Steganografia :)

UPOZORNENIE

Špeciálna kategória kryptografie – nespočíva ani tak v šifrovaní obsahu (i keď môže byť jej súčasťou) ako skôr v snahe o utajenie faktu, že komunikácia vôbec prebieha.



V minulosti sa na utajenie výmeny informácií používali rôzne neviditeľné atramenty, vyrývanie textu do drevených doštičiek, ktoré sa zaliali voskom a vyzerali ako nepopísané. Zaujímavou myšlienkou bolo tetovanie správy na hlavu kuriéra, ktorá sa potom nechala zarásť vlasmi. Počas 20. storočia bolo populárne skrývanie informácií do mikrobodiek, ktoré sa priliepali na miesta, kde mala byť v texte bodka alebo čiarka. Skryté údaje adresát dokázal prečítať až prostredníctvom silného mikroskopu.

Čakať v dnešnej dobe, kým niekomu narastú vlasy alebo príde štandardnou poštou list, je nepredstaviteľné, preto sa ako prostriedky steganografie využívajú najrozličnejšie digitálne prostriedky, ktoré sa navyše kombinujú s klasickým kryptovaním – ak bude správa zachytená neznamená to automaticky, že bude odhalený jej obsah.

Populárne je skrývanie správ do súborov s obrázkami, zvukom alebo videom. Pri obrázkoch sa využíva napr. posledný bit definujúci farbu bodu, ktorého zmena pri údajoch s 24-bitovou hĺbkou nespôsobí viditeľné zmeny. Zmenený súbor sa najčastejšie anonymne umiestni na anonymnú stránku, ku ktorej má adresát anonymný prístup spolu s miliónmi ďalších používateľov.

Súčasnosť šifrovania - symetrické a asymetrické šifry, DES, IDEA, RSA, PGP ↑

Copyright © 2013 - 2026 Encyklopédia poznania