Kriptografija i njena praktična primena

Vrsta: Seminarski | Broj strana: 11 | Nivo: Visoka škola za računovodstvo i berzansko poslovanje, Beograd

Uvodna reč

Kriptografija (kriptologija) je izvedenica iz grčkog pridjeva κρυπτός kriptós „skriven“ i glagola γράφω gráfo „pisati“. Kriptografija je moderna nauka bazirana na primenjenoj matematici. Ključ kao pojam vezan uz kriptografiju predstavlja podatak koji omogućava šifriranje i/ili dešifriranje. Ključ predstavlja jedan ili više podataka koji uz poznati algoritam vode do početnih podataka i obratno.

Kroz celu istoriju čovečanstva postojala je potreba za sigurnom razmenom informacija. Problemom sigurne komunikacije bavili su se već Egipćani i Indijci pre više od 3000 godina i od tada do danas osnovna ideja se nije promijenila – preneti neku poruku s jednog mesta na drugo što je sigurnije moguće, tj. napraviti algoritam koji bi omogućio skrivanje originalne poruke tako da bude potpuno nerazumljiva osobama koje bi neovlašteno došle u njen posed. Prve korištene metode nisu bili složeni matematički algoritmi nego se počelo korišćenjem alternativnih jezika koji su bili poznati samo malom broju ljudi. Razvoj složenijih metoda sigurne komunikacije počeo je tek razvojem pisma, što je omogućilo da se bilo koja informacija prikaže određenim brojem znakova koji bi, nakon upotrebe određenog ključa, formirali ponovno početnu poruku. S vremenom se javila i ideja prikaza slova drugim simbolima. Primeri koji su i danas u upotrebi su: Morseov kod, Braille-ovo pismo i ASCII kod.

Moderna civilizacija duguje mnogo staroj istočnjačkoj. Iz Vavilonske kulture su prenete priče o stvaranju sveta i potopu i mnogi naučni principi, kao podela kruga na 360 stepeni i dana na 24 sata. Utvrđeno je da ploča iz Mesopotamije sadrži kodiranu formulu za pravljenje posebnog premaza za lončariju.

Slika 01

Glinena ploča poreklom iz Mesopotamije

Nikad nije tačno utvrđen početak kriptografije, ali se smatra da je počela više od 2000 godina p. n. e i iz tog vremena potiču prvi pronađeni tragovi šifriranja. Tačnije, oko 1900. godine p. n. e. u Egiptu nastao je natpis koji se danas smatra prvim dokumentiranim primerom pisane kriptografije. U 6. veku p. n. e. u zapisu iz Biblije, Knjige o Jeremiji, korišćena jednostavna šifra koja izvrće abecedu naopako. Šifra je poznata pod imenom ATBASH, a bila je jedna od hebrejskih šifri koje su u to vrijeme korišćene.

Oko 487. godine pre nove ere Grci su upotrebljavali napravu zvanu nebeski štap oko kojeg je bio zamotan dugačak, uzan komad kože na koji se pisalo. Koža se zatim skidala i nosila kao pojas. Verovatno je lice koje prima takav pojas imao odgovarajući štap a ispisani skup bi ostavio kod kuće (predpostavlja se da bi upotreba nebeskog štapa mogla biti mit).