφησης/αποκρυπτογράφησης</li> <li>• κάνουν πιο περίπλοκες κρυπτογραφήσεις και αποκρυπτογραφήσεις</li> <li>• αναγνωρίζουν αποτελεσματικές τεχνικές κρυπτογράφησης</li> <li>• αναγνωρίζουν μοτίβα</li> <li>• κατανοούν αποτέλεσμα εντοπισμού τους</li> </ul>	<p><b>4ο εργαστήριο: Ο αλγόριθμος κρυπτογράφησης Vigenère (Βιζενέρ)</b></p>	<p><b>ΦΑΣΗ Α:</b> Πιθανότατα μπορεί να χρειαστεί κάποιος χρόνος εδώ για συνέχιση των δραστηριοτήτων προηγούμενων εργαστηρίων. Το εργαστήριο αυτό είναι λίγο πιο δύσκολο αλλά οι δραστηριότητες προτείνεται να είναι λιγότερες όπως προκύπτει κι από το αντίστοιχο φύλλο εργασίας. Ο/Η εκπαιδευτικός κάνει μια σύνδεση των προηγούμενων εργαστηρίων και παρέχει μια σύντομη περιγραφή του αλγορίθμου προς εξέταση ή χρησιμοποιεί κάποιο βίντεο από το διαδίκτυο. Δεν αναμένεται να έχουν ιδιαίτερες δυσκολίες.</p> <p><b>ΦΑΣΗ Β:</b> οι μαθήτριες και οι μαθητές αντιμετωπίζουν το τρίτο φύλλο εργασίας όπως παρατίθεται παρακάτω.</p>



Προσδοκώμενα μαθησιακά αποτελέσματα	Εργαστήριο/τίτλος	Δραστηριότητες – (ενδεικτικές)
<p>Οι μαθητές και οι μαθήτριες θα</p> <ul style="list-style-type: none"> <li>• κατανοήσουν τον ρόλο της στεγανογραφίας ιστορικά</li> <li>• υλοποιούν απλές στεγανογραφικές μεθόδους</li> <li>• κατανοήσουν τις έννοιες στεγανογραφία/υδατογράφιση</li> </ul>	<p><b>5ο εργαστήριο: Στεγανογραφία/υδατογράφιση</b></p>	<p><b>ΦΑΣΗ Α:</b> Ο/Η εκπαιδευτικός μπορεί να προχωρήσει σε μια σύντομη περιγραφή των τεχνικών στεγανογραφίας και υδατογράφισης και πως βρίσκουν εφαρμογή στις μέρες μας. Κάποια ιστορικά στοιχεία μπορούν να ενεργοποιήσουν το ενδιαφέρον των μαθητών. Το αντίστοιχο τέταρτο φύλλο εργασίας είναι αρκετό για την βασική κατανόηση και αντιμετώπιση τόσο των ερωτημάτων όσο και των δραστηριοτήτων που περιέχει.</p> <p><b>ΦΑΣΗ Β:</b> Οι μαθήτριες και οι μαθητές λαμβάνουν το φύλλο εργασίας, απαντούν και συζητούν στην ολομέλεια τα ερωτήματα. Στη συνέχεια υλοποιούν τις δραστηριότητες που είναι μέρος του παιχνιδιού για να μαζέψουν πόντους και να βαθμολογηθούν με τον τρόπο που αναφέρθηκε εκτενώς.</p>



