**OSNOVNE METODE KRIPTOLOŠKE ZAŠTITE**

Mateja Dimić 4/6

**UVOD:**

Kroz istoriju postojala je potreba da se omogući komunikacija izmedju 2 ili više strana, ali i da se zadrži privatnost prenošenih informacija, naročito u slučaju kada postoji prisluškivanje komunikacionog kanala.

Sa tom potrebom nastala je kriptografija.

Čak iako je glavni cilj ostao obezbedjivanje privatnosti, polje kriptografije se proširilo na mnoge druge oblasti, ne samo u okviru bezbednosti komunikacija, kao što su integritet i autentičnost komunikacija, već i na mnoge druge ciljeve.

Danas je primena kriptografije široko rasprostranjena, iako je nekada bila primenjena samo u vojnim okvirima.

Na primer, pri kupovini preko interneta, koristi se kriptografija da bi se osigurala privatnost informacije sa kartice dok se prenosi od korisnika do servera prodavnice. U elektronskom bankarstvu kriptografija se koristi da bi bio obezbedjen pristup ličnim podatcima i transakcijama.

Danas je kriptologija temelj računarske i komunikacione tehnologije.

Zasniva se na strogim matematičkim principima i spaja oblasti kao što su teorija brojeva, teorija računarske kompleksnosti i teorija verovatnoće.

**CILJEVI KRIPTOLOGIJE:**

Moderna kriptologija se koristi za rešavanje velikog broja problema. Najvažniji od svih tih problema je i dalje ostvarivanje bezbedne komunikacije preko nesigurnih komunikacionih kanala. Da bih lakše predstavio taj problem, definisaću određene pojmove:

**Pošiljalac**, i **primalac** koji žele da uspostave komunikaciju medju sobom. U kriptologiji se uvek razmatra i treća strana, a to je protivnik, i on predstavlja izvor pretnji. Koristiću ga kao primer osobe koja ima pristup komunikacionom kanalu i želi da kompromituje bezbednost informacija strana koje komuniciraju.

Međutim, to ne znači da su pošiljalac i primalac samo ljudska bića, već oni mogu biti i nešto drugo kao na primer: mobilni telefon, računar, ili neki računarski proces.



**KOMUNIKACIONI  
KANAL**

Pošiljalac Primalac



Protivnik

Svi aspekti idealnog kanala se ne mogu dostići, tako da kriptolozi imaju još neke ciljeve kojima konstantno žele da se približe. Prva cilj je privatnost. Obezbediti privatnost znači sakriti sadržaj komunikacije od protivnika. Drugi cilj je autentičnost i integritet.