Τι είναι η κρυπτογράφηση;

Η **κρυπτογράφηση** είναι ένας τρόπος να μετατρέπουμε ένα μήνυμα σε μορφή που **δεν μπορούν να διαβάσουν** οι άλλοι.

Πού χρειάζεται;

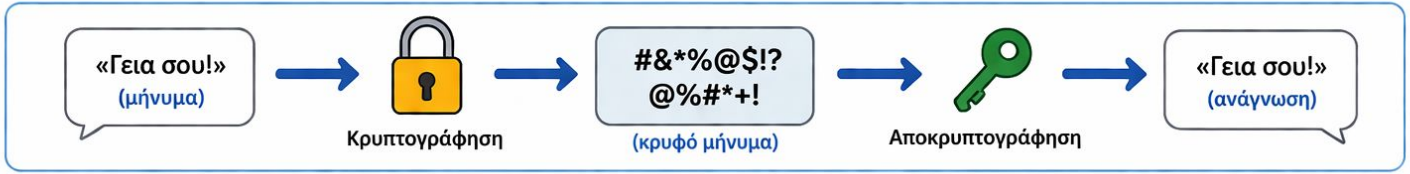
στις ιστοσελίδες

στα μηνύματα

στις αγορές στο διαδίκτυο

στα email

στις ηλεκτρονικές υπογραφές



Δύο τρόποι κρυπτογράφησης

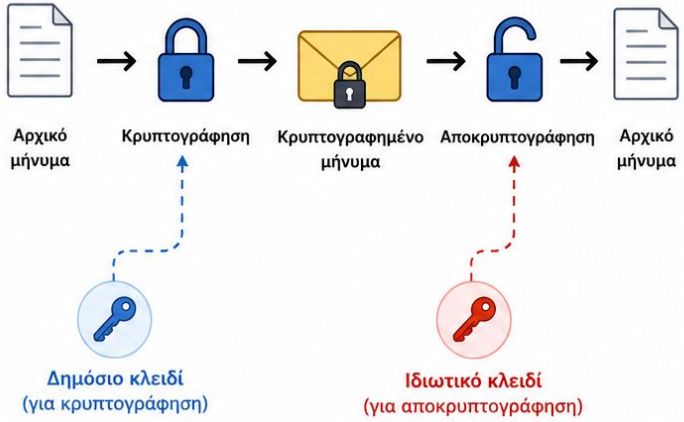
Υπάρχουν δύο βασικοί τρόποι:

Συμμετρική κρυπτογράφηση

Ένα κοινό κλειδί

Ασύμμετρη κρυπτογράφηση

Δύο διαφορετικά κλειδιά



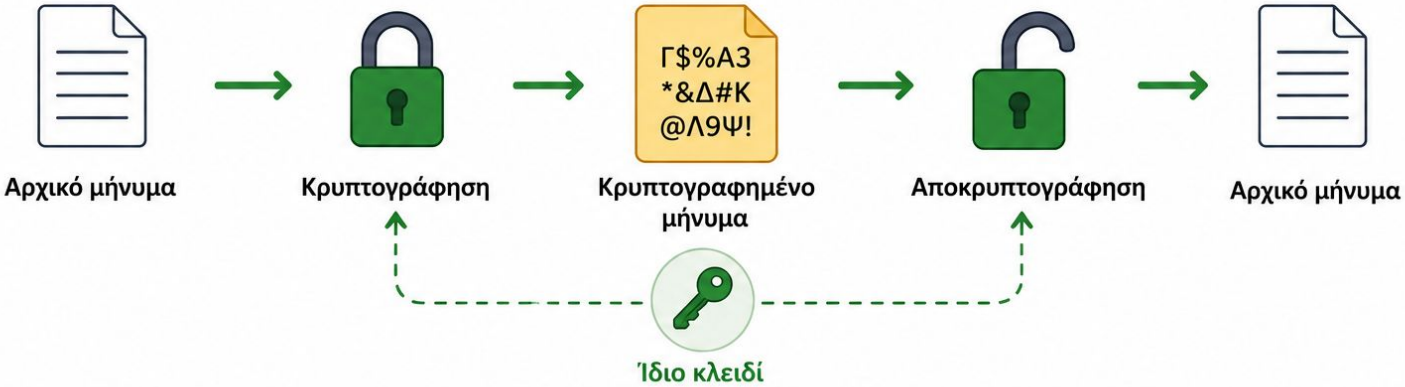
Συνοπτικά:

Συμμετρική: χρησιμοποιεί το **ίδιο κλειδί** για κρυπτογράφηση και αποκρυπτογράφηση.

