

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 Blokovaná šifra AES	59
6.4 PROVOZNI 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 PEČETĚ HMAC.....	73
7.2 DOKONALÁ PEČETĚ	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
REJSTRÍK	105