Προσδοκώμενα μαθησιακά αποτελέσματα	Εργαστήριο/τίτλος	Δραστηριότητες – (ενδεικτικές)
<p>Οι μαθητές και οι μαθήτριες θα</p> <ul style="list-style-type: none"> <li>• αναπτύξουν στρατηγική και μεταγνώση για την ανάπτυξη κρυπτογράφησης</li> <li>• δημιουργούν κρυπτογραφημένα και στεγανογραφημένα μηνύματα</li> </ul>	<p><b>6ο εργαστήριο: Τελικός του παιχνιδιού</b></p>	<p>Οι μαθήτριες και οι μαθητές σε αυτό το εργαστήριο καλούνται να δημιουργήσουν δύο κρυπτογραφημένα μήνυμα κι ένα στεγανογραφημένο. Τα μηνύματά τους μπορούν να τα μοιράσουν ηλεκτρονικά (π.χ. σε έναν κοινόχρηστο τοίχο - padelt) ώστε οι υπόλοιπες ομάδες να μπορέσουν να ανακαλύψουν τα κρυφά μηνύματα. Για το κάθε μήνυμα που βρίσκουν από τις υπόλοιπες ομάδες κερδίζουν 10 πόντους. Για τα κρυπτογραφημένα μηνύματα θα πρέπει να σημειώσουν τον αλγόριθμο που χρησιμοποίησαν. Για την περίπτωση του κώδικα του Καίσαρα δεν χρειάζεται να κοινοποιήσουν το κλειδί τους. Αν χρησιμοποιήσουν τον αλγόριθμο Βιζενέρ θα πρέπει να οι λέξεις κλειδιά να έχουν επιλεχθεί από μια μικρή ομάδα μικρών λέξεων (ΝΑΙ, ΟΧΙ, ΕΔΩ, ΤΩΡΑ, ΜΕΡΑ, ΚΑΤΙ, ΕΞΩ, ΜΕΣΑ). Για τα στεγανογραφημένα μηνύματα δεν κρίνεται απαραίτητο να κοινοποιήσουν τη μέθοδο που χρησιμοποιούν.</p>



Προσδοκώμενα μαθησιακά αποτελέσματα	Εργαστήριο/τίτλος	Δραστηριότητες – (ενδεικτικές)
<p>Οι μαθήτριες και οι μαθητές θα</p> <ul style="list-style-type: none"> <li>• κατανοήσουν τη σημασία της κρυπτογράφησης και της στεγανογραφίας στις σύγχρονες τεχνολογίες</li> <li>• θα αναφέρουν το μαθηματικό υπόβαθρο μια εφαρμογής</li> <li>• θα περιγράψουν τον τρόπο λειτουργίας μια μεθόδου κρυπτογράφησης ή στεγανογραφίας στην εποχή μας</li> </ul>	<p><b>7ο εργαστήριο: Ερευνώ παρουσιάζω</b></p>	<p><b>ΦΑΣΗ Α:</b> Οι μαθητές και οι μαθήτριες δημιουργούν μια σύντομη παρουσίαση/βίντεο/ κινούμενο σχέδιο κατόπιν μιας μικρής έρευνας που θα διενεργήσουν στο διαδίκτυο για τις μεθόδους κρυπτογράφησης και στεγανογραφίας/υδατογράφησης που χρησιμοποιούνται στα ψηφιακά δεδομένα και τις ψηφιακές επικοινωνίες. Θα κληθούν να επιλέξουν μια εφαρμογή/χρήση απαντήσουν κάποια βασικά όπως να περιγράψουν τον τρόπο χρήσης, να προσδιορίσουν τον χώρο κλειδιού, και να αναφέρουν το μαθηματικό υπόβαθρο της συγκεκριμένης εφαρμογής.</p> <p><b>ΦΑΣΗ Β:</b> Η επιτροπή των κριτών θα ανακοινώσει την τελική βαθμολογία του παιχνιδιού και θα βραβεύσει με τα μετάλλια τα μέλη των ομάδων.</p>



### Εκπαιδευτικό Υλικό/ Συνδέσεις/

Τεχνολογία, Πληροφορική, Φυσική, Μαθηματικά, Διαθεματική προσέγγιση

### Φορείς και άλλες συνεργασίες που θα εμπλουτίσουν το πρόγραμμά μας

Ο ENISA δημιουργήθηκε για να ενδυναμώσει τη δυνατότητα της Ευρωπαϊκής Ένωσης, των Κρατών μελών της Ε.Ε. και της επαγγελματικής κοινότητας να αποφεύγει, να διευθύνει και να ανταποκρίνεται σε προβλήματα που αφορούν την ασφάλεια των δικτύων και πληροφοριών και εδρεύει στην Ελλάδα.

Συνεργασία με τον εν λόγω ευρωπαϊκό οργανισμό δύναται να εμπλουτίσει το πρόγραμμα.

