

SADRŽAJ:

1 UVOD	6
1.1.Kriptografija.....	6
1.2.Elektronski potpis	8
1.3.Svrha i ciljevi istraživanja	9
1.4.Struktura rada.....	9
2 DIGITALNI POTPIS	10
2.1.Simetrična kriptografija	11
2.2.Asimetrična kriptografija.....	13
2.3.PKI-Infrastruktura javnog ključa.....	15
2.4.SSL protokol	17
2.4.1.SSL protokol rukovanja.....	18
2.4.2.Serverska autentifikacija.....	19
2.4.2.Čovjek u sredini napad	21
2.4.3.Klijentska autentifikacija.....	21
3 PRETPOSTAVKE KRIPTOGRAFSKE TVRDOĆE	23
3.1.Jednosmjerne funkcije i permutacije	24
3.2.Trapdoor penetracija	24
3.3. Permutacije bez kandži (zamka).....	24
3.4. Tvrdoća faktoringa.....	25
3.5. Hash funkcije	25
4 DIGITALNI SERTIFIKAT	25
4.1.Tipovi digitalnih sertifikata	27
4.1.1.Potvrde o indentitetu.....	27
4.1.2.Cerifikati o akreditaciji.....	27
4.1.3.Potvrde o ovlaštenjima i dozvolama.....	28
5 ŠEME POTPISA ZASNOVANE NA RSA PRETPOSTAVKAMA	29
6 REALIZACIJA ELEKTRONSKOG POTPISA	32
6.1.Upotreba digitalnih potpisa i sertifikata	32
6.1.2.PGP (Pretty Good Privacy).....	32
6.1.3.Web stranice i ssl sertifikati.....	33

5.1.4.Windows Server Active Directory Certificate Services (AD CS)	34
7 SMART KARTICE	36
7.2.Tipovi smart kartica	38
7.2.1.Memorijske kartice	38
7.2.2.Mikroprocesorske kartice	38
7.2.3.Beskontakne pametne kartice	39
8 DIGITALNI POTPIS U BIH I SRBIJI.....	40
9 ZAKLJUČAK.....	43
10 LITERATURA	44