

## SADRŽAJ

1.	Uvod.....	3
2.	Kriptografija.....	4
3.	Simetrični algoritmi.....	8
3.1.	DES algoritam .....	9
3.2.	AES algoritam .....	10
3.3.	Drugi algoritmi .....	11
3.3.1.	IDEA .....	12
3.3.2.	RC4.....	13
3.3.3.	Blowfish .....	13
3.3.4.	Twofish.....	14
3.3.5.	TEA .....	14
4.	Asimetrični algoritmi .....	16
4.1.	RSA algoritam .....	17
4.1.1.	Digitalni potpis i RSA šema digitalnog potpisa .....	19
4.1.2.	Digitalna koverta (envelop).....	21
4.2.	DSA algoritam.....	22
4.2.1.	Primjer slanja poruke kroz DSA .....	23
4.3.	Kriptografija eliptične krive ECDSA .....	25
4.4.	Diffie – Hellmanov algoritam.....	26
5.	Hash funkcije.....	28
5.1.	MD5.....	29
5.2.	SHA algoritmi.....	30
5.2.1.	SHA – 1 .....	30
5.2.2.	SHA – 2.....	31
5.2.3.	SHA – 3.....	32
5.3.	Primjena hash funkcija .....	33
5.3.1.	HMAC.....	34
6.	PKI sistem .....	36
6.1.	Digitalni sertifikat.....	37
7.	Autentifikacija.....	40
7.1.	Komponente autentifikacije.....	40
7.1.1.	Faktori znanja .....	41
7.1.2.	Faktori posjedovanja .....	41
7.1.3.	Inherentni faktori.....	41

7.1.4. Faktori zasnovani na lokaciji.....	41
7.2. Primjena autentifikacije .....	42
8. Protokoli zaštite na različitim nivoima OSI modela .....	43
8.1. Protokoli zaštite u mrežnom sloju .....	43
8.1.1. VPN protokoli .....	44
8.1.2. IP Security (IPSec) .....	46
8.2. Protokoli u transportnom sloju .....	48
8.2.1. SSL/TSL protokol .....	48
8.2.2. SSH protokol.....	51
8.3. Protokoli u aplikativnom sloju .....	52
8.3.1. PGP protokol.....	52
9. Wireless komunikacija .....	54
9.1. Wi – Fi.....	54
9.2. Sistemi za mobilnu komunikaciju .....	55
9.3. Bluetooth .....	56
10. Šifrovanje na hardverskom nivou .....	58
10.1. Open source rješenja .....	58
11. Kvantna kriptografija i trendovi u kriptografiji.....	60
12. Kriptovalute.....	62
12.1. Blockchain i Bitcoin .....	62
13. Zaključak.....	65
14. Literatura .....	66