

OBSAH

ÚVOD.....	1
1 STEGANOGRAFIA, KRYPTOGRAFIA A INFORMAČNÁ BEZPEČNOSŤ	3
1.1 Steganografia.....	3
1.2 Kryptografia	4
1.3 Informačná bezpečnosť	6
2 KLASICKÉ KRYPTOGRAFICKÉ SYSTÉMY	8
2.1 Základné pojmy	8
2.2 Princíp konvenčného šifrovania	8
2.3 Model konvenčného kryptografického systému.....	9
2.4 Klasifikácia kryptografických systémov a šifier	10
2.5 Kryptoanalýza	11
2.6 Bezpečnosť kryptografických algoritmov	13
2.7 Substitučné šifry	14
2.8 Transpozičné šifry	25
2.9 Rotorové stroje	28
3 ALGEBRAICKÉ SYSTÉMY V KRYPTOGRAFII	31
3.1 Grupy, okruhy, telesá a polia.....	31
3.1.1 Grupy.....	31
3.1.2 Okruhy.....	32
3.1.3 Obor integrity	33
3.1.4 Telesá a polia.....	33
3.2 Modulárna aritmetika	34
3.2.1 Deliteľnosť čísel na množine Z	34
3.2.2 Najväčší spoločný deliteľ	34
3.2.3 Euklidov algoritmus	35
3.2.4 Modulárny operátor	36
3.2.5 Vlastnosti modulárnej aritmetiky	37
3.3 Konečné polia.....	41
3.3.1 Konečné polia $GF(p)$	41
3.3.2 Multiplikatívna inverzia v $GF(p)$	42
3.3.3 Polynómy a polynomiálna aritmetika.....	43
3.3.3.1 Bežná polynomiálna aritmetika.....	44
3.3.3.2 Polynomiálna aritmetika v poli $GF(p)$	45
3.3.3.3 Najväčší spoločný deliteľ polynómov	48
3.3.4 Konečné polia $GF(2^n)$	49
3.3.4.1 Modulárna polynomiálna aritmetika nad $GF(2^n)$	49
3.3.4.2 Multiplikatívna inverzia v modulárnej polynomiálnej aritmetike	51
3.3.5 Binárny tvar operácií v $GF(2^n)$	53
4 PRINCÍPY MODERNÝCH KRYPTOGRAFICKÝCH SYSTÉMOV	56
4.1 Charakteristiky dobrých šifier	56
4.2 Utajenie v kryptografických systémoch	56
4.2.1 Ideálne utajenie.....	56
4.2.2 Informačný obsah otvoreného a zašifrovaného textu	57
4.3 Teória zložitosti v kryptografii	59
4.4 Praktická bezpečnosť kryptografických systémov	62
4.5 Princípy moderných šifier	64
5 SYMETRICKÉ ŠIFRY.....	71
5.1 Princípy symetrických blokových šifier	71

5.2	Šifrovací štandard DES	74
5.2.1	Opis algoritmu DES	74
5.2.2	Bezpečnosť algoritmu DES	80
5.3	AES	81
5.3.1	Opis štandardu AES	81
5.3.2	Operácia Substitute bytes	84
5.3.3	Operácia Shift Row Transformation	88
5.3.4	Operácia Mix Column Transformation	88
5.3.5	Operácia Add Round Key	91
5.3.6	Operácia Key Expansion	91
5.4	Režimy blokových šifier	93
5.4.1	Elektronická kódová kniha	93
5.4.2	Zrežazenie zašifrovaného textu	94
5.4.3	Spätná väzba zo zašifrovaného textu	95
5.4.4	Spätná väzba z výstupu	96
5.4.5	Čítačový režim	98
5.5	Vybrané symetrické šifry	98
5.5.1	Trojnásobný DES	99
5.5.2	Blowfish	100
5.5.3	Šifra RC5	102
5.5.4	Vlastnosti najpoužívanejších blokových šifier	104
5.5.5	Symetrická prúdová šifra RC4	104
5.6	Symetrické šifrovanie v sieťovej bezpečnosti	107
5.6.1	Umiestnenie šifrovacích funkcií	107
5.6.2	Distribúcia kľúčov v symetrickom šifrovaní	110
5.7	Generátory náhodných čísel	113
5.7.1	Generátory pseudonáhodných čísel na báze lineárnej kongruencie	115
5.7.2	Kryptograficky bezpečné generátory pseudonáhodných čísel	116
5.7.2.1	Generátor PRNG s využitím čítača	116
5.7.2.2	Generátor PRNG ANSI X 9.17	117
5.7.2.3	Generátor BBS	118
6	TEÓRIA ČÍSEL V KRYPTOGRAFII	120
6.1	Kategorizácia prirodzených čísel	120
6.2	Základná veta aritmetiky	120
6.3	Prvočísla a zložené čísla	121
6.4	Fermatova veta	123
6.5	Eulerova funkcia	124
6.6	Eulerova veta	125
6.7	Generovanie prvočísel	126
6.8	Čínska veta o zvyškoch	128
6.9	Diskrétné logaritmy	132
6.9.1	Logaritmická funkcia	134
6.9.2	Výpočet diskretných logaritmov	136
7	KRYPTOGRAFIA S VEREJNÝM KLÚČOM	139
7.1	Princíp kryptografie s verejným kľúčom	139
7.2	Kryptografické systémy s verejným kľúčom	140
7.3	Podmienky realizovateľnosti kryptografického systému s verejným kľúčom	143
7.4	Kategorizácia kryptografických systémov s verejným kľúčom	144
7.5	Algoritmy kryptografických systémov s verejným kľúčom	144
7.5.1	Algoritmus na výmenu kľúčov Diffie – Hellman	145
7.5.2	Algoritmus El Gamal	148
7.5.3	Algoritmus RSA	149
7.5.3.1	Popis algoritmu RSA	149

7.5.3.2	Analýza algoritmu RSA	152
7.5.3.3	Bezpečnosť algoritmu RSA.....	153
7.5.4	Kryptografia na báze eliptických kriviek	154
7.5.4.1	Eliptické krivky nad reálnymi číslami.....	154
7.5.4.2	Geometrická interpretácia sčítania	156
7.5.4.3	Algebraická interpretácia sčítania	156
7.5.4.4	Eliptické krivky nad konečným poľom $GF(p)$	157
7.5.4.5	Eliptické krivky nad konečným poľom $GF(2^n)$	160
7.5.4.6	Diskrétny logaritmus v eliptických krivkách	161
7.5.4.7	Výmena tajného kľúča na báze ECC.....	162
7.5.4.8	Šifrovanie na báze ECC	163
7.5.4.9	Bezpečnosť kryptografických algoritmov na báze ECC	163
8	MANAŽMENT KĹÚČOV V KRYPTOGRAFIÍ S VEREJNÝM KĹÚČOM.....	164
8.1	Distribúcia verejných kľúčov	164
8.2	Certifikáty podľa odporúčania X.509	168
8