

S A D R Ž A J

1. UVOD	5
2. KRIPTOGRAFIJA	6
2.1 Kriptografski algoritmi	8
3. METODE ZA ŠIFROVANJE	9
3.1 Simetrična kriptografija	11
3.1.1 Osnovni pojmovi i terminologija	13
3.1.2. Simetrični ključ	14
3.1.3 Kriptografski načini rada (cipher modes of operation)	14
3.1.4 Padding	15
3.1.5 Algoritmi simetričnog šifrovanja	17
3.1.6 Aplikacije i slučajevi upotrebe	31
3.1.7 Prednosti i ograničenja	32
3.2 Asimetrična kriptografija	35
3.2.1 Osnovni pojmovi	35
3.2.2 Postupak šifrovanja asimetričnom kriptografijom	36
3.2.3 Algoritmi asimetrične kriptografije	37
4. UNAPREĐENJE POSTOJEĆIH METODA ZA ŠIFROVANJE	40
5. Primjeri	45
6. Zaključak	55
7. Literatura	56
8. Reference	57