UVOD

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Sama riječ kriptografija je grčkog podrijetla i mogla bi se doslovno prevesti kao tajnopis.

*Zadaća je kriptografije da omogući dvjema osobama (pošiljatelj i primatelj) očuvanje tajnosti poruka, čak i u komunikaciji nesigurnim komunikacijskim*[*kanalom*](https://enciklopedija.hr/natuknica.aspx?ID=30148)*(računalna mreža, telefonska linija), koji je dostupan trećim osobama. Kriptografija se stoljećima primjenjivala za osiguravanje tajnosti pretežito vojne i diplomatske komunikacije.*

Grana znanosti koja obuhvaća kriptografiju, a i kriptoanalizu, naziva se kriptologija. Za razliku od dešifriranja, kriptoanaliza ili dekriptiranje je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa.

Matematička funkcija koja se koristi za šifriranje i dešifriranje naziva se Kriptografski algoritam ili šifra. Općenito, radi se o dvije funkcije, jednoj za šifriranje, a drugoj za dešifriranje. Te funkcije preslikavaju osnovne elemente otvorenog teksta (najčešće su to slova, bitovi, grupe slova ili bitova) u osnovne elemente šifrata, i obratno. Funkcije se biraju iz određene familije funkcija u ovisnosti o ključu. Skup svih mogućih vrijednosti ključeva nazivamo prostor ključeva.

ZAKLJUČAK

Danas, u doba razmjene poruka globalnim računalnim i komunikacijskim mrežama, kriptografija se široko primjenjuje: bilo da se želi osigurati privatnost poruka, ili se time nastoji zaštititi njihova tajnost, kao npr. pri slanju naloga u elektroničkom bankarstvu. U oba se slučaja kriptografija bavi podatcima u digitalnom obliku, postupci kriptiranja i dekriptiranja matematičke su naravi, a provode se automatski, uz pomoć računala. Zbog toga se suvremena kriptologija, kao interdisciplinarna znanost, uglavnom oslanja na informatiku, a znatno je potpomognuta [teorijom brojeva](https://enciklopedija.hr/natuknica.aspx?ID=60873) i dr. matematičkim teorijama.