

SEMINARSKI RAD

**PANEVROPSKI UNIVERZITET APEIRON
FAKULTET POSLOVNE INFORMATIKE**

**Vanredne studije
Smjer »Poslovna informatika«**

Predmet: PRINCIPI PROGRAMIRANJA

Tema:

**»Kriptografija«
»simetrični i asimetrični algoritmi«**

**Predmetni nastavnik
Prof. dr Zoran Ž. Avramović, dipl.inž.elek.**

**Student
Dražen Petrović, vandredni student 2. godine
Index br:0097/06**

Banja Luka, maj, 2008

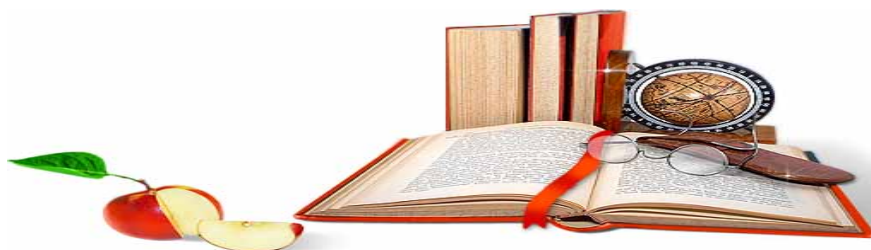
KRATKI SADRŽAJ

1.Uvod	3
2.Osnovni termini	4
3.Osnovni kriptografski algoritmi	4
4.Simetrična kriptografija	5
4.1 Simetrični algoritmi	7
4.1.1 Lucifer	7
4.1.2 DES	8
4.1.2.1 Probijanje DES-a	10
4.1.2.3 Triple DES 2 Key DES	12
4.1.3 AES	12
5. Asimetrična kriptografija	13
5.1 Digitalni potpis	14
5.2 Digitalni sertifikat	16
6.Asimetrični algoritmi	17
6.1 RSA algoritam	17
6.2 PGP algoritam	18
6.2.1 Zašto PGP korist hibridnu enkripciju	18
7. Kriptoanaliza	18
7.1 Osnovna pravila zaštite	20
8.Zaključak	21
9.Literatura	22

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

**BESPLATNI GOTOVI SEMINARSKI, DIPLOMSKI I MATURSKI TEKST
RAZMENA LINKOVA - RAZMENA RADOVA
RADOVI IZ SVIH OBLASTI, POWERPOINT PREZENTACIJE I DRUGI EDUKATIVNI MATERIJALI.**

**WWW.SEMINARSKIRAD.ORG
WWW.MAGISTARSKI.COM
WWW.MATURSKIRADOVI.NET**



NA NAŠIM SAJTOVIMA MOŽETE PRONAĆI SVE, BILO DA JE TO **SEMINARSKI, DIPLOMSKI** ILI **MATURSKI** RAD, POWERPOINT PREZENTACIJA I DRUGI EDUKATIVNI MATERIJAL. ZA RAZLIKU OD OSTALIH MI VAM PRUŽAMO DA POGLEDATE SVAKI RAD, NJEGOV SADRŽAJ I PRVE TRI STRANE TAKO DA MOŽETE TAČNO DA ODABERETE ONO ŠTO VAM U POTPUNOSTI ODGOVARA. U BAZI SE NALAZE **GOTOVI SEMINARSKI, DIPLOMSKI I MATURSKI RADOVI** KOJE MOŽETE SKINUTI I UZ NJIHOVU POMOĆ NAPRAVITI JEDINSTVEN I UNIKATAN RAD. AKO U **BAZI** NE NAĐETE RAD KOJI VAM JE POTREBAN, U SVAKOM MOMENTU MOŽETE NARUČITI DA VAM SE IZRADI NOVI, UNIKATAN SEMINARSKI ILI NEKI DRUGI RAD RAD NA LINKU **IZRADA RADOVA**. PITANJA I ODGOVORE MOŽETE DOBITI NA NAŠEM **FORUMU** ILI NA

maturskiradovi.net@gmail.com