

Sadržaj

1. UVOD.....	1
2. PODJELA SLUČAJNIH BROJEVA.....	2
3. PRIMJENE SLUČAJNIH BROJEVA.....	4
4. GENERATORI.....	5
4.1. Hardverski generatori.....	5
4.1.1. Linearan kongruentan generator (engl. Linear Congruential Generator - LCG).....	7
4.1.2. Fibonačijev generator sa kašnjenjem (engl. Lagged Fibonacci Generator - LFG).....	8
4.1.3. Zaključak.....	10
4.1.4. Kvantni generator slučajnih brojeva – Quantis.....	11
4.1.5. Samostalni generator – Ranger.....	14
5. PRIMJERI SLUČAJNIH UZORAKA IZ TABLICE SLOŽENIH BROJEVA.....	15
5.1. Upotreba tablice.....	16
5.2. Zaključak problema.....	16
6. KRIPTOGRAFIJA.....	17
6.1. Osnovni pojmovi kriptografije.....	18
6.2. Kriptoanaliza.....	21
7. KRIPTOGRAFSKI BEZBJEDNI GENERATORI PSEUDOSLUČAJNIH BROJEVA (BITOVA).....	23
7.1. ANSI X9.17 generator.....	24
7.2. RSA generator pseudoslučajnih brojeva.....	25
8. ISPITIVANJE GENERATORA SLUČAJNIH BROJEVA.....	26
8.1. Ispitivanje učestalosti u nizu.....	28
8.2. Ispitivanje učestalosti u bloku.....	28
8.3. Ispitivanje uzastopnih ponavljanja istih bitova u nizu.....	28
8.4. Ispitivanje najdužeg uzastopnog ponavljanja jedinica u bloku.....	28
8.5. Ispitivanje ranga matrice.....	29
8.6. Spektralno ispitivanje.....	29
8.7. Ispitivanje ponavljanja predloška u generisanom nizu.....	29
8.8. Maurerov univerzalni statistički test.....	29
8.9. Ispitivanje na temelju Lempel-Ziv kompresije.....	30
8.10. Ispitivanje linearne složenosti.....	30

8.11.	Ispitivanje preklapajućih uzoraka.....	30
8.12.	Ispitivanje približne entropije	31
8.13.	Ispitivanje kumulativne sume	31
8.14.	Ispitivanje slučajnog hoda.....	31
9.	STANDARDIZOVANI TESTOVI SLUČAJNOSTI	32
9.1.	ENT – skup statističkih testova	33
9.2.	DIEHARD (ER) – skup statističkih testova.....	35
9.3.	NIST skup statističkih testova	37
10.	TESTIRANJE SLUČAJNOSTI BINARNIH SEKVENCI.....	38
10.1.	Prikaz rezultata testiranja	39
11.	ZAKLJUČAK	53
	LITERATURA	54