

**VISOKA TEHNIČKA ŠKOLA STRUKOVNIH STUDIJA  
ODSEK INFORMATIKA  
KRAGUJEVAC**

**DIPLOMSKI RAD**

Predmet: Bezbednost informacionih sistema

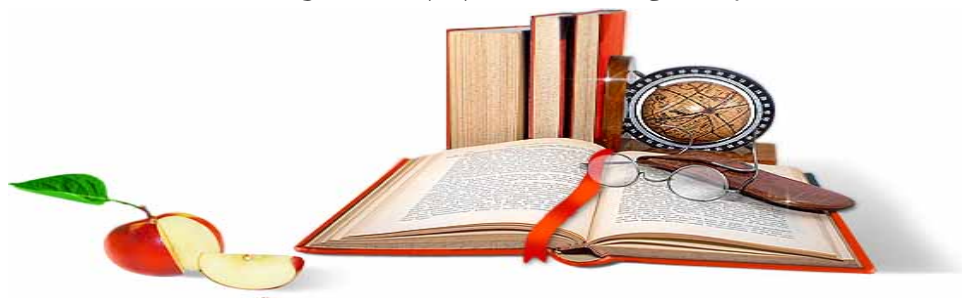
**DES**  
**(Data Encryption Standard)**

Kragujevac, 2011.

## S A D R Ź A J

1.	UVOD .....	3
2.	ISTORIJA RAZVOJA DES STANDARDIZACIJE .....	4
3.	DES ALGORITAM – KARAKTERISTIKE .....	5
4.	OPIS RADA DES ALGORITMA .....	6
	4.1 Osnovne etape DES algoritma .....	6
	4.2 Odredjivanje funkcije enkripcije $f$ .....	7
	4.3 Odredjivanje tablice ključeva .....	8
	4.4 Postupak dešifriranja .....	9
5.	SVOJSTVA DES ALGORITMA .....	10
6.	NAČINI KORIŠĆENJA DES-a .....	12
	6.1 ECB mod .....	12
	6.2 CBC mod .....	12
	6.3 CFB mod .....	13
	6.4 OFB mod .....	14
	6.5 CTR mod .....	14
7.	SIGURNOST I KRIPTOANALIZA .....	16
	7.1 Brute force attack – napad grubom silom .....	17
	7.2 Diferencijalna analiza .....	18
	7.3 Linearna kriptanaliza .....	18
8.	PRIMENA DES ALGORITMA .....	19
9.	MANE DES-a .....	22
10.	NADGRADNJA DES-a .....	23
	9.1 AES - <i>Advanced Encryption Standard</i> .....	23
	9.2 Triple DES .....	23
11.	ZAKLJUČAK .....	24
	<i>Literatura</i> .....	25

**GOTOVI SEMINARSKI, DIPLOMSKI I MATURSKI TEKST**  
**RADOVI IZ SVIH OBLASTI, POWERPOINT PREZENTACIJE I DRUGI**  
**EDUKATIVNI MATERIJALI.**



**[WWW.SEMINARSKIRAD.ORG](http://WWW.SEMINARSKIRAD.ORG)**  
**[WWW.MAGISTARSKI.COM](http://WWW.MAGISTARSKI.COM)**  
**[WWW.MATURSKIRADOVI.NET](http://WWW.MATURSKIRADOVI.NET)**  
**[WWW.MATURSKI.NET](http://WWW.MATURSKI.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](mailto:MATURSKIRADOVI.NET@GMAIL.COM)**