

## SADRŽAJ

1	UVOD.....	1
2	TEORIJSKO-METODOLOŠKA OSNOVA RADA.....	4
2.1	Predmet i problem istraživanja.....	4
2.2	Cilj i značaj istraživanja.....	4
2.3	Hipoteze.....	5
3	KRIPTOGRAFIJA.....	7
3.1	Istorija kriptografije.....	8
3.1.1	Osnove kriptografije.....	12
4	ZNAČAJ I ULOGA AUTENTIFIKACIJE U KOMUNIKACIJI.....	17
4.1	Šta je to autentifikacija?.....	18
4.2	Metode autentifikacije.....	19
4.3	Autentifikacione razmjene.....	22
4.4	Protokol potvrde vjerodostojnosti.....	23
4.4.1	Protokoli zasnovani na simetričnim kriptosistemima.....	24
4.4.2	DES (Data Encryption Standard).....	26
4.4.3	AES (Advanced Encryption Standard).....	28
4.4.4	Protokoli zasnovani na asimetričnoj kriptografiji.....	28
4.4.5	RSA (Rives-Shamir-Adleman).....	31

5	Elektronski i digitalni potpis .....	34
5.1	Elektronski potpis.....	34
5.2	Digitalni potpis.....	35
5.3	HASH ALGORITMI.....	37
5.4	Značajnije hash funkcije.....	38
5.4.1	MD5 .....	38
5.4.2	SHA algoritam.....	42
6	Sertifikacioni autoriteti.....	47
6.1	Ko odlučuje da li se sertifikacionom autoritetu može vjerovati?.....	48
6.2	Infrastruktura javnog ključa (PKI) .....	48
6.3	PKI i hijerarhija povjerenja .....	49
6.4	Kako pokrenuti sertifikacioni autoritet?.....	50
6.5	Nedostaci infrastrukture javnog ključa .....	50
6.6	Uticaj organa vlasti na mogućnost lažiranja SSL sertifikata.....	51
6.7	SSH (Secure Shell).....	53
7	WEB OF TRUST .....	54
7.1	PGP (Pretty Good Privacy) .....	54
7.2	Open PGP.....	56
7.2.1	Kritike OpenPGP-a .....	57

7.2.2	Savremeni komunikacioni protokoli .....	58
7.3	GnuPG.....	59
7.3.1	Istorijat .....	60
7.3.2	Podaci u mirovanju.....	61
7.3.3	Obrada poruka bez međuspremnik.....	62
7.3.4	OpenPGP poruke.....	63
7.3.5	Šifrovanje .....	64
7.3.6	Potpisivanje .....	66
7.3.7	Ključevi .....	72
7.3.8	Potpisivanje ključeva.....	82
7.3.9	Provjera valjanosti drugih ključeva na javnom ključu .....	84
8	Algebra za ocjenu povjerenja u sertifikacionim lancima .....	87
8.1	Model povjerenja.....	88
8.2	Subjektivna logika.....	91
8.2.1	Problem zavisnosti .....	94
8.3	Autentifikacija i sertifikacija u otvorenim mrežama.....	95
8.3.1	Sertifikaciona algebra.....	95
8.3.2	Dokazi iz prve i druge ruke .....	102
8.3.3	Navigacija zasnovana na povjerenju u otvorenim mrežama.....	103

8.3.4	Poređenje sa PGP-om.....	106
8.3.5	Skrivene zavisnosti u vrijednostima PGP pouzdanosti.....	107
9	Blockchain tehnologija.....	111
9.1	Struktura podataka.....	111
9.2	Pouzdana distribuisane baze zasnovane na blok lancima .....	113
9.3	Autentifikacija i povjerenje .....	114
9.4	Framework .....	115
9.4.1	Model mrežnih usluga.....	115
9.5	Blockchain autentifikacija i modul povjerenja.....	116
9.6	BATM autentifikacija .....	117
9.6.1	Rudarenje blokova.....	117
9.6.2	BATM podaci koji se prenose.....	119
9.7	BATM trust management.....	120
9.7.1	Knowledge based trust for BATM.....	121
9.7.2	Trust evaluation.....	122
9.8	Pravila podataka BATM modula.....	124
9.9	Problem izvornog bloka .....	126
9.10	Dalji razvoj.....	127
9.11	Primjena .....	127

10	ISTRAŽIVANJE .....	128
10.1	Rezultati istraživanja.....	129
10.2	Analiza i zaključci.....	141
11	Izgradnja sopstvene mreže povjerenja.....	142
12	Eksperiment .....	145
12.1	Analiza .....	157
12.2	Kako šifrovati email na androidu.....	157
12.3	KAKO KREIRATI SAVRŠEN GPG PAR KLJUČEVA NA LAPTOPU .....	160
12.3.1	Podključevi pomažu u zaštiti vašeg identiteta u slučaju krađe privatnog ključa (laptopa) 160	
13	TOFU za OpenPGP .....	162
13.1	Pozadina .....	164
13.2	Arhitektura .....	165
13.2.1	Prava mjera korisničke interakcije .....	165
13.2.2	Izbjegavanje mimikrija.....	166
13.2.3	Mimikrijski napad .....	168
13.2.4	Odbrana od mimikrijskih napada .....	168
13.2.5	Uvez (Binding).....	174
13.3	Implementacija.....	175

13.3.1	Ključevi .....	176
13.3.2	Verifikacija i šifrovanje.....	176
13.3.3	Kombinovanje WOT i TOFU .....	177
13.3.4	Izvoz uvezivanja.....	177
ZAKLJUČAK .....		179
Literatura .....		188
Prilog 1: Tabela skraćenica .....		191
Prilog 2: Popis futnota.....		193
Prilog 3: Popis slika .....		196
Prilog 4: Popis tabela .....		199
Prilog 5: Popis grafikona.....		200