

# Κωδικοποίηση

|                     |                                                                           |
|---------------------|---------------------------------------------------------------------------|
| Θέμα                | Αλγόριθμοι                                                                |
| Μαθησιακοί στόχοι   | Γνωριμία με τους διαφορετικούς τρόπους κωδικοποίησης και αποκωδικοποίησης |
| Ηλικιακή ομάδα      | 12-16 έτη (προσαρμόσιμη για κάθε χώρα)                                    |
| Εκτιμώμενη διάρκεια | 45 λεπτά                                                                  |
| Εργασίες            | Κρυπτογράφηση και αποκρυπτογράφηση                                        |
| Σχετικές επισκέψεις | Παρίσι                                                                    |

## Προαπαιτούμενες γνώσεις

Δεν απαιτούνται συγκεκριμένες προϋποθέσεις

## Βήμα - βήμα: η ακολουθία στην πράξη

### Βήμα 1: Εισαγωγή στο θέμα

#### Σύντομη παρουσίαση των ιστορικών στοιχείων της συγκεκριμένης ακολουθίας

Η κρυπτογραφία είναι μια επιστήμη κάπου ανάμεσα στα μαθηματικά και στην επιστήμη των υπολογιστών αλλά με πολύ πρακτικές εφαρμογές. Σκοπός της είναι να προστατεύσει τις πληροφορίες, κάνοντάς τες συνήθως να φαίνονται ακατανόητες, αναμιγνύοντας και μετασχηματίζοντάς τες, σύμφωνα με μια συγκεκριμένη μέθοδο.

Υπάρχει, επίσης, μια κρυπτογραφική τεχνική που ονομάζεται *στεγανογραφία*, η οποία χρησιμοποιείται για να κρύψει ένα μήνυμα σε ένα φαινομενικά απλό κείμενο ή σε εικόνες. Αυτά τα μηνύματα μπορούν να σταλούν δημόσια, χωρίς να ανησυχείτε μήπως υποκλαπούν ή ανακαλυφθούν, ακόμη και κατά λάθος.



VISIT MATH



Με τη συγχρηματοδότηση  
της Ευρωπαϊκής Ένωσης

## Λίγη ιστορία

- Από το 800 π.Χ. ως το 200 π.Χ.: Οι Σπαρτιάτες χρησιμοποιούν σκυτάλες.
- Γύρω στο 600 π.Χ.: Ο Ναβουχοδονόσορ χρησιμοποιούσε ξυρισμένα κρανία
- Γύρω στο 480 π.Χ.: Ο Δημάρατος (Έλληνας), απομονωμένος στην Περσία, χρησιμοποιεί κέρνα δισκία για να προειδοποιήσει τη χώρα του για τα σχέδια του Ξέρξη (Περσία)
- 100 π.Χ. / 44 π.Χ.: Η κρυπτογράφηση του Καίσαρα (αλφαβητική μετατόπιση)
- 1ος αιώνας: Εμφάνιση αόρατου μελανιού (οργανικά υγρά, πλούσια σε άνθρακα)
- 1580: Ψηφίο που αντικαθίσταται από σύμβολο (Ονοματολογία κώδικα) - Mary Stuart
- 1586: Πραγματεία για τους κρυπτογράφους: κρυπτογράφηση Vigenère
- 1930: Συσκευή Enigma
- Τέλη 20ου αιώνα: Εμφάνιση κρυπτογράφησης δημόσιου κλειδιού – RSA

Ορισμοί για την κωδικοποίηση:

**Κρυπτολογία:** Η επιστήμη της κρυπτογραφίας και της κρυπτανάλυσης.

**Κρυπτογραφία:** Επιστήμη της δημιουργίας κρυπτογραφημάτων.

**Κρυπτανάλυση:** Επιστήμη της ανάλυσης κρυπτογραφημάτων με σκοπό την αποκρυπτογράφηση τους.

**Κρυπτόγραμμα:** Κρυπτογραφημένο μήνυμα.

**Κρυπτογράφηση / Κρυπτογράφιση / Κρύπτη:** Μετατροπή ενός κειμένου ή μιας πληροφορίας με αντικατάσταση των γραμμάτων (ή των λέξεων προς κωδικοποίηση) σε ένα σενάριο που αποτελείται από προκαθορισμένα σημάδια.

**Αποκρυπτογράφηση / Αποκωδικοποίηση:** μετατροπή ενός κρυπτογραφημένου μηνύματος σε ένα σαφές μήνυμα που συμμορφώνεται με το πρωτότυπο.

**Αποκρυπτογράφιση:** η αποκάλυψη της κρυπτογράφησης που χρησιμοποιείται στο κρυπτόγραμμα.

**Μη κρυπτογραφημένο κείμενο:** το αρχικό μήνυμα πριν από την κρυπτογράφιση.

**Κρυπτοκείμενο:** κείμενο που λαμβάνεται μετά από κρυπτογράφιση.



Με τη συγχρηματοδότηση  
της Ευρωπαϊκής Ένωσης

**Κλειδί:** Στοιχείο (λέξη ή αριθμός) που μεταφέρει την πληροφορία κατά την εφαρμογή της μεθόδου κρυπτογράφησης ή/και αποκρυπτογράφησης

### Ταξινόμηση κωδικών

**Αντικατάσταση κρυπτογράφησης:** Κρυπτοσύστημα στο οποίο κάθε γράμμα του μηνύματος αντικαθίσταται από άλλο χαρακτήρα, αλλά διατηρεί τη θέση του στο μήνυμα.

**Μεταφορά κρυπτογράφησης:** Κρυπτοσύστημα στο οποίο κάθε γράμμα του μηνύματος παραμένει αμετάβλητο, αλλά μετακινείται σε άλλο σημείο του μηνύματος.

**Μονοαλφαβητική αντικατάσταση:** Κρυπτογράφηση αντικατάστασης όπου το κρυπτογραφημένο αλφάβητο παραμένει το ίδιο καθ' όλη τη διάρκεια της κρυπτογράφησης. Αντικατάσταση με γράμματα, σύμβολα, ψηφία ή αριθμούς κ.λπ.

**Πολυαλφαβητική αντικατάσταση:** Κρυπτογράφηση αντικατάστασης όπου το κρυπτογραφημένο αλφάβητο αλλάζει κατά τη διάρκεια της κρυπτογράφησης. Αυτή η αλλαγή πραγματοποιείται σύμφωνα με ένα κλειδί.

**Κωδικός ονοματολογίας:** Αυτός ο τύπος κρυπτογράφησης συνδυάζει την απλή αντικατάσταση (κάθε γράμμα αντικαθίσταται από ένα σύμβολο) και έναν κωδικό ευρετηρίου (ορισμένες λέξεις αντικαθίστανται επίσης από ένα σύμβολο, καθώς και διασπαστικά σύμβολα).

## Βήμα 2: Εργασίες στην τάξη

Παραδείγματα από τα πιο γνωστά συστήματα κωδικοποίησης

### 1. Ο κώδικας του Καίσαρα

Για σημαντικές επικοινωνίες με τον στρατό του, ο Καίσαρας κρυπτογραφούσε τα μηνύματά του. Αυτό που είναι γνωστό ως κρυπτογράφηση του Καίσαρα (μονοαλφαβητική αντικατάσταση) είναι μια μετατόπιση των γραμμάτων στη θέση 4: για να κρυπτογραφηθεί ένα μήνυμα, το **A** γίνεται **D**, το **B** γίνεται **E**, το **C** γίνεται **F** κ.ο.κ.

Για να ληφθούν υπόψη όλα τα γράμματα του αλφαβήτου, είναι σοφότερο να αναπαραστήσετε το αλφάβητο σε έναν τροχό.



Credit Fermat Science

Για να κρυπτογραφήσετε το μήνυμα

DOHD MDFWD HVW

οπότε το μόνο που έχετε να κάνετε είναι να μετακινήσετε τα γράμματα προς την άλλη κατεύθυνση: το D αποκωδικοποιείται ως A, το E ως B, κ.λπ.

Το κωδικοποιημένο μήνυμα είναι:

ALEA JACTA EST

Αποκωδικοποίησε τα ακόλουθα κρυπτογραφημένα μηνύματα:

WKH URPDQV

YLFWRUB

HPSHURU

## 2 Ο κώδικας του Βιζενέρ

Ο κώδικας κρυπτογράφησης του Βιζενέρ είναι ένας πολυαλφαβητικός αλγόριθμος υποκατάστασης. Αντί να αντιστοιχίζονται τα γράμματα κυκλικά, κάθε γράμμα συνδέεται πλέον με ένα άλλο γράμμα (χωρίς σταθερή σειρά ή κατά έναν γενικό κανόνα).

Για παράδειγμα :

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



Με τη συγχρηματοδότηση  
της Ευρωπαϊκής Ένωσης

Για να κρυπτογραφήσετε το μήνυμα

**TO BE OR NOT TO BE THAT IS THE QUESTION**

να ελέγξετε την αντιστοιχία και να αντικαταστήσετε το γράμμα Ε με το γράμμα Χ,  
μετά το γράμμα Τ με το γράμμα G και μετά το γράμμα R με το γράμμα Κ...

Το κωδικοποιημένο μήνυμα είναι:

**GDQXDKSDGGDQXGEFGPVGEX ZRXVPDS**

Για να το αποκρυπτογραφήσουμε, γνωρίζοντας τις αντικαταστάσεις, κάνουμε την  
αντίστροφη πράξη.

Να αποκρυπτογραφήσετε τα τρία ακόλουθα μηνύματα:

HFGE PV IFSGF VGPB

OWFJ NPGE SRHQX KV

FSDGEXK PMXF IKDH HFGEV

### 3. Το σύστημα κρυπτογράφησης Πόρτα

Ο Πόρτα ήταν Ιταλός φυσικός και εφευρέτης του πρώτου κυριολεκτικά συστήματος διπλού κλειδιού, δηλαδή της πρώτης κρυπτογράφησης στην οποία το αλφάβητο αλλάζει με κάθε γράμμα.

Αυτό το πολυαλφαβητικό σύστημα ήταν εξαιρετικά ισχυρό για την εποχή του, τόσο που πολλοί θεωρούν τον Πόρτα ως τον «πατέρα της σύγχρονης κρυπτογραφίας». Ο Τζιοβάννι ντέλα Πόρτα εφηύρε το σύστημα κρυπτογράφησης του το 1563 και χρησιμοποιήθηκε με επιτυχία για τρεις αιώνες.

Ακολουθεί ένα παράδειγμα του πίνακα κρυπτογράφησης Πόρτα:

|    |                                                        |
|----|--------------------------------------------------------|
| AB | a b c d e f g h i j k l m<br>n o p q r s t u v w x y z |
| CD | a b c d e f g h i j k l m<br>z n o p q r s t u v w x y |
| EF | a b c d e f g h i j k l m<br>y z n o p q r s t u v w x |
| GH | a b c d e f g h i j k l m<br>x y z n o p q r s t u v w |
| IJ | a b c d e f g h i j k l m<br>w x y z n o p q r s t u v |
| KL | a b c d e f g h i j k l m<br>v w x y z n o p q r s t u |
| MN | a b c d e f g h i j k l m<br>u v w x y z n o p q r s t |
| OP | a b c d e f g h i j k l m<br>t u v w x y z n o p q r s |
| QR | a b c d e f g h i j k l m<br>s t u v w x y z n o p q r |
| ST | a b c d e f g h i j k l m<br>r s t u v w x y z n o p q |
| UV | a b c d e f g h i j k l m<br>q r s t u v w x y z n o p |
| WX | a b c d e f g h i j k l m<br>p q r s t u v w x y z n o |
| YZ | a b c d e f g h i j k l m<br>o p q r s t u v w x y z n |

Credit photo – apprendre-en-ligne.net

Για να κρυπτογραφήσετε, χρησιμοποιώντας ένα από αυτά τα αλφάβητα, θα επιλέξετε το αντίστοιχο γράμμα στη δεύτερη σειρά του πίνακα, για να αντικαταστήσει το γράμμα στο απλό κείμενο. Για παράδειγμα, εάν κρυπτογραφείτε χρησιμοποιώντας το αλφάβητο **AB**, θα χρησιμοποιήσετε αντί για το **a** το **n**, αντί για το **b** το **o**, αντί για το **q** το **d**, και ούτω καθεξής.

Για παράδειγμα, εάν η λέξη-κλειδί είναι **STEEL**, τα αλφάβητα **S, T, E, E, L, S, T, E, E, L**, κ.λπ. χρησιμοποιούνται διαδοχικά για την κρυπτογράφηση του μηνύματος. Αν κρυπτογραφήσουμε τη φράση "**Porta cipher**" με το κλειδί STEEL, θα έχουμε:

|                    |   |   |   |   |   |   |   |   |   |   |   |
|--------------------|---|---|---|---|---|---|---|---|---|---|---|
| Μη κρυπτογραφημένο | p | o | r | t | a | c | i | p | h | e | r |
| Κλειδί             | S | T | E | E | L | S | T | E | E | L | S |
| Κωδικοποιημένο     | L | K | G | I | V | T | Z | E | S | Z | A |

Η αποκρυπτογράφηση του Πόρτα χρησιμοποιήθηκε από τη βασίλισσα Μαρία-Αντουανέτα, με σκοπό να την τροποποιήσει και να τη βελτιώσει, προκειμένου να τη χρησιμοποιήσει στην αλληλογραφία της. Συγκεκριμένα, πρόσθεσε τη δυνατότητα κωδικοποίησης γράμματος για κάθε γράμμα.

### Βήμα 3: Εργασίες για το σπίτι και ιδέες ανάπτυξης

Τι θα λέγατε για μια πρόκληση; Να περάσετε, δηλαδή, κωδικοποιημένα μηνύματα στους συμμαθητές σας, για να τα αποκρυπτογραφήσουν;

Για παράδειγμα, να επιλέξετε μια μέθοδο κωδικοποίησης και να κρυπτογραφήσετε το μήνυμά σας και μετά να το μεταδώσετε, χωρίς όμως να φανερώσετε τη μέθοδο που χρησιμοποιήθηκε.

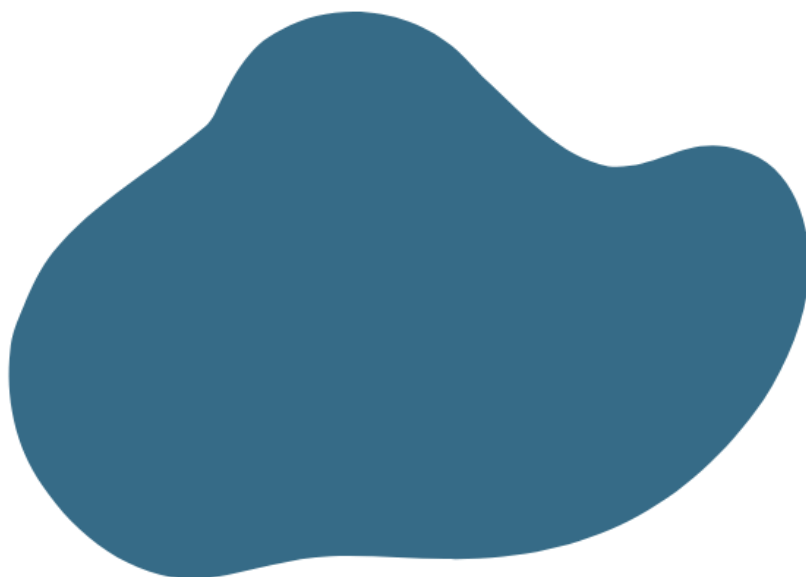
Προσθέστε λίγο σασπένς δίνοντας ένα χρονικό όριο ή μια ανταμοιβή.

Μπορείτε επίσης να δημιουργήσετε τον δικό σας τροχό αποκρυπτογράφησης, που είναι εύκολο να βρείτε στο διαδίκτυο:

<https://www.youtube.com/watch?v=0Xuv58Uwu9o>

### Υλικό που απαιτήθηκε

Οι μαθητές που συμμετέχουν στην ξενάγηση θα πρέπει να έχουν μολύβι, γόμα και χαρτί για να βρουν τον σωστό κωδικό.



Αυτό το έργο έχει χρηματοδοτηθεί με την υποστήριξη της Ευρωπαϊκής Επιτροπής. Αυτή η δημοσίευση αντικατοπτρίζει μόνο τις απόψεις του συγγραφέα και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν.

Κωδικός έργου: 1-FR01-KA220-SCH-00027771

Μάθετε περισσότερα για το Visit Math στη διεύθυνση:

<https://visitmath.eu>

Αυτό το έργο αδειοδοτείται με την άδεια Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (<http://creativecommons.org/licenses/by-nc-sa/4.0/>).

