PANEVROPSKI UNIVERZITET APEIRON FAKULTET POSLOVNE INFORMATIKE Vanredne studije Smjer »Poslovna informatika«

Predmet: PRINCIPI PROGRAMIRANJA

Tema:

»Kriptografija« »simetrični i asimetrični algoritmi«

Banja Luka, maj, 2008

1. Uvod

Sigurnost računarskih sistema postaje sve važnija, jer sve više korisnika na sve više načina koristi sve više informacija u računarskom svijetu. U takvom sistemu postoji i sve veća opasnost od neovlaštene upotrebe informacija, podmetanja krivih 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 najdjelotvornija 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.

2.Osnovni termini

Kriptografija je nauka "tajnog pisanja", tj. nauka čuvanja informacija u onoj formi koja će biti čitljiva samo onima kojima je informacija namijenjena dok će za ostale biti neupotrebljiva. Usporedo sa razvojem kriptografije razvila se i nauka kojoj je cilj analizom kriptirane poruke odgonetnuti njen sadržaj. Ta nauka se naziva kriptoanaliza. Pored gore navedenog, valja spomenuti jednu bitnu razliku između termina kriptografija i termina kriptologija. Kriptografija je nauka koja se bavi svim aspektima sigurnosnog transporta podataka kao što su na primjer autentifikacija (web, lokalne mreže i sl.), digitalni potpisi, razmjena elektroničkog novca. Kriptologija, je za razliku grana matematike koja se bavi matematičkim načelima, te matematičkom implementacijom kriptografskih metoda. Originalna poruka koju je pošiljaoc će slati u daljnjem razmatranju će se zvati čisti tekst ili original. Zatim, kodiranje poruke tj. postupak pretvaranja originala (čistog teksta) u nečitljiv oblik ćemo nazvati enkripcija. Tako enkriptiran tekst ima engleski termin ciphertext, a mi ćemo je jednostavno nazvati kodiranom porukom. Nadalje, postupak dekodiranja poruke, tj. vraćanja poruke iz njenog enkriptiranog

oblika u originalni (čisti tekst) oblik naziva se dekripcija. Vrlo važan termin u kriptografiji je ključ. Ključ ima veliku ulogu u enkripciji i dekripciji poruke.

3. Osnovni kriptografski algoritmi