Uvod
Istorijat kriptografije
Kada postoje informacije koje ne bi trebale da budu otkrivene od strane trećih lica, onda se pribegava metodi sakrivanja tih informacija. Veoma često, neke lične, vojne,finansijske ili informacije koje predstavljaju državne tajne, kada trebaju da se prenesu sa mesta na mesto, a trebaju da ostanu u tajnosti,dovodi se u pitanje sigurnost njihovog prenosa. Sadašnje društvo, u kome Internet kao svetska mreža predstavlja jedan, možda i najvažniji, izvor informacija, jako je podložno svakoj vrsti malverzacija. Elektronske transakcije, koje se danas obavljaju upravo putem računarskih mreža i Interneta kao takvog, zahtevaju zaštitu u što većoj meri.Jedna od metoda koja se u najvećoj meri koristi za zaštitu informacija, jeste kriptovanje ili šifrovanje.
Kriptografija ima dugu, zanimljivu, ali prilično tajnovitu prošlost. Još u vreme starih Egipćana, pre nekih 4000 godina, počela je da se upotrebljava.Zapravo, u tom periodu su urezivani razni hijeroglifi u spomenicima Starog carstva. To je bilo više iz znatiželje, jer je bilo jako malo pismenih, tako da ideja sakrivanja pravog značenja tih poruka najverovatnije nije postojala.Kasnije, kada se pojavilo pismo kao sredstvo komunikacije, bilo je potrebno da se neka od tih pisama sačuvaju od tuđih pogleda. Tada je kriptografija ugledala svetlost dana.
Međutim, od samog početka, enkripcija podataka koristila se u vojne svrhe.Učeni Jevreji su između 500. i 600. godine pre nove ere zamenjivali neka slova brojevima, kako bi sakrili određenu poruku od zavojevača.
Tako, na primer, broj 666 predstavlja najčuveniju šifru - „znak zveri“ - iz knjige Otkrovenja u hrišćanskom Novom zavetu. Ona je ukazivala na progon pred rimskim osvajačima, a pretpostavlja se da se odnosila na cara Nerona, od koga je „vrebala“ opasnost.
Neki elementi kriptografije su bili prisutni i kod starih Grka. Naime, Spartanci su u 5. veku pre nove ere upotrebljavali spravu za šifrovanje zvanu skital. To je bio drveni štap oko kojeg se namotavala vrpca od pergamenta, pa se na nju nanosila poruka. Nakon upisivanja poruke, vrpca bi se odmotala, a na njoj bi ostali izmešani znakovi koje je mogao da pročita samo onaj ko je imao štap iste debljine.
Herodot još spominje javke na tablama, prekrivene voskom, i pisanje na glavama robova (prvo tetoviranje) koje bi kasnije prekrila kosa.
I Rimljani su koristili kriptografiju. Jedan od velikih vojskovođa, Julije Cezar,koristio je šifrovane poruke kada je išao u osvajanja. Zapravo, kada je Cezar slao svoje poruke vojskovođama, on ih je šifrovao na taj način što su sva ili pojedina slova u reči bila pomerena za tri, četiri ili više mesta u abecedi. Samo ko je poznavao pravilo ”pomeri za” mogao je da pročita pravu poruku. Tako, kada je prešao Rubikon, on je rekao: Alea iacta est (kocka je bačena), a to bi u šifrovanom dopisivanju izgledalo: fqkf ofhzf kyz.Ključ je predstavljao pomeranje slova u abecedi za šest mesta.