Εξέταση με ανοιχτό βιβλίο.

Παρωχημένος ορισμός: Κρυπτογραφία είναι η τέχνη της συγγραφής και της επίλυσης με κώδικες.

Πλέον η κρυπτογραφία είναι επιστήμη.

Γιατί χρειαζόμαστε την κρυπτογραφία;
Τη χρησιμοποιούμε σε περιπτώσεις που θέλουμε να επικοινωνήσουμε παρουσία ενός αντιπάλου.

Στόχοι:

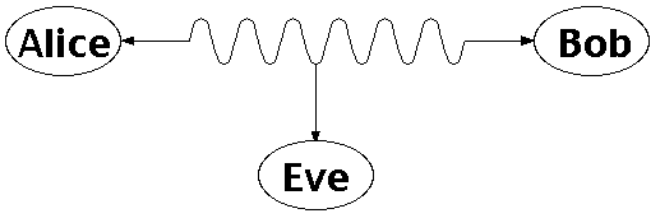
μυστικότητα (confidentiality)
ταυτοποίηση (authentication)
ακεραιότητα δεδομένων (data integrity)
μη-απάρνηση (non repudiation): Σημαίνει τη δυνατότητα ταυτοποίησης της πηγής του μηνύματος. Σε συγκεκριμένες περιπτώσεις λέγεται και ψηφιακή υπογραφή (digital signature).

Κλειδιά:

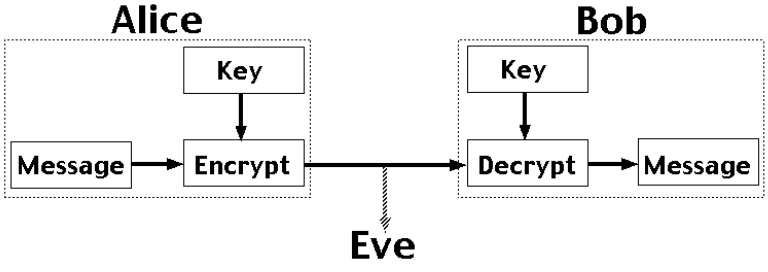
ασύμμετρα (public key) μοντέρνα κρυπτογραφία, 1976 και ύστερα
συμμετρικά (private key) κλασική κρυπτογραφία, έως το 1976

Κρυπτογραφία Συμμετρικού Κλειδιού:

Έστω ότι έχουμε δύο χρήστες που θέλουν να επικοινωνήσουν, την Αλίκη και το Μπόμπο. Το κανάλι μέσω του οποίου μπορούν να επικοινωνήσουν δεν είναι ασφαλές, αφού στο κανάλι κρυφακούει η Εύα (eavesdropper).



Η Αλίκη θέλει να στείλει ένα μήνυμα στον Μπόμπο χωρίς να το ακούσει η Εύα. Συνδυάζει το μήνυμα (M) με το κλειδί (key) και στέλνει το κωδικοποιημένο μήνυμα (C) μέσα στο κανάλι.



Αυτή η μέθοδος χρησιμοποιεί **συμμετρικά κλειδιά,** αφού η Αλίκη και ο Μπόμπος έχουν τα ίδια κλειδιά.

$$\begin{Bmatrix} \textit{κρυπτογράφηση}: & C = e_k(M) \\ \textit{αποκρυπτογράφηση}: & M = d_k(C) \end{Bmatrix} \quad M = d_k(e_k(M))$$

Χαρακτηριστικά:

- Μειονεκτήματα
  - Το πρόβλημα ανάγεται στο πώς θα δώσει η Αλίκη το κλειδί στο Μπόμπο για να αποκρυπτογραφήσει το μήνυμά της.
  - Για κάθε ζευγάρι χρηστών χρειάζεται διαφορετικό κλειδί. Έτσι για n χρήστες χρειαζόμαστε n^2 κλειδιά.
- Πλεονεκτήματα:
  - Τα πρωτόκολλα αυτά είναι πολύ γρήγορα.

Κρυπτογραφία δημόσιου κλειδιού (ασύμμετρα κλειδιά):

Τα κλειδιά αυτά ανακοινώνονται δημόσια.

Σύγκριση δημοσίων και ιδιωτικών κλειδιών:

Τα δημόσιο κλειδιά δεν χρειάζεται να ανανεωθούν αν μαθευτούν. Αντίθετα, τα ιδιωτικά κλειδιά θα πρέπει να ανανεωθούν αμέσως αν διαρρεύσουν.

Χαρακτηριστικά:

- Τα πρωτόκολλα που χρησιμοποιούν ασύμμετρα κλειδιά είναι πιο αργά από αυτά που χρησιμοποιούν συμμετρικά.
- Χρειαζόμαστε πολύ λιγότερα κλειδιά σε σχέση με τα συμμετρικά και συγκεκριμένα n κλειδιά για n χρήστες.
- Δεν χρειάζεται δύο χρήστες να συμφωνήσουν σε ένα κλειδί.

Κώδικας/Πρωτόκολλο του Καίσαρα:

Κωδικοποίηση: (το γράμμα +3)mod26

μεταθέτουμε το κάθε γράμμα κατά 3 θέσεις δεξιά.

Γενικά, όσο τα κλειδιά είναι ελάχιστα, η αποκωδικοποίηση είναι trivial, ενώ όσο περισσότερα πιθανά κλειδιά έχουμε, τόσο πιο δύσκολο είναι να αποκωδικοποιηθεί το μήνυμά μας.

Vigenère cipher

Τα μηνύματα που είναι σε φυσική γλώσσα μπορούν εύκολα να αποκωδικοποιηθούν λόγω της συχνοτικής ανάλυσης χαρακτήρων. Το πρόβλημα αυτό μπορεί να λυθεί μέσω του κλειδιού του Vigenère. Σύμφωνα με τη μέθοδο αυτή, γράφουμε όλα τα γράμματα του αλφαβήτου και από κάτω επαναλαμβάνουμε το κλειδί μέχρι να τελειώσουν τα γράμματα. Ύστερα προσθέτουμε τα γράμματα μεταξύ τους.

M=	s	h	e	s	e	l	l	s	s	e	a	s	h	e	l	l	s	b	y	t	h	e	s	e	a	s	h	o	r	e

key=	k	e	y	k	e	y	k	e	y	k	e	y	k	e	y	k	e	y	k	e	y	k	e	y	k	e	y	k	e	y
C=	c	l	c	c	i	j	v	w	q	o	e	q	r	i	j	v	w	z	i	x	f	o	w	c	k	w	f	y	v	c

Η κρυπτογράφηση αυτή πήρε πολλά χρόνια για να σπάσει. Σημαντική βοήθεια είναι αν γνωρίζουμε το μήκος του κλειδιού. Παρατηρούμε ότι υπάρχει ένας συνδυασμός 4 γραμμάτων που επαναλαμβάνεται. Καταγράφουμε όλες αυτές τις ομοιότητες και προσπαθούμε να βρούμε συσχετίσεις μεταξύ των αποστάσεων αυτών των γραμμάτων για να βρούμε το μήκος του κλειδιού.

Vernam cipher – One Time Pad

Μια βελτίωση αυτής της μεθόδου έγινε το 1922 από το Vernam. Το μήκος του κλειδιού θα είναι ίσο με το μήκος του μηνύματος (**μεγάλο**) και **τυχαίο**. Αν το κλειδί πληροί αυτά τα χαρακτηριστικά, δεν θα σπάσει ποτέ. Το κλειδί αυτό λέγεται **one time pad**. Όμως στην πραγματικότητα ένα τέτοιο κλειδί δεν υπάρχει, μιας και δεν μπορούμε στην πραγματικότητα να εξασφαλίσουμε και τις δύο αυτές απαιτήσεις.