

SADRŽAJ

1.Uvod	3
2.Osnovni termini	8
3.Osnovni kriptografski algoritmi	12
4.Simetrična kriptografija	14
4.1 Simetrični algoritmi	16
4.2 Lucifer	17
4.3 DES	18
4.4 Probijanje DES-a	18
4.5 Triple DES 2 Key DES	21
4.6 AES	22
5. Asimetrična kriptografija	2
5.1 Digitalni potpis	
5.2 Digitalni sertifikat	
6.Asimetrični algoritmi	
6.1 RSA algoritam	
6.2 PGP algoritam	
6.3 Zašto PGP korist hibridnu enkripciju	
7. Kriptoanaliza	
7.1 Osnovna pravila zaštite	
8.Zaključak	
9.Literatura	

3

8

12

14

16

17

18

18

21

22

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 neovlašćene 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 nastojanje napadača 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

**----- OSTATAK TEKSTA NIJE PRIKAZAN. CEO RAD MOŽETE
PREUZETI NA SAJTU. -----**

www.maturskiradovi.net

MOŽETE NAS KONTAKTIRATI NA E-MAIL: maturskiradovi.net@gmail.com