Ασύμμετρη: χρησιμοποιεί δύο διαφορετικά κλειδιά, δημόσιο και ιδιωτικό.

Συμμετρική κρυπτογράφηση

Στη συμμετρική κρυπτογράφηση χρησιμοποιούμε το **ίδιο κλειδί** για την κρυπτογράφηση και την αποκρυπτογράφηση.



Παράδειγμα:

Κρυπτογράφηση του Καίσαρα

Κάθε γράμμα του μηνύματος μετακινείται κατά **3** θέσεις μπροστά στο αλφάβητο.

Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
			+3	+3	+3																		
Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ

Παράδειγμα: ΓΕΙΑ → ΔΟΚΔ (κάθε γράμμα μετακινείται 3 θέσεις μπροστά)

Δύο κλειδιά αντί για ένα

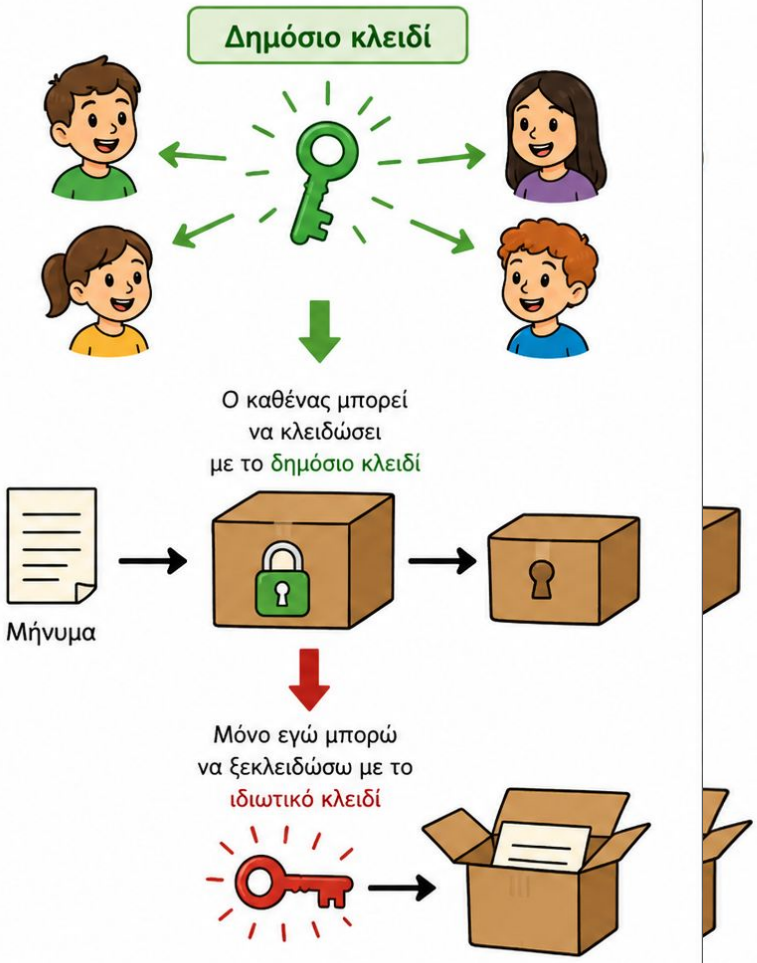
Στην ασύμμετρη κρυπτογράφηση έχουμε **δύο διαφορετικά κλειδιά**:

Δημόσιο κλειδί
Το δίνουμε σε όλους.

Ιδιωτικό κλειδί
Το κρατάμε μόνο εμείς.

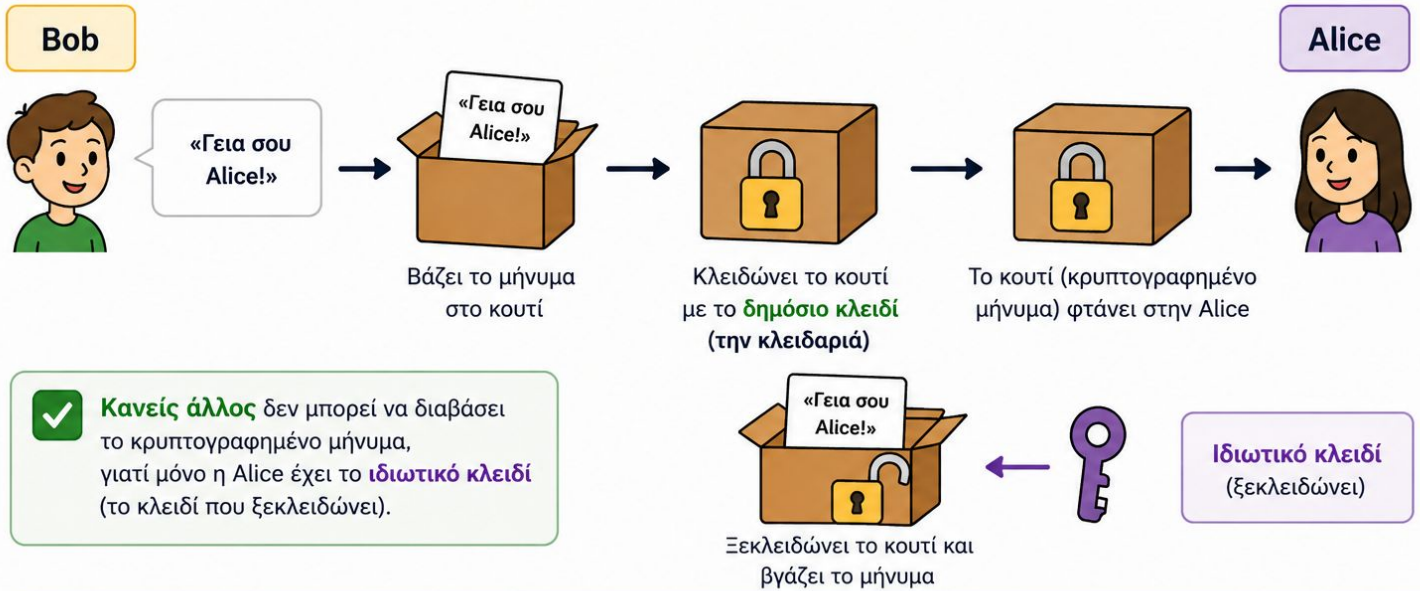
Ό,τι κλειδώνει με το **δημόσιο κλειδί**, ξεκλειδώνει μόνο με το **ιδιωτικό κλειδί**.

Σκεφτείτε ότι το **δημόσιο κλειδί** είναι σαν ένα λουκέτο που μπορώ να το μοιράσω σε όλους. Όποιος θέλει μπορεί να βάλει ένα μήνυμα μέσα σε ένα κουτί και να το κλειδώσει με το λουκέτο μου. Όμως το κλειδί που ανοίγει το λουκέτο το έχω μόνο εγώ.



Παράδειγμα: ο Bob στέλνει μυστικό στην Alice

Χρησιμοποιούμε το δημόσιο κλειδί της Alice.



Κανείς άλλος δεν μπορεί να διαβάσει το κρυπτογραφημένο μήνυμα, γιατί μόνο η Alice έχει το **ιδιωτικό κλειδί** (το κλειδί που ξεκλειδώνει).

Γιατί είναι ασφαλές;

Είναι εύκολο να κλειδώσεις, μα όχι να ξεκλειδώσεις χωρίς το σωστό κλειδί.

Στην πραγματικότητα οι αριθμοί είναι τεράστιοι — όχι σαν το 391.

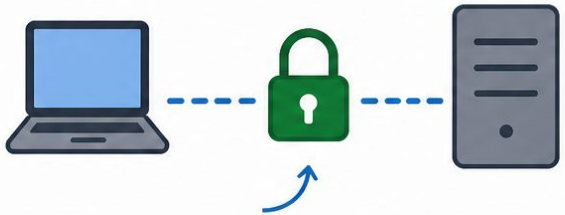
Πού το βλέπουμε καθημερινά;

Αυτή την ιδέα με το **δημόσιο** και το **ιδιωτικό** κλειδί τη χρησιμοποιούμε κάθε μέρα όταν μπαίνουμε σε ιστοσελίδες.

HTTPS

https:// www.sxoleio.gr

Όταν βλέπουμε **https://** και ένα λουκέτο μπροστά από τη διεύθυνση της ιστοσελίδας, σημαίνει ότι τα δεδομένα που στέλνουμε και λαμβάνουμε είναι **κρυπτογραφημένα.**



Οι πληροφορίες ταξιδεύουν κρυπτογραφημένες, οπότε **κανείς τρίτος** δεν μπορεί να τις διαβάσει.

Δεν σημαίνει ότι το site (η ιστοσελίδα) είναι «καλό».
Σημαίνει **μόνο** ότι η σύνδεση είναι **κρυπτογραφημένη**.

Πώς το ψηφιακό πιστοποιητικό συνδέεται με το δημόσιο και το ιδιωτικό κλειδί;

Το ψηφιακό πιστοποιητικό είναι η **«ταυτότητα»** που επιβεβαιώνει ότι το δημόσιο κλειδί ανήκει στο σωστό site (ή στο σωστό πρόσωπο).

1 Η φίλη σου σου δίνει ένα λουκέτο.

Το **δημόσιο κλειδί** (λουκέτο) μπορεί να το δώσει σε όλους.

2 Εσύ βάζεις το γράμμα σε ένα κουτί και το κλειδώνεις.

Χρησιμοποιείς το **δημόσιο κλειδί** (λουκέτο) για να κλειδώσεις και στέλνεις το κουτί.

ΤΟ ΠΡΟΒΛΗΜΑ

Πώς ξέρεις ότι το λουκέτο που πήρες είναι όντως της φίλης σου και όχι κάποιου άλλου που προσποιείται ότι είναι αυτή;

3 Η λύση: Ψηφιακό πιστοποιητικό.

Εσύ ελέγχεις την ταυτότητα **(ψηφιακό πιστοποιητικό)** και βεβαιώνεσαι ότι το λουκέτο είναι όντως της φίλης σου.

4 Μόνο η φίλη σου μπορεί να το ανοίξει.

Χρησιμοποιεί το **ιδιωτικό της κλειδί** (το κρατάει μόνο αυτή) για να ξεκλειδώσει το κουτί και να διαβάσει το γράμμα.

Συνοπτικά:

Δημόσιο κλειδί (το δίνει η φίλη σου) → Εσύ κλειδώνεις και στέλνεις → **Ψηφιακό πιστοποιητικό:** είναι η ταυτότητα που επιβεβαιώνει ότι το λουκέτο (δημόσιο κλειδί) είναι σωστό. → Ιδιωτικό κλειδί (το κρατάει μόνο η φίλη σου) = **Ασφαλής επικοινωνία!**

Το λουκέτο χωρίς την ταυτότητα μπορεί να είναι ψεύτικο. Με την **ταυτότητα (ψηφιακό πιστοποιητικό)** είμαστε σίγουροι ότι μιλάμε με το σωστό πρόσωπο (ή site).

Τι είναι η ψηφιακή υπογραφή;

Η ψηφιακή υπογραφή είναι σαν την υπογραφή μας σε ένα έγγραφο.
Δημιουργείται με το **ιδιωτικό κλειδί** και επαληθεύεται με το **δημόσιο κλειδί**.

Η Alice

έχει το δικό της προσωπικό «στυλό υπογραφής»

Ιδιωτικό κλειδί

→ με αυτό δημιουργεί την υπογραφή

→ το γνωρίζει μόνο η ίδια

Η Alice δημιουργεί την υπογραφή.

Οι άλλοι

έχουν έναν τρόπο ελέγχου (ανιχνευτή)

Δημόσιο κλειδί

→ ελέγχει αν η υπογραφή είναι αληθινή

→ μπορεί να το γνωρίζουν όλοι

Οι άλλοι ελέγχουν την υπογραφή.

Ροή διαδικασίας

Τι αποδεικνύει;

- Ποιος έστειλε το έγγραφο
- Ότι το έγγραφο δεν αλλοιώθηκε

Σημαντικό

Το δημόσιο κλειδί **ΔΕΝ** δημιουργεί υπογραφές.

Μόνο ελέγχει αν είναι γνήσιες.

Η πιο σωστή μαθητική διατύπωση

Το ιδιωτικό κλειδί λειτουργεί σαν το προσωπικό «στυλό υπογραφής» του κατόχου. Το δημόσιο κλειδί λειτουργεί σαν εργαλείο ελέγχου που επιβεβαιώνει ότι η υπογραφή είναι αυθεντική.