Uvod
Ljudi sve više koriste Internet za kupovinu, poslovanje, rad, komunikaciju itd. Elektronsko poslovanje zahteva razmenu poverljivih i osetljivih podataka kao što su brojevi kreditnih kartica, poslovne tajne i planovi. Da bi se omogućio ovaj vid komunikacije razvijene su mnogobrojne sigurnosne tehnike i načini za zaštitu podataka i informacija. Kombinujući razne tehnike dolazi se do visokog nivoa sigurnosti koji obezbeđuje 4 osnovna načela u sigunosnoj komunikaciji:
da podaci nisu promenjeni na bilo koji način - integritet
da podaci nisu presretani i čitani od strane bilo kog - privatnost
imaju dokaz da je pošiljaoc inicirao transakciju - neodricljivost
Integritet i privatnost su postignuti enkripcijom podataka dok autentifikacija i neodricljivost zahtevaju razmenu enkriptovanih poruka između dve strane.
Enkripcija podataka
Znanje o računaraima i mrežama danas je sve više dostupno ljudima. Postoji veliki broj načina i tehnika za dolaženje do poverljivih informacija koje mogu biti eksploatisane na štetu korisnika. Ljudska komunikacija i poslovanje jesu olakšani ali sa sobom nose rizike koji se povećavaju svakodnevno. Uzmimo za primer bankarsku transakciju. Da bi se obavila potrebna je razmena poverljivih podataka koji se mogu zlonamerno iskoristit ukoliko se ne primenjuju sigurnosne mere. Napadač može korititi razne tehnike za dolaženje do istih. Zatim pomoću raznih metoda može ukloniti protokolno kontrolnu informaciju na početku svake poruke koja mu zatim ostavlja sadržaj poruke. Ovaj vid presretanja podataka se naziva prisluškivanje. Kada je došao do željenog sadržaja napadač prelazi na maskiranje poruke kao da je poslata od njegove strane da bi došao do željene svote novca. Zbog toga je enkripcija poželjna na svim nivoima koji uključuj bilo koji vid mreža.
Enkripcija zahteva da strana koja salje podatke obrati pažnju i enkriptuje sve potadke koji se šalju da ukoliko se desi slučajno ili namerno presretanje ti podaci budu neupotrebljivi. Naravno, treba voditi računa da se ti podaci kasnije mogu i dekriptovati kada stignu do željenog primaoca. Da bi ovakva razmena podataka bila moguća koriste se enkripcioni ključevi koji bi trebalo da su poznati samo stranama koje vrše razmenu. Ključ se upotrebljava kod enkripcije i dekripcije. Običan tekst nakon enkripcije postaje šifrovan. Cilj enkripcije je da ukoliko dođe do presretanja napadač ne može u realnom vremenskom periodu izvršiti dekriptovanje. Zbog toga se obraća pažnja koji će metod biti korišćen. Što je podatak bolje enkriptovan to je manja verovatnoća da će ,čak i uz upotrebu veoma snažnih računara, biti otkriven sadržaj.