# OBSAH

PŘEDMLUVA ..... 5

**1 ZÁKLADY KRYPTOGRAFIE ..... 7**

1.1 Základní pojmy ..... 7
1.2 Kryptografické systémy ..... 8
1.2.1 Utajovací kryptosystémy ..... 9
1.2.2 Autentizační kryptosystémy ..... 11
1.2.3 Hybridní kryptosystémy ..... 13
1.2.4 Bezpečnost kryptosystémů ..... 14
1.2.5 Kryptografické proměnné ..... 17
1.3 Stručná historie kryptografie ..... 18

**2 MATEMATIKA PRO KRYPTOGRAFII ..... 21**

2.1 Logické operace ..... 21
2.2 Operace modulo ..... 22
2.3 Substituce ..... 23
2.4 Rotace ..... 24

**3 TEORIE UTAJENÍ A AUTENTIZACE ZPRÁV ..... 27**

3.1 Teorie utajení zpráv ..... 27
3.1.1 Šifrovací funkce ..... 27
3.1.2 Stupně důvěrnosti zpráv ..... 29
3.2 Teorie autentizace zpráv ..... 32
3.2.1 Stupně autentičnosti zpráv ..... 32
3.2.2 Pečetící funkce ..... 33

**4 JEDNOSMĚRNÉ FUNKCE ..... 37**

4.1 Hešovací funkce ..... 37
4.1.1 Požadavky na hešovací funkce ..... 38
4.1.2 Merkle–Damgårdova konstrukce ..... 39
4.1.3 Hešovací funkce SHA-256 ..... 40
4.2 Expanzní funkce ..... 42

**5 GENERÁTORY NÁHODNÝCH BITŮ ..... 45**

5.1 Nedeterministické generátory náhodných bitů ..... 45
5.2 Deterministické generátory náhodných bitů ..... 47
5.3 Hybridní generátory náhodných bitů ..... 49

**6 SYMETRICKÉ UTAJOVACÍ KRYPTOSYSTÉMY ..... 53**

6.1 Proudové šifry ..... 53
6.2 Dokonalá šifra ..... 55
6.3 Blokové šifry ..... 58
6.3.1 Kaskádová šifra ..... 58
6.3.2 Bloková šifra AES ..... 59
6.4 Provozní režimy blokových šifer ..... 66
6.4.1 Režim ECB ..... 68
6.4.2 Režim CBC ..... 69
6.4.3 Režim CTR ..... 70

**7 SYMETRICKÉ AUTENTIZAČNÍ KRYPTOSYSTÉMY ..... 73**

7.1 Pečeť HMAC ..... 73
7.2 Dokonalá pečeť ..... 75

**8 ASYMETRICKÉ UTAJOVACÍ KRYPTOSYSTÉMY ..... 79**

8.1 Šifra RSA ..... 79
8.1.1 Princip šifry RSA ..... 80
8.1.2 Bezpečnost šifry RSA ..... 83
8.1.3 Šifra RSA-OAEP ..... 85
8.2 Diffie-Hellmanův protokol ..... 88

**9 ASYMETRICKÉ AUTENTIZAČNÍ KRYPTOSYSTÉMY ..... 91**

9.1 Podpis RSA-PSS ..... 91
9.2 Certifikáty ..... 94
9.2.1 Struktura certifikátu ..... 94
9.2.2 Infrastruktura veřejných klíčů ..... 96

**DOSLOV ..... 99**

**LITERATURA ..... 101**

**REJSTŘÍK ..... 105**