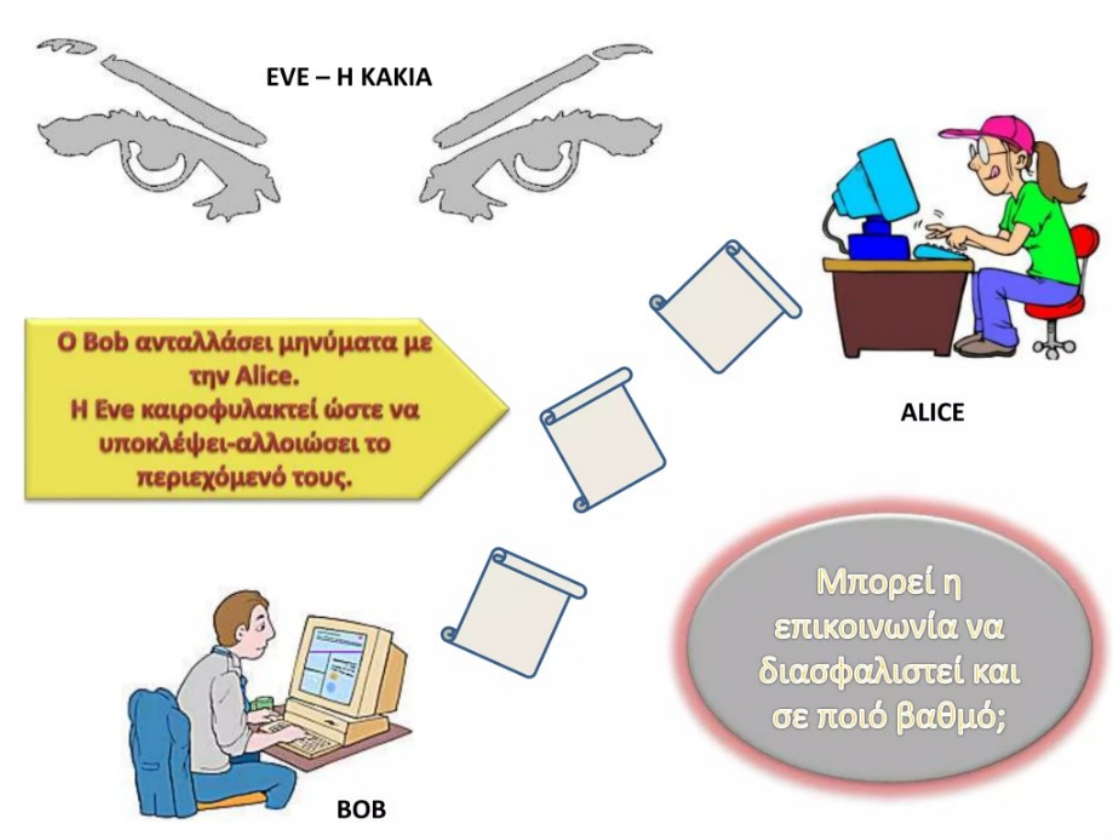


Κυβερνοασφάλεια- Κρυπτογραφία



Συμμετρική Κρυπτογράφηση

Συμμετρική Κρυπτογράφηση



Ο Καίσαρας «διδάσκει» τον αλγόριθμο Caesar Cipher

1. **Κρυπτογράφηση** : Το αλφάβητο ολισθαίνει προς τα αριστερά (το Α αντιστοιχεί στο Δ).
Εναλλακτικά «πηγαίνουμε» προς τα εμπρός.

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

2. **Αποκρυπτογράφηση** : Το αλφάβητο ολισθαίνει προς τα δεξιά (το Δ αντιστοιχεί στο Α).
Εναλλακτικά «γυρνάμε» προς τα πίσω.

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

Το παράδειγμα έχει ολίσθηση 3 γράμματα

Γνωστοί
αλγόριθμοι

- DES
- 3DES
- IDEA

Δέχονται σαν είσοδο μηνύματα των 64bits. Αν το μήνυμα είναι μεγαλύτερο, σπάει σε τμήματα των 64 bits.

Εργασία σε ομάδες:

Μπορείτε να αποκρυπτογραφήσετε το ακόλουθο μήνυμα; Σας στο στέλνει η δασκάλα σας χρησιμοποιώντας την κρυπτογράφηση του Καίσαρα που βασίζεται στην τεχνική ολίσθησης του αλφαβήτου. Πιο συγκεκριμένα ως κοινό μυστικό κλειδί έχει χρησιμοποιήσει **ολίσθηση τριών γραμμάτων**. Δείτε τη εικόνα από πάνω.

«ΘΥΑΣΠΧΔΜ ΧΔ ΑΥΜΦΧΨΖΘΠΔ»

Στη συνέχεια αποφασίζετε να τις στείλετε και εσείς το εξής μήνυμα: **«ΕΠΙΤΕΛΟΥΣ ΞΕΚΟΥΡΑΣΗ»**. Χρησιμοποιήστε την κρυπτογράφηση του Καίσαρα με ολίσθηση τριών γραμμάτων ώστε να το στείλετε στη δασκάλα σας.