FAKULTET ZA POSLOVNU INFORMATIKU

Seminarski rad iz Zaštite računarskih sistema

Tema: ENIGMA

Beograd, 10.01.2007. godine

UVOD

Sve više i više ljudi širom sveta koristi Internet za prenos podataka. Mnogi od njih čak prenose i lične podatke, kao i matične brojeve i brojeve računa u banci. Ovo zahteva da korisnik bude povezan bezbednom konekcijom. Bezbedna konekcija predstavlja mehanizam da podatke šalje u enkriptovanom obliku, kako drugi ne bi mogli da ih pročitaju. Takođe je ovde bitno da primaoci tih podataka mogu da pročitaju poruke u obliku u kom su poslate. Kripcija ili kodiranje podataka nije nov pojam, već datira još iz starih vremena.

„Istorija je preplavljena kodovima. Oni su odlučivali o pobednicima u bitkama i vodili u smrt kraljeve i kraljice” Simon Singh

OSNOVNI POJMOVI

Reč **kriptografija** potiče od grčke reči *kryptos* što znači skriveno, i reči *graf* što znači pisati, tako da u prevedenom značenju kriptografija predstavlja učenje o skrivenim pisanim informacijama koje su kodiirane ili šifrovane. **Kod** je zamena reči ili fraze sa rečju, brojem ili simbolom, dok **šifra** predstavlja zamenu slovo-za-slovo. Mnogi moderni kriptografski algoritmi koriste spoj kodiranja i šifrovanja. **Kriptologija** je uopštena nauka o kodovima i šiframa, dok je **kriptoanaliza** nauka o dešifrovanju kodova i šifara.

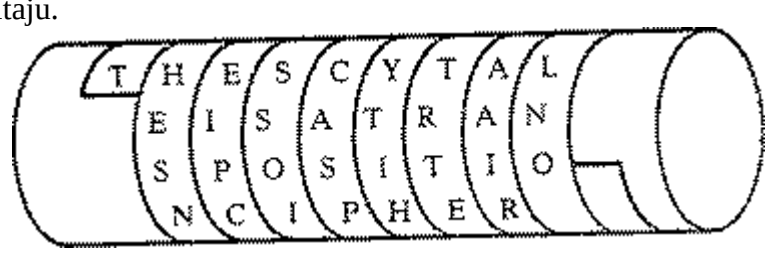
KRIPTOGRAFIJA KROZ ISTORIJU

Enkrpicija, tj skriveno značenje poruke, počelo je da se koristi u Egiptu oko 1900. godine p.n.e.. U zapisima o Faraonu Amenemhetu II korištene su hijeroglifske zamene kako bi saopštili dostojanstvo i autoritet u odnosu na ostale natpise u piramidi.

U periodu između 1500.g.p.n.e - 500 g.p.n.e. Asirci i drugi narodi (Mesopotamci, Indijci, Kinezi i Egipćani) počinju skrivati informacije koristeći raznolike metode: tetovirajući poruke na glavi kurira, urezivanjem poruke u utrobi mrtvih životinja itd. To su bili počeci **stenografije** (skrivanja poruke).

Oko 600.g.p.n.e. Jevreji počinju se služiti prvim prostim šifarskim sistemom poznatim pod imenom ATBASH. ATBASH koristi reverzni alfabet, tako da recimo četvrto slovo postaje četvrto slovo sa kraja alfabeta. Tako je napisana knjiga o Jeremiji.

Prvi šifarski uređaj pod nazivom "SCYTALE" napravljen je i korišten u Sparti oko 500.g.p.n.e. Uređaj se sastojao od parčeta drveta određene debljine, oko koga bi se čvrsto obmotalo parče papirusa, kože ili pergamenta. Poruka bi bila ispisana po dužini pergamenta u kolonama reči, pergament bi se zatim odmotao i dobio bi se skup nepovezanih slova. Tajna dešifrovanja bila je u debljini uređaja. Samo sa određenom debljinom dobijala bi se smislena poruka. Ipak ukoliko bi neprijatelji presreli poruku, sa odgovarajućom debljinom uređaja mogli bi i da je pročitaju.



Slika 1. SCYTALE