Kriptografija

Teo Noel Bjelobrk OŠ Majstora Radovana, Trogir

6. razred prof. Ana Marija Saćer

Kriptografija

Znanstvena disciplina o metodama za slanje poruka (informacija) u obliku koji će biti razumljiv samo onima koji ih znaju pročitati, odnosno samo onima kojima su namijenjene. Riječ dolazi od grčkog pridjeva kriptós (κρυπτός) za skriven i glagola gráfo (γράφω) za pisati. Kriptografija je, uz kriptoanalizu koja razvija postupke za odgonetanje poruka bez poznavanja ključa, grana kriptologije.

Kako kriptografija radi?

Kriptografija omogućava dvjema osobama, pošiljatelju i primatelju, očuvanje tajnosti poruka čak i kada se one prenose nesigurnim vezama koje su dostupne trećim osobama. Kriptografija se stoljećima primjenjivala za osiguravanje tajnosti pretežito vojne i diplomatske komunikacije. Ispočetka su se postupci kriptiranja svodili na razmještanje (dislokaciju) znakova teksta ili na njihovu zamjenu (supstituciju). Danas je, u doba razmjene poruka globalnim komunikacijskim mrežama, kriptografija u širokoj uporabi. Ona se bavi podatcima u digitalnom obliku, a postupci kriptiranja i dekriptiranja matematičke su naravi i provode se uz pomoć računala. Suvremena je kriptologija tako informatička disciplina koja se oslanja na teoriju brojeva i druge matematičke teorije.

Steganografija

Steganografija je umjetnost i nauka o pisanju skrivenih poruka na takav način da niko, osim pošiljaoca i namjerenog primaoca, posumnja u postojanje poruke. Riječ steganografija je grčkog porijekla i znači "skriveno pisanje". Sastoji se od riječi steganos (στεγανός) što znači "pokriveno" ili "zaštićeno", i graphei (γραφή) što znači pisanje. Prva zabilježena upotreba pojma je iz 1499. godine sa strane Johannesa Trithemiusa u njegovom pismenom radu Steganographia u kojem opisuje kriptografiju i steganografiju. Prednost steganografije nad samom kriptografijom je da poruke ne privlače pažnju na sebe. Očito vidljive i šifrirane poruke - bez obzira koliko zaštićene - mogu probuditi pažnju drugih i sa tim u sebi biti inkriminirajući u zemljama gdje je enkripcija protivzakonita. Dakle, dok kriptografija štiti sadržaj poruke, za steganografiju se može reći da u nekom smislu može zaštiti poruku i komunikaciju preko koje se ona šalje.

Steganografija

Cezarova šifra

U kriptografiji, Cezarova šifra jedan je od najjednostavnijih i najrasprostranjenijih načina šifriranja. To je tip šifre zamjene (supstitucije), u kome se svako slovo otvorenog teksta zamjenjuje odgovarajućim slovom abecede, pomaknutim za određeni broj mjesta. Na primjer, s pomakom 3, A se zamjenjuje slovom D, B slovom E itd. Ova metoda je dobila ime po Juliju Cezaru, koji ju je koristio za razmjenu poruka sa svojim generalima. Cezarova šifra često se koristi kao korak u izradi složenijih načina šifriranja, kao što je