1. UVOD 3
2. MATEMATIČKE OSNOVE ELIPTIČNIH KRIVIH 4
2.1 Definicija eliptične krive 4
2.2 Vajerštrasova jednačina 5
2.2.1 Eliptične krive nad poljem $\mathbb{R}$ 5
2.2.2 Geometrijska interpretacija sabiranja u eliptičnoj krivoj 6
2.2.3 Formula za sabiranje dvije tačke na eliptičnoj krivoj 10
2.2.4 Osobine sabiranja tačaka na eliptičnoj krivoj 12
2.2.5 Eliptične krive nad konačnim poljima 13
2.3 Edvardsove krive 14
2.4 Montgomerijeva kriva 15
2.5 Uvrnuta Edvardsonova kriva 16
3. PRIMJENA ELIPTIČNIH KRIVIH U RAČUNARSKIM MREŽAMA 18
3.1 Eliptične krive Difi–Helman (ECDH) 18
3.2 Primjena eliptičnih krivih u algoritamu za digitalno potpisivanje (ECDSA - Elliptic Curve Digital Signature Algorithm) 19
3.3 Generisanje slučajnih brojeva 20
3.4 Napadi na eliptične krive 21
3.4.1 Problem diskretnog logaritma 21
3.4.2 Polig-Helmanov napad 21
3.4.3 Polard-ro napad 23
3.4.4 Napad malih podgrupa 24
3.4.5 Napad lažnim eliptičnim krivama 24
3.5 Standardizacija parametara eliptične krive 25
3.5.1 SECG – standardizacija parametara eliptične krive 25
3.5.2 NIST - standardizacija parametara eliptične krive 28
3.6 Eliptične krive u praksi 30
3.6.1 Bitkoin 30
3.6.2 Secure Shell (SSH) 31
3.6.3 Transport Layer Security (TLS) 31
3.6.4 Elektronska lična karta 31
4. Implementacija 32

4.1 Implementacija operacija u konačnim poljima 32
4.1.1 Implementacija polja ostataka 32
4.1.2 Implemetacija operacija u proširenim poljima 36
4.2 Implementacija operacija nad eliptičnim krivima 43
4.2.1 Implementacija operacija na Vajerštrasovoj krivoj 45
4.2.2 Implementacija operacija nad Uvrnutom Edvrdsonovom krivom 53
4.2.3 Implemetacija operacija na Montgomerijevoj krivoj 59
4.3 Implementacija protokola baziranih na eliptičnim krivima 66
4.3.1 Implementacija Diffe-Hellman protokola 66
4.3.2 Implementacija ECDSA 68
4.4 Implementacija klase koja pribavlja informacije o nekim poznatim eliptičnim krivima 70
5. Zaključak 73
6. Literatura 75