

SADRŽAJ

UVOD.....	4
1. TEORIJSKA OSNOVA ZIMMERMAN METODE.....	6
1.1. Istorijat PGP metode.....	6
1.2. Principi kriptozastite.....	7
1.3. Zakonski i etički aspekti.....	14
2. TEHNIČKI ASPEKTI ZIMMERMAN METODE.....	16
2.1. Arhitektura PGP algoritma.....	16
2.2. Šifarski ključevi.....	17
2.3. Sigurnosne karakteristike.....	19
3. KOMPARATIVNA ANALIZA ZIMMERMAN METODE SA DRUGIM METODAMA KRIPTOZAŠTITE.....	21
3.1. Prednosti i nedostaci.....	21
3.2. Upotreba u različitim industrijama.....	23
3.3. Performanse i sigurnost.....	25
4. PRAKTIČNA PRIMJENA I STUDIJE SLUČAJEVA.....	27
4.1. Primjena u zaštiti podataka.....	27
4.2. Studije slučajeva iz prakse.....	28
4.2.1. <i>Slučaj primjene PGP-a u banci</i>	28
4.2.2. <i>Slučaj kompanije Amex GBT</i>	30
4.3. Integracija sa softverskim alatima.....	31
4.3.1. <i>Integracija sa email klijentima</i>	31
4.3.2. <i>Integracija sa poslovnim aplikacijama</i>	32
5. IZAZOVI I BUDUĆNOST ZIMMERMAN METODE.....	34
5.1. Kvantna prijetnja i otpornost PGP algoritma.....	34
5.1.1. <i>Kako kvantni računari potencijalno ugrožavaju javno-ključne sisteme</i>	35
5.1.2. <i>Trenutne strategije za kvantno otpornu kriptozastitu</i>	36
5.2. Ograničenja u implementaciji PGP-a.....	37