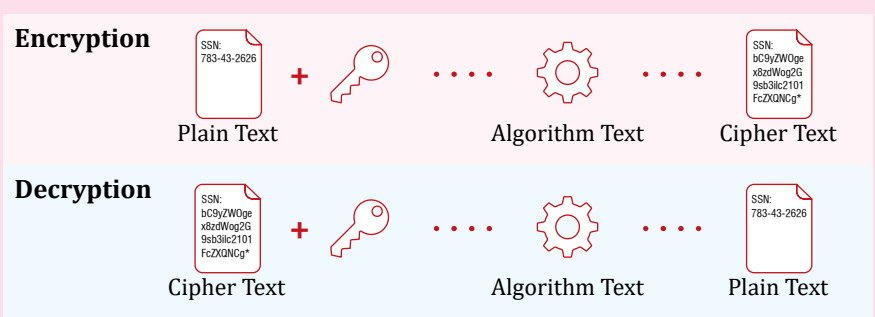
1.1 Αλγόριθμοι και εφαρμογές στην καθημερινότητα

Κρυπτογράφηση – Αποκρυπτογράφηση

Η **κρυπτογραφία** *(cryptography)* αποτελεί γνωστικό πεδίο των εφαρμοσμένων μαθηματικών και της πληροφορικής, που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Με την εκτεταμένη χρήση του Διαδικτύου και γενικότερα των επικοινωνιών δεδομένων *(data communications)* για τη φύλαξη και μετάδοση πλήθους πληροφοριών, είναι προφανής ο κίνδυνος, αυτές, να «πέσουν σε λάθος χέρια».

Ένας τρόπος περιορισμού, αν και όχι πλήρους αντιμετώπισης, αυτού του κινδύνου είναι η **κρυπτογράφηση** (encryption / cyphering) των δεδομένων, δηλαδή η μετατροπή τους σε μια μορφή που να μην είναι κατανοητή σε μη εξουσιοδοτημένα άτομα. Η αντίστροφη διαδικασία, δηλαδή η μετατροπή των κρυπτογραφημένων δεδομένων στην αρχική τους μορφή είναι γνωστή με τον όρο **αποκρυπτογράφηση** (decryption/decyphering).



Εικόνα 1: Κρυπτογράφηση – αποκρυπτογράφηση με τη χρήση ενός κοινού κλειδιού (συμμετρική)

Η κρυπτογράφηση είναι ιδιαίτερα σημαντική για τη διαφύλαξη του απορρήτου στα προσωπικά δεδομένα, στις τραπεζικές συναλλαγές και γενικότερα στις επικοινωνίες.
Όση προσπάθεια γίνεται για τη διαφύλαξη του απορρήτου των δεδομένων μέσω της κρυπτογράφησης, άλλη τόση γίνεται για την ανακάλυψη των αντίστοιχων αλγορίθμων και την αποκρυπτογράφηση των δεδομένων από μη εξουσιοδοτημένα άτομα. Στους αλγορίθμους αυτούς ο αποστολέας χρησιμοποιεί και ένα τουλάχιστον «κλειδί» για τη μετατροπή του αρχικού μηνύματος σε κρυπτογραφημένο μήνυμα (Εικόνα 1). Ωστόσο, διαρκώς αναπτύσσονται κι άλλοι αλγόριθμοι και τεχνικές κρυπτογράφησης που βελτιώνονται διαρκώς.

Τίτλος: **«Κρυπτογραφία»**

Έκδοση: **1.5**

Ημερομηνία: **10/09/2024**

Συντονιστής ομάδας σχεδιασμού και ανάπτυξης: **Κέλλυ Σαρρή Πασχαλίδη**

Δημιουργία: **ΕΚΔΟΣΕΙΣ ΕΛΛΗΝΙΚΗ ΓΡΑΦΗ**

Το παρόν αναπτύχθηκε στο πλαίσιο της Πράξης «Συγγραφή, Αξιολόγηση και Ένταξη διδακτικών βιβλίων στο Μητρώο Διδακτικών Βιβλίων και στην Ψηφιακή Βιβλιοθήκη Διδακτικών Βιβλίων» με κωδικό ΟΠΣ (MIS) 6010165, του Προγράμματος «Ανθρώπινο Δυναμικό και Κοινωνική Συνοχή 2021-2027» που υλοποιείται από το Ινστιτούτο Εκπαιδευτικής Πολιτικής και συγχρηματοδοτείται από το Ευρωπαϊκό Κοινωνικό Ταμείο.