Uvod

Kriptografija je nauka koja se bavi metodima očuvanja tajnosti informacija. Kada se lične, finansijske, vojne ili informacije državne bezbednosti prenose sa mesta na mesto, one postaju ranjive na prisluškivačke taktike. Ovakvi problemi se mogu izbeći kriptovanjem (šifrovanjem) informacija koje ih čini nedostupnim neželjenoj strani. Šifra i digitalni potpis su kriptografske tehnike koje se koriste da bi se implementirali bezbednosni servisi.

Osnovni element koji se koristi naziva se šifarski sistem ili algoritam šifrovanja. Svaki šifarski sistem obuhvata par transformacija podataka, koje se nazivaju šifrovanje i dešifrovanje. Šifrovanje je procedura koja transformiše originalnu informaciju (otvoreni tekst) u šifrovane podatke (šifrat). Obrnut proces, dešifrovanje, rekonstruiše otvoreni tekst na osnovu šifrata. Prilikom šifrovanja, pored otvorenog teksta, koristi se jedna nezavisna vrednost koja se naziva ključ šifrovanja. Slično, transformacija za dešifrovanje koristi ključ dešifrovanja. Broj simbola koji predstavljaju ključ (dužina ključa) zavisi od šifarskog sistema i predstavlja jedan od parametara sigurnosti tog sistema. Kriptoanaliza je nauka koja se bavi razbijanjem šifri, odnosno otkrivanjem sadržaja otvorenog teksta na osnovu šifrata, a bez poznavanja ključa. U širem smislu, kriptoanaliza obuhvata i proučavanje slabosti kriptografskih elemenata, kao što su, na primer, hash funkcije ili protokoli autentifikacije. Različite tehnike kriptoanalize nazivaju se napadi.

Istorijat kriptografije

Kada je pismo postalo sredstvo komunikacije, pojavila se potreba da se neka pisma sačuvaju od tuđih pogleda. Tada je i kriptografija ugledala svetlost dana. Od samog početka, enkripcija podataka koristila se prvenstveno u vojne svrhe. Jedan od prvih velikih vojskovođa koji je koristio šifrovane poruke bio je Julije Cezar. Naime, kada je Cezar slao poruke svojim vojskovođama, on je te poruke šifrovao tako što su sav ili pojedina slova u tekstu bila pomerana za tri, četri ili više mesta u abecedi. Takvu poruku mogli su da dešifruju samo oni koji su poznavali ovo pravilo. Poznata Cezarova izjava prilikom prelaska Rubikona u šifriranom dopisivanju glasila bi: fqkf ofhzf kyz. Pomicanjem svakog slova za šest mesta u abecedi lako se može pročitati pravi smisao poruke: Alea iacta est (kocka je bačena) .

Prvu poznatu raspravu o kriptografiji napisao na 25 stranica italijanski arhitekta Leone Batista Alberti 1467. godine. On je takođe tvorac takozvanog šifarskog kruga i nekih drugih rešenja dvostrukog prikrivanja teksta koja su u XIX veku prihvatili i usavršavali nemački, engleski i francuski šifrantski biroi. Pola veka nakon toga objavljeno je u pet svezaka delo Johanesa Trithemusa prva knjiga iz područja kriptografije. U 16. značajan doprinos daju milanski doktor Girolamo Kardano, matematičar Batisto Porta i francuski diplomata Blaise de Vigener.