### Αξιολόγηση Εργαστηρίου- Συνολική αποτίμηση & αναστοχασμός πάνω στην υλοποίηση - Εκδηλώσεις διάχυσης

Ένα εργαστήριο δραστηριοτήτων αποτελεί επιπρόσθετα της διδακτικής πράξης πλαίσιο δυναμικό, διαφορετικό του παραδοσιακού τρόπου εκπαίδευσης και με σύνθετους στόχους. Τα προβλήματα και οι δυσκολίες που μπορεί να προκύψουν εξαρτώνται από πολλούς και πολυπαραμετρικούς παράγοντες όπως τα κατάλληλα μέσα, η δυναμική του τμήματος, η ευελιξία χρόνου και χώρου. Κρίνεται, λοιπόν, απαραίτητο ο εκπαιδευτικό να ανατροφοδοτεί και να αναπροσαρμόζει συνεχώς κάθε πτυχή του προγράμματος από τους μαθησιακούς στόχους μέχρι τις δραστηριότητες που θα αντιμετωπίσουν οι μαθητές και οι μαθήτριες. Ο παιγνιώδης τρόπος διεξαγωγής και η φύση των εννοιών και των δραστηριοτήτων θεμελιώνουν τις βάσεις για ομαλή διδακτική πράξη με αυξημένη συνεργασία και συμμετοχή όλων των μελών. Οι μαθήτριες και οι μαθητές θα είναι σε θέση να εμβαθύνουν σε βαθμό που θα μπορούν να παρουσιάσουν τα αποτελέσματα των εργασιών τους στο ευρύτερο κοινό. Μπορεί να οργανωθεί ημέρα ασφάλειας που οι μαθητές και οι μαθήτριες ως ειδικοί θα δείξουν και θα συμβουλέψουν όλη τη σχολική κοινότητα σε μια ημερίδα ασφάλειας και ιδιωτικότητας.

### Σημειώσεις:



**Υποδειγματικό Υλικό- Δειγματικά Φύλλα εργασίας - Περιγραφή εργαστηρίων & δράσεων (3-5 φύλλα)**

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

Η πιο απλή και γνωστή τεχνική κρυπτογράφησης ακολουθεί ένα 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. 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.

<b>A</b>	<b>B</b>	<b>Γ</b>	<b>Δ</b>	<b>E</b>	<b>Z</b>	<b>H</b>	<b>Θ</b>	<b>I</b>	<b>K</b>
0	1	2	3	4	5	6	7	8	9
<b>Λ</b>	<b>M</b>	<b>N</b>	<b>Η</b>	<b>O</b>	<b>Π</b>	<b>P</b>	<b>Σ</b>	<b>T</b>	<b>Υ</b>
10	11	12	13	14	15	16	17	18	19
<b>Φ</b>	<b>Χ</b>	<b>Ψ</b>	<b>Ω</b>						
20	21	22	23						

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

<b>A</b>	<b>B</b>	<b>Γ</b>	<b>Δ</b>	<b>E</b>	<b>Z</b>	<b>H</b>	<b>Θ</b>	<b>I</b>	<b>K</b>
4	5	6	7	8	9	10	11	12	13
<b>Λ</b>	<b>M</b>	<b>N</b>	<b>Η</b>	<b>O</b>	<b>Π</b>	<b>P</b>	<b>Σ</b>	<b>T</b>	<b>Υ</b>
14	15	16	17	18	19	20	21	22	23
<b>Φ</b>	<b>Χ</b>	<b>Ψ</b>	<b>Ω</b>						
0	1	2	3						

Με ΑΚ: Απλό Κείμενο και ΚΚ: Κρυπτογραφημένο Κείμενο.

Κρυπτογράφο λέμε αυτόν που κάνει τη διαδικασία κρυπτογράφησης δηλαδή μετατρέπει το Απλό Κείμενο σε Κρυπτογραφημένο Κείμενο. Έτσι στο παράδειγμα μας ο Κρυπτογράφος κάνει την πράξη  $(ΚΚ = ΑΚ + \text{Κλειδί}) \bmod 24$ . Το mod μας κάνει το υπόλοιπο της ακέραιας διαίρεσης μεταξύ 2 ακεραίων.

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

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

Κρυπταναλυτή λέμε αυτόν που κάνει την αντίστροφη διαδικασία δηλαδή μετατρέπει το Κρυπτογραφημένο Κείμενο σε Απλό Κείμενο. Έτσι στο παράδειγμα μας ο Κρυπταναλυτής κάνει την πράξη  $(ΑΚ = ΚΚ - \text{Κλειδί}) \bmod 24$





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 κρυπταναλυτής;

**Απάντηση:**.....

.....

.....

.....

**1<sup>η</sup> Δραστηριότητα (10 πόντους για την 1<sup>η</sup> ομάδα για κάθε απάντηση -2 για κάθε επόμενη):**

Τώρα είστε κρυπταναλυτές. Γνωρίζετε ότι ο Κώδικας είναι αυτός του Καίσαρα και το κλειδί που χρησιμοποιήθηκε είναι το 8. Αποκρυπτογραφήστε τις παρακάτω φράσεις και ανεβάστε τις απαντήσεις στην ηλεκτρονική πλατφόρμα που θα σας υποδείξει ο εκπαιδευτικός.

α) ΙΔΓΨΝΡΦΙΡΥΔΒΓΡΣΨ

.....

β) ΩΙΑΝΓΟΤΝΕΘΦΨΙΥΝΒΘΒ

.....

γ) ΜΘΒΝΓΨΛΑΙΥΥΙΒΓΨΦΦΡΣΨ

.....

δ) ΥΨΔΙΑΝΒΝΡΟΣΑΔΩΓΨΛΑΙΕΟΒΟ

.....



**2<sup>η</sup> Δραστηριότητα (10 πόντους για την 1<sup>η</sup> ομάδα για κάθε απάντηση -2 για κάθε επόμενη):**

Τώρα είστε κρυπτογράφοι. Χρησιμοποιείτε 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 ΠΡΟΙΟΝ ΠΡΟΣΤΕΘΗΚΕ ΣΤΟ ΚΑΛΑΘΙ ΣΑΣ  
.....



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

Όπως είδαμε η πιο απλή και γνωστή τεχνική κρυπτογράφησης ακολουθεί ένα 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 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.

**1<sup>η</sup> 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.

Γράμμα	Αντίστοιχος αριθμός	
A	0	Απλό κείμενο: M O Y A P E Σ E I H K P Y Π Τ Ο Γ Ρ Α Φ Η Σ Η
B	1	Αντίστοιχος αριθμός: 11 14 19 0 16 4 17 4 8 6 9 16 19 15 18 14 2 16 0 20 6 17 6 #Δ/Υ #Δ/Υ
Γ	2	Αντίστοιχος αριθμός + Κλειδί: 19 22 3 8 0 12 1 12 16 14 17 0 3 23 2 22 10 0 8 4 14 1 14 #Δ/Υ #Δ/Υ
Δ	3	Κρυπτογραφημένο κείμενο: Y Ψ Δ Ι Α Ν Β Ν Ρ Ο Σ Α Δ Ω Γ Ψ Λ Α Ι Ε Ο Β Ο
E	4	
Z	5	Κρυπτογραφημένο κείμενο: YΨΔΙΑΝΒΝΡΟΣΑΔΩΓΨΛΑΙΕΟΒΟ
H	6	
Θ	7	Κρυπτογραφημένο κείμενο: Y Ψ Δ Ι Α Ν Β Ν Ρ Ο Σ Α Δ Ω Γ Ψ Λ Α Ι Ε Ο Β Ο
I	8	Αντίστοιχος αριθμός + Κλειδί: 19 22 3 8 0 12 1 12 16 14 17 0 3 23 2 22 10 0 8 4 14 1 14 #Δ/Υ #Δ/Υ
K	9	Αντίστοιχος αριθμός: 11 14 19 0 16 4 17 4 8 6 9 16 19 15 18 14 2 16 0 20 6 17 6 #Δ/Υ #Δ/Υ
Λ	10	Απλό κείμενο: M O Y A P E Σ E I H K P Y Π Τ Ο Γ Ρ Α Φ Η Σ Η
M	11	
N	12	Απλό κείμενο: ΜΟΥΑΡΕΞΕΙΗΚΡΥΠΤΟΓΡΑΦΗΣΗ
Ξ	13	
Ο	14	
Π	15	
Ρ	16	
Σ	17	
Τ	18	
Υ	19	
Φ	20	
Χ	21	
Ψ	22	
Ω	23	



**2<sup>η</sup> Δραστηριότητα (10 πόντους για την 1<sup>η</sup> ομάδα για κάθε απάντηση -2 για κάθε επόμενη):**

Τώρα είστε κρυπταναλυτές. 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) ΠΩΜΔΠΠΞΧΜΣΚΠΘΩΘΥΔΞ

.....

