

Γυμνάσιο Διαπολιτισμικής Εκπαίδευσης Α Αθήνας

Πληροφορική

Γ ΤΑΞΗ

ΦΥΛΛΑΔΙΟ 1



Τι είναι η κρυπτογραφία ;

Η κρυπτογραφία είναι η επιστήμη και η τέχνη της προστασίας πληροφοριών μέσω της μετατροπής τους σε μορφή που είναι δυσανάγνωστη για μη εξουσιοδοτημένα άτομα. Η

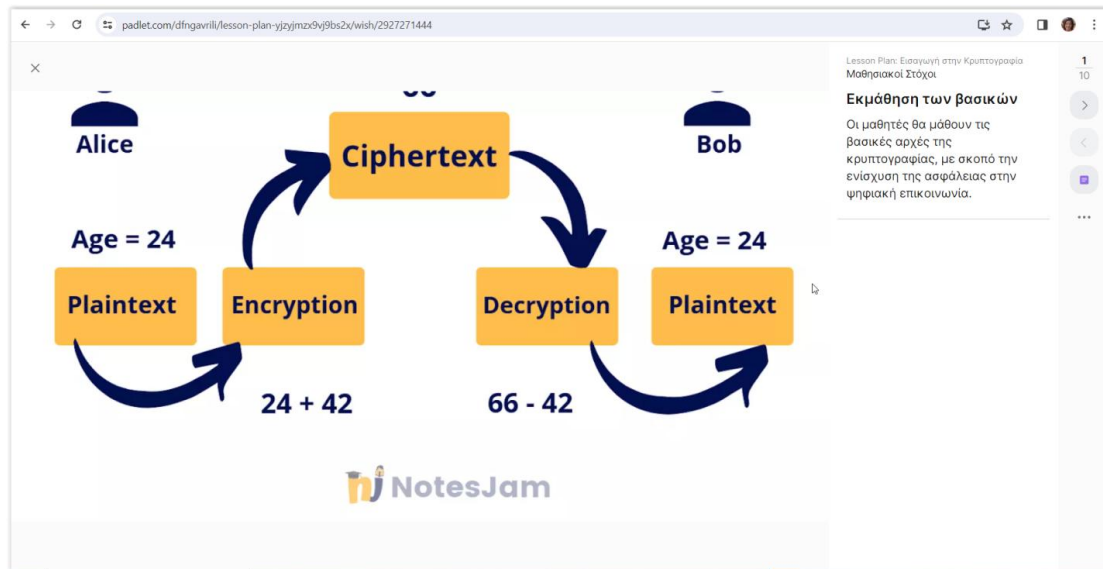
διαδικασία αυτή επιτυγχάνεται με τη χρήση μαθηματικών αλγορίθμων και κρυπτογραφικών κλειδιών.

1. Βασικοί στόχοι της κρυπτογραφίας είναι:

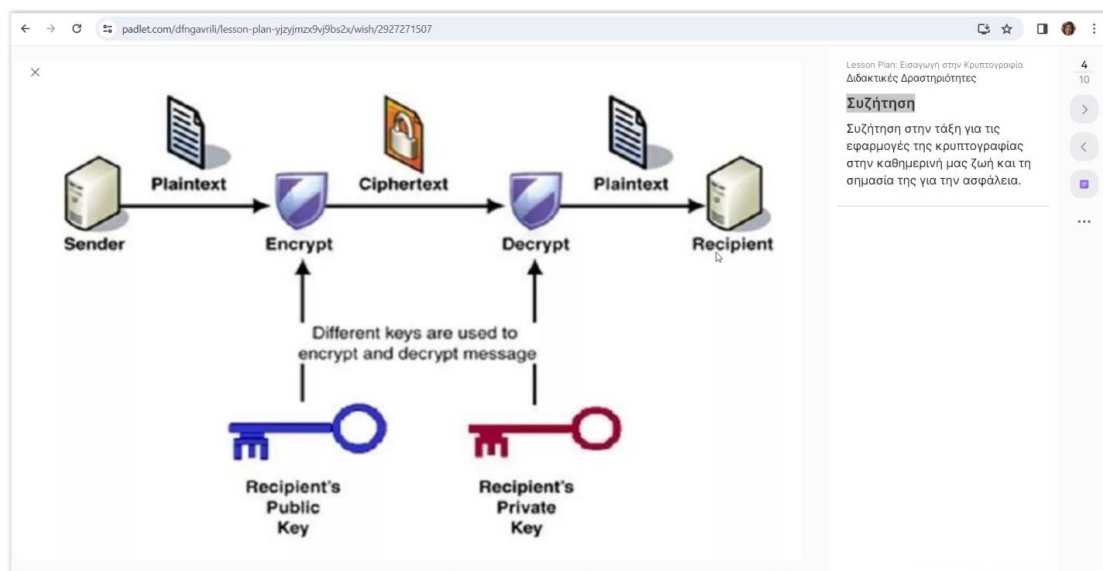
Η Κρυπτογραφία γενικότερα είναι η ανταλλαγή μηνυμάτων μεταξύ δύο μερών με τέτοιο τρόπο, ώστε η κατανόηση του περιεχομένου των μηνυμάτων να είναι δυνατή μόνο από τον αποστολέα και τον παραλήπτη.

Ως εκ τούτου έχει στόχο :

1. Εμπιστευτικότητα : Εξασφαλίζει ότι οι πληροφορίες είναι προσβάσιμες μόνο σε εκείνους που έχουν εξουσιοδοτημένη πρόσβαση.
2. Ακεραιότητα : Διασφαλίζει ότι οι πληροφορίες δεν έχουν αλλοιωθεί ή παραποιηθεί κατά τη μεταφορά ή την αποθήκευση.
3. Αυθεντικότητα : Επαληθεύει την ταυτότητα των μερών που επικοινωνούν και διασφαλίζει ότι οι πληροφορίες προέρχονται από αξιόπιστες πηγές.
4. Μη άρνηση : Εξασφαλίζει ότι ο αποστολέας των πληροφοριών δεν μπορεί να αρνηθεί ότι έστειλε το μήνυμα.



2. Βασικές έννοιες της κρυπτογραφίας:



1. Κρυπτογράφηση και αποκρυπτογράφηση :

- Κρυπτογράφηση : Η διαδικασία μετατροπής των δεδομένων σε μια μορφή που δεν είναι αναγνώσιμη (κρυπτογράφημα) χρησιμοποιώντας έναν αλγόριθμο και ένα κλειδί.

- Αποκρυπτογράφηση : Η αντίστροφη διαδικασία, όπου το κρυπτογράφημα μετατρέπεται πίσω στα αρχικά δεδομένα με τη χρήση του σωστού κλειδιού.

2. Κρυπτογραφικά κλειδιά :

- Συμμετρική κρυπτογραφία : Χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων. Παραδείγματα αλγορίθμων είναι το AES και το DES.

- Ασύμμετρη κρυπτογραφία : Χρησιμοποιεί δύο διαφορετικά κλειδιά, ένα δημόσιο κλειδί για την κρυπτογράφηση και ένα ιδιωτικό κλειδί για την αποκρυπτογράφηση. Παραδείγματα αλγορίθμων είναι το RSA και το ECC.

3. Ψηφιακές υπογραφές :

- Χρησιμοποιούνται για την επαλήθευση της αυθεντικότητας και της ακεραιότητας των μηνυμάτων ή των εγγράφων. Η ψηφιακή υπογραφή δημιουργείται με την χρήση του ιδιωτικού κλειδιού και επαληθεύεται με το αντίστοιχο δημόσιο κλειδί.

3. Ιστορία και εξέλιξη της κρυπτογραφίας:

Η κρυπτογραφία έχει τις ρίζες της στην αρχαιότητα, με παραδείγματα όπως ο κώδικας του Καίσαρα και οι ελληνικοί κρυπτογραφικοί μηχανισμοί. Στη σύγχρονη εποχή, η ανάπτυξη των υπολογιστών και των δικτύων απαιτούσε πιο σύνθετους και ισχυρούς κρυπτογραφικούς αλγόριθμους, οδηγώντας στην ανάπτυξη της συμμετρικής και ασύμμετρης κρυπτογραφίας και της κρυπτογραφίας δημόσιου κλειδιού.

Η κρυπτογραφία συνεχίζει να εξελίσσεται για να αντιμετωπίσει τις νέες προκλήσεις της ασφάλειας στον ψηφιακό κόσμο, όπως οι επιθέσεις κβαντικών υπολογιστών, και να εξασφαλίσει την προστασία των πληροφοριών σε διάφορες εφαρμογές και συστήματα.

4. Πού χρησιμοποιείται αναφορικά με τους υπολογιστές ;

Η κρυπτογραφία χρησιμοποιείται σε πολλούς τομείς αναφορικά με τους υπολογιστές και τις ψηφιακές επικοινωνίες. Μερικές από τις βασικές χρήσεις της περιλαμβάνουν:

1. Ασφαλής επικοινωνία :

- Email : Χρήση πρωτοκόλλων όπως το S/MIME και το PGP για την κρυπτογράφηση των μηνυμάτων ηλεκτρονικού ταχυδρομείου.
- Instant messaging : Εφαρμογές όπως το Signal και το WhatsApp χρησιμοποιούν κρυπτογράφηση end-to-end για την προστασία των συνομιλιών.

2. Ασφαλής αποθήκευση δεδομένων :

- Κρυπτογράφηση δίσκων : Εργαλεία όπως το BitLocker και το FileVault κρυπτογραφούν τα δεδομένα στον σκληρό δίσκο.
- Κρυπτογράφηση αρχείων : Λογισμικά όπως το VeraCrypt και το GnuPG χρησιμοποιούνται για την κρυπτογράφηση αρχείων και φακέλων.

3. Ασφάλεια στο Διαδίκτυο :

- HTTPS : Χρήση πρωτοκόλλου SSL/TLS για την κρυπτογράφηση των δεδομένων που μεταφέρονται μεταξύ του προγράμματος περιήγησης και του διακομιστή.

- VPN : Τα εικονικά ιδιωτικά δίκτυα χρησιμοποιούν κρυπτογράφηση για την προστασία των δεδομένων που μεταφέρονται μέσω μη ασφαλών δικτύων.

4. Ασφάλεια δικτύων :

- Wi-Fi : Πρωτόκολλα όπως το WPA3 κρυπτογραφούν τα δεδομένα που μεταφέρονται μέσω ασύρματων δικτύων.

- IPSec : Χρησιμοποιείται για την κρυπτογράφηση των δεδομένων σε δίκτυα IP.

5. Ηλεκτρονικές συναλλαγές :

- Πληρωμές : Χρήση κρυπτογράφησης στις ηλεκτρονικές συναλλαγές και στις πλατφόρμες πληρωμών (π.χ. πιστωτικές κάρτες, PayPal).

- Κρυπτονομίσματα : Τα κρυπτονομίσματα όπως το Bitcoin βασίζονται στην κρυπτογραφία για την ασφάλεια και την επαλήθευση των συναλλαγών.

6. Πιστοποίηση και ταυτοποίηση :

- Ψηφιακές υπογραφές : Χρήση κρυπτογραφίας για την επαλήθευση της αυθεντικότητας και της ακεραιότητας των εγγράφων.

- Πιστοποιητικά : Χρήση πιστοποιητικών για την ταυτοποίηση των χρηστών και των διακομιστών.

7. Προστασία της ιδιωτικότητας :

- Ανωνυμοποίηση δεδομένων : Χρήση τεχνικών κρυπτογράφησης για την προστασία της ιδιωτικότητας των χρηστών (π.χ. TOR).

Η κρυπτογραφία είναι ένας κρίσιμος τομέας για την ασφάλεια των πληροφοριών και των επικοινωνιών στον σύγχρονο ψηφιακό κόσμο.

Παραδείγματα κρυπτογραφίας :

The screenshot shows a presentation slide titled "What Is Cryptography". The slide content includes:

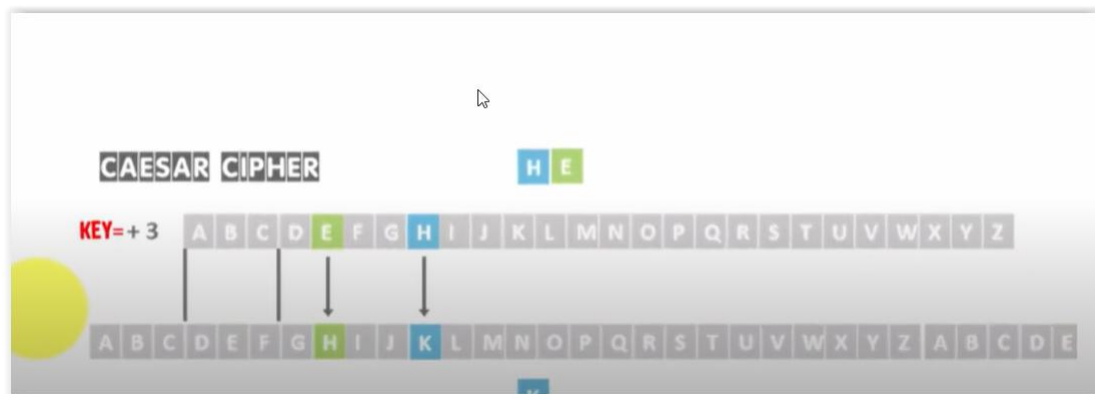
- Cryptology
 - The art (science) of communication with secret codes.
- Cryptography
 - The making of secret codes.
- Cryptanalysis
 - The "breaking" of codes.

Below the text, there is a diagram illustrating a simple substitution cipher. The top row shows the alphabet "X Y Z A B C D E F ...". The bottom row shows "A B C D E F G H I ...". Arrows indicate a mapping: X to A, Y to B, Z to C, A to D, B to E, C to F, D to G, E to H, and F to I. The letter 'B' in the top row and 'E' in the bottom row are highlighted in blue.

On the right side of the slide, there is a sidebar with the following text:

Lesson Plan: Εισαγωγή στην Κρυπτογραφία
Διακτινικές Δραστηριότητες
Παρουσίαση Θεμάτων
Εισαγωγή στην κρυπτογραφία:
ορισμοί, ιστορική αναδρομή, και
σημασία της στη σύγχρονη εποχή.

The sidebar also shows a progress indicator with the number 3 out of 10.



Πώς γίνεται η κρυπτογράφηση ?

Η κρυπτογράφηση ενός μηνύματος γίνεται για κάθε γράμμα του μηνύματος ξεχωριστά , ακολουθώντας τα εξής βήματα :

Βήμα 1 : Μετατρέπουμε το γράμμα σε έναν αριθμό που αντιστοιχεί στη σειρά του γράμματος μέσα στο αλφάβητο ξεκινώντας από το 0.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Αντιστοίχιση γραμμάτων στο Αγγλικό αλφάβητο

