SADRŽAJ

2
1. Uvod
Sigurnost računarskih sistema postaje sve važnija, jer sve više korisnika na sve više načina koristi sve više informacija u računarskom svetu. U takvom sistemu postoji i sve veća opasnost od neovlaćene upotrebe informacija, podmetanja lažnih informacija ili uništavanja informacija. U računarskim sistemima informacije se prenose raznovrsnim otvorenim i nesigurnim komunikacijskim putevima. Pristup do tih puteva ne može se fizički zaštititi pa svaki neprijateljski nastrojen napadač može narušiti sigurnost sistema. Zbog toga zaštitni komunikacijski mehanizmi nad nesigurnim komunikacijskim kanalom postaju najvažniji oblik ostvarenja sigurnosti. Pokazuje se da je najdelotvornija zaštita poruka njihovo kriptiranje.
U ovom radu ću pobliže objasniti osnovne pojmove vezane za kriptovanje i algoritme koji su se koristili i koji se koriste kako bi se zaštitila privatnost unutar mreže računara.
3
2. Osnovni termini
Kriptografija je nauka "tajnog pisanja", tj. nauka čuvanja informacija u onoj formi koja