**Ερώτηση:** Πως 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:**.....  
.....  
.....  
.....



**Φύλλο εργασίας 3: Κρυπτογράφηση – Ο αλγόριθμος Vigenère (Βιζενέρ)**

Εδώ τα πράγματα δυσκολεύουν κάπως και το κλειδί που μας δείχνει το γράμμα που θα χρησιμοποιήσω αντί του απλού κειμένου δίνεται από μια λέξη ή μια φράση. Ο κρυπτογράφος έχει μπροστά του τον πίνακα που ακολουθεί και για κάθε γράμμα αντικαθιστά από τη στήλη που του υποδεικνύει η λέξη κλειδί.

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

Έτσι αν η λέξη κλειδί είναι «ΓΡΙΦΟΣ» και το ΑΚ: «ΔΕΝ ΜΟΥ ΑΡΕΣΕΙ» ο κρυπτογράφος για να αντικαταστήσει το Δ θα κοιτάξει στην στήλη του Γ και θα το αντικαταστήσει με το γράμμα που συναντά σε αυτή τη γραμμή άρα με το Ζ. Για το Ε θα κοιτάξει στη στήλη του Ρ και θα βρει το γράμμα Φ κτλ.. Όταν θα εξαντληθούν τα γράμματα της λέξης κλειδί θα συνεχίσει γυρνώντας στην αρχή κι επομένως κοιτώντας πάλι στη στήλη του Γ. Προκύπτει επομένως το ΚΚ: ΖΦΦΘΕΝΓΙΝΞΤΒ



**Ερώτηση:** Θυμηθείτε πως η συχνότητα εμφάνισης των γραμμάτων του ΚΚ μας βοηθούσε να βγάζουμε συμπεράσματα για το ΑΚ. Εδώ μπορεί να μας δώσει αντίστοιχα πληροφορία; Τι αναπαριστά το πρώτο Φ και τι το δεύτερο στο ΚΚ;

**Απάντηση:**.....  
.....  
.....

**Ερώτηση:** Από τι εξαρτάται τώρα ο χώρος κλειδιού;

**Απάντηση:**.....  
.....  
.....

**1<sup>η</sup> Δραστηριότητα (10 πόντους για την 1<sup>η</sup> ομάδα για κάθε απάντηση -2 για κάθε επόμενη):**

Με τη βοήθεια του αλγόριθμου Vigenère (Βιζενέρ) και με κλειδί τη λέξη «ΟΧΙ» κρυπτογραφήστε τις παρακάτω φράσεις

α) Η ΑΣΦΑΛΕΙΑ ΑΥΞΗΘΗΚΕ

.....

β) ΓΙΑ ΥΠΟΛΟΓΙΣΤΗ ΕΥΚΟΛΟ

.....

**2<sup>η</sup> Δραστηριότητα (10 πόντους για την 1<sup>η</sup> ομάδα για κάθε απάντηση -2 για κάθε επόμενη):**

Τώρα είστε κρυπταναλυτές. Γνωρίζετε πως το κλειδί είναι η λέξη «ΝΑΙ» και ο ίδιος αλγόριθμος. Αποκρυπτογραφήστε τη φράση «ΝΥΓΓΤΨΒΕΑΜ»





**Φύλλο εργασίας 4: Στεγανογραφία/υδατογράφηση**

Η στεγανογραφία δεν είναι τίποτα άλλο από την απόκρυψη της πληροφορίας σε κάτι που μοιάζει εντελώς αθώο. Μόνο ο παραλήπτης γνωρίζει πως μπορεί να δει την κρυμμένη πληροφορία παρότι όλοι μπορούν να τη δουν.

Παράδειγμα: Στέλνει κάποιος το μήνυμα «θέλω άμεσα, στην επόμενη δυνατόν ώρα, μερικές ελιές, ταραμά, αυγά». Ο παραλήπτης ξέρει πως το μήνυμα είναι αν βάλει στη σειρά τα πρώτα γράμματα των λέξεων και λαμβάνει το μήνυμα «Θα σε δω μετά»

Ερώτηση: Τι άλλους τρόπους μπορείτε να σκεφτείτε για την απόκρυψη πληροφορίας

Απάντηση:.....  
.....  
.....

Ερώτηση: Πως πιστεύετε πως μπορεί αυτή η τεχνική να αξιοποιηθεί στον ψηφιακό μας κόσμο;

Απάντηση:.....  
.....  
.....

**1<sup>η</sup> Δραστηριότητα (10 πόντους για την 1<sup>η</sup> ομάδα -2 για κάθε επόμενη):**

Ξέρετε πως το κείμενο που ακολουθεί περιέχει κάποιο μήνυμα. Ποιο μπορεί να είναι αυτό;

Ασυναρτησίες, αυτά ανέκαθεν βαριόμουν! Αν ατελείωτα σήμερα, ας τελειώσουν αμέσως! Με κάθε ημέρα περάτωσης ασταμάτητα παράγονται.

.....  
.....

**2<sup>η</sup> Δραστηριότητα (10 πόντους για την 1<sup>η</sup> ομάδα για κάθε απάντηση -2 για κάθε επόμενη):**

Θέλετε να στείλετε το μήνυμα «Πάρε με τηλέφωνο». Προσπαθήστε να στείλετε αυτό το μήνυμα σε ένα παραλήπτη χωρίς να μπορεί κάποιος να το καταλάβει. Δε χρειάζεται υποχρεωτικά να είναι με τους προηγούμενους τρόπους.



### Ενδεικτικές δραστηριότητες για την περιγραφική αξιολόγηση

Προτείνεται οι επιλογή των δραστηριοτήτων για την περιγραφική αξιολόγηση να γίνεται από τον/την εκπαιδευτικό λαμβάνοντας υπόψη όλες τις παραμέτρους και τους συγκεκριμένους στόχους που θέτει κατέχοντας καθολική και καλύτερη εικόνα της ομάδας στόχου. Οι δραστηριότητες αυτές αναπροσαρμόζονται συνεχώς και διαμορφώνονται με τη δυναμική της τάξης. Ενδεικτικά μια σύντομη ρουμπρίκα παρατήρησης για το κάθε μέλος της ομάδας θα βοηθήσει τον/την εκπαιδευτικό να κρατά σημειώσεις που θα βοηθήσουν στην τελική περιγραφική αξιολόγηση.

Ομάδα Α(1-5)	Πρωτοβουλία(1-5)	Συνεργασία	Ενδιαφέρον	Ένδειξη κατανόησης	....
Μαθητής Α	4	2	5	3	....
Μαθητής Β	....	....	....	....	....
Μαθητής Γ	....	....	....	....	....
.....	....	....	....	....	....
Ομάδα Β	....	....	....	....	....

### Φύλλα περιγραφικής αυτο-αξιολόγησης (έως 2 σελίδες)

Οι μαθητές και οι μαθήτριες καλούνται στο τέλος του προγράμματος να συμπληρώσουν ένα σύντομο ερωτηματολόγιο για τον εαυτό τους κι ένα για δύο μέλη της ομάδας τους. Τόσο η αυτοαξιολόγηση όσο και η ετεροαξιολόγηση θα βοηθήσουν στην βαθύτερη κατανόηση των στόχων του προγράμματος και στην ανάδειξη υπεύθυνης και κριτικής στάσης. Ενδεικτικά παρατίθενται και προτείνεται να δημιουργηθούν σε μια εφαρμογή νέφους ώστε οι μαθητές και οι μαθήτριες να μπορούν εύκολα να το συμπληρώσουν οποιαδήποτε στιγμή από οποιαδήποτε συσκευή(π.χ. google forms):



## Φύλλο Αυτοαξιολόγησης

Ον/μο:

Τάξη:

Τμήμα:

Απαντήστε στις παρακάτω ερωτήσεις.

- Πιστεύω ότι βοήθησα την ομάδα μου να πετύχει και κατάφερα να δώσω ιδέες σε όλες τις δραστηριότητες  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Συμμετείχα ενεργά και βοήθησα στην πορεία της ομάδας μου στο παιχνίδι  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Άκουγα προσεκτικά τα υπόλοιπα μέλη της ομάδας και δεχόμουν τις ιδέες τους ακόμα κι όταν διαφωνούσα  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Έκανα ερωτήσεις και προσπαθούσα να λύσω όλες τις απορίες μου  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Οι δικές μου προτάσεις χρησιμοποιήθηκαν από την ομάδα μου  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Μπορώ να δημιουργήσω ένα κρυπτογραφημένο κείμενο  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Μπορώ να δημιουργήσω ένα στεγανογραφημένο κείμενο  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Μπορώ να περιγράψω τις τεχνικές κρυπτογράφησης/στεγανογραφίας που χρησιμοποιούνται στον ψηφιακό κόσμο  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Μπορώ να φτιάξω συναρτήσεις και να κάνω πράξεις με κελιά σε ένα υπολογιστικό φύλλο  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Μπορώ να χρησιμοποιήσω μια εφαρμογή παρουσιάσεων/δημιουργίας βίντεο για να δείξω τα αποτελέσματα της έρευνάς μου  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Μπορώ να εξηγήσω σε κάποιον/α γιατί είναι σημαντική η ασφάλεια και η ιδιωτικότητα στο διαδίκτυο  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου



## Φύλλο αξιολόγησης του/της συμμαθητή/τριας μου Α

Ον/μο:

Τάξη:

Τμήμα:

Ον/μο του/της συμμαθητή/τριας μου:

Τάξη:

Τμήμα:

Απαντήστε στις παρακάτω ερωτήσεις.

- Πιστεύω ότι βοήθησε την ομάδα μου να πετύχει και κατάφερε να δώσει ιδέες σε όλες τις δραστηριότητες  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Συμμετείχε ενεργά και βοήθησα στην πορεία της ομάδας μου στο παιχνίδι  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Άκουγε προσεκτικά τα υπόλοιπα μέλη της ομάδας και δεχόταν τις ιδέες τους ακόμα κι όταν διαφωνούσε  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Έκανε ερωτήσεις και προσπαθούσε να λύσει όλες τις απορίες του/της  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Οι δικές του/της προτάσεις χρησιμοποιήθηκαν από την ομάδα μου  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Μπορεί να δημιουργήσει ένα κρυπτογραφημένο κείμενο  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Μπορεί να δημιουργήσει ένα στεγανογραφημένο μήνυμα  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Μπορώ να περιγράψω τις τεχνικές κρυπτογράφησης/στεγανογραφίας που χρησιμοποιούνται στον ψηφιακό κόσμο  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Μπορεί να φτιάξει συναρτήσεις και να κάνει πράξεις με κελιά σε ένα υπολογιστικό φύλλο  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Μπορεί να χρησιμοποιήσει μια εφαρμογή παρουσιάσεων/δημιουργίας βίντεο για να δείξει τα αποτελέσματα της έρευνάς του/της  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου
- Μπορεί να εξηγήσει σε κάποιον/α γιατί είναι σημαντική η ασφάλεια και η ιδιωτικότητα στο διαδίκτυο  
5. Πάρα πολύ 4. Πολύ 3. Αρκετά 2. Λίγο 1. Καθόλου



## Περιγραφή ενδεικτικών δραστηριοτήτων για το portfolio μαθητή/-τριας

Σε κάθε φάση ζητούμε από τον κάθε μαθητή και μαθήτρια να καταγράψει πέντε λέξεις/φράσεις μια για το συναίσθημά μου μία για το τι έμαθα, μια για το τι με δυσκόλεψε για το τι με ενόχλησε και ποιο το μεγαλύτερο επίτευγμά μου. Στο τέλος του προγράμματος θα συμπεριλάβουν στο προσωπικό τους portfolio ένα σύννεφο των λέξεων φράσεων όλων των εργαστηρίων. Το μετάλλιο που κατέκτησαν που μπορεί να συνοδεύεται κι από ένα πιστοποιητικό επίδοσης δημιουργημένο από την επιτροπή των κριτών. Μια φωτογραφία ή στιγμιότυπο οθόνης (printscreen) από την παρουσίαση της εργασίας μπορεί επίσης να συμπεριληφθεί.

## Βιβλιογραφία

- Duerden, M. D., Witt, P. A., Fernandez, M., Bryant, M. J., & Theriault, D. (2012). Measuring Life Skills: Standardizing the Assessment of Youth Development Indicators. *Journal of Youth Development*, 7(1), 99–117.  
<https://doi.org/10.5195/jyd.2012.155>
- Johnson, R. T., & Johnson, D. W. (2008). Active Learning: Cooperation in the Classroom. *The Annual Report of Educational Psychology in Japan*, 47(0), 29–30.  
[https://doi.org/10.5926/arepj1962.47.0\\_29](https://doi.org/10.5926/arepj1962.47.0_29)
- Werbach, K. (2014). (Re)defining gamification: A process approach. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8462 LNCS, 266–272.  
[https://doi.org/10.1007/978-3-319-07127-5\\_23](https://doi.org/10.1007/978-3-319-07127-5_23)
- Ινστιτούτο Εκπαιδευτικής Πολιτικής (2020) Επιμορφωτικό Υλικό: Εργαστήριο Δεξιοτήτων Πιλοτική Εφαρμογή
- Ευρωπαϊκή Επιτροπή - Περιφερειακή Διεύθυνση Πρωτοβάθμιας και Δευτεροβάθμιας Εκπαίδευσης Κρήτης. (2020). *CRISS - Απόκτηση, αξιολόγηση και πιστοποίηση της Ψηφιακής Ικανότητας - Διδακτικά Σενάρια Πιστοποίησης* (Γ. Γώγουλος, Γ. Πανσεληνάς, & Ι. Τζωρτζάκης, Eds.). Π.Δ.Ε. Κρήτης.



## Ερωτήσεις 1<sup>ου</sup> προγράμματος

1. Το παιγνιδοποιημένο πλαίσιο δε θα βοηθήσει σημαντικά στην ενεργοποίηση των μαθητών και των μαθητριών.
  - Σωστό
  - Λάθος
2. Η κρυπτογράφηση και η στεγανογραφία περιέχουν τεχνικές και μεθόδους που κεντρίζουν το ενδιαφέρον των νέων.
  - Σωστό
  - Λάθος
3. Στο πρώτο εργαστήριο προτείνεται μια συζήτηση αφόρμησης
  - για την ασφάλεια των δεδομένων και των επικοινωνιών
  - για τον Ιούλιο Καίσαρα και την αλληλογραφία του
  - για τον χώρο κλειδιού του προτύπου κρυπτογράφησης AES
4. Οι μαθητές και οι μαθήτριες θα κληθούν στα φύλλα εργασίας να κρυπτογραφήσουν και να αποκρυπτογραφήσουν μηνύματα.
  - Σωστό
  - Λάθος
5. Στον κώδικα του Καίσαρα οι μαθήτριες και οι μαθητές θα προβληματιστούν και θα κληθούν να βρουν
  - πως κρυπτογραφείται ένα μήνυμα με λατινικούς χαρακτήρες
  - τον μέγιστο αριθμό κλειδιών που μπορεί κάποιος να χρησιμοποιήσει
  - πως αποκρυπτογραφούνται τα σημεία σίξης
6. Οι μαθήτριες και οι μαθητές θα βρεθούν αντιμέτωποι με την πρόκληση της χρήσης συναρτήσεων και πράξεων σε λογιστικό φύλλο.
  - Σωστό
  - Λάθος
7. Στο κρυφό μήνυμα που θα δημιουργήσουν οι μαθητές και οι μαθήτριες αν χρησιμοποιήσουν την κρυπτογράφηση Βιζενέρ θα
  - χρησιμοποιήσουν οποιοδήποτε κλειδί - λέξη
  - χρησιμοποιήσουν μια λέξη- κλειδί από μια μικρή ομάδα μικρών λέξεων
  - χρησιμοποιήσουν μια κωδικοποιημένη σε κώδικα Καίσαρα λέξη
8. Οι μαθητές και οι μαθήτριες θα πρέπει σε ένα εργαστήριο να αναρτήσουν ένα κρυπτογραφημένο κι ένα στεγανογραφημένο μήνυμα
  - στον πίνακα ανακοινώσεων του σχολείου
  - σε μια κοινόχρηστη ηλεκτρονική πλατφόρμα
  - σε έναν οποιοδήποτε υπολογιστή του εργαστηρίου πληροφορικής