Šifrovanie, kryptológia, kryptografia, kryptoanalýza, šifrovací/dešifrovací algoritmus, kľúč :)

Kódy veľmi často používajú vojaci, námorníci alebo policajti. Napr. kód 22 môže znamenať nepriateľ na dohľad, kód 75 – naháňam zlodeja a pod. Pokiaľ je účelom kódovania aj určité utajenie informácií, hovoríme o **šifrovaní**. Niekedy sa používa aj pojem kryptovanie a veda, zaoberajúca sa šiframi, je podľa toho **kryptológia**. Kryptológia pozostáva z **kryptografie**, ktorej cieľom je vytvoriť nerozlúštiteľnú šifru a **kryptoanalýzy**, ktorá ju má rozlúštiť.

Pokiaľ chceme údaje zašifrovať, potrebujeme na to minimálne **šifrovací/dešifrovací algoritmus** – postup, na základe ktorého sa pôvodná správa zmení na zašifrovanú (a naopak). Väčšina algoritmov vyžaduje na šifrovanie a dešifrovanie **kľúč**. Zatiaľ čo **algoritmus** je vec verejná, kľúč by mal byť známy len odosielateľovi, ktorý na základe neho správu zašifruje a prijímateľovi, ktorý zvyčajne na základe toho istého kľúča správu dešifruje.

Poznámka

Jedným z najjednoduchších spôsobov je zámena písmena za iné. Algoritmus spočíva v zamieňaní písmen, kľúčom je tabuľka so zodpovedajúcimi dvojicami.

Kódovanie, písmo ↑

História a princípy šifrovania. Scytale, Cézarova šifra, šifrovací disk, Vigenerova šifra, Cardanova šifra, Vernamova šifra, kľúč, substitučné a transpozičné šifry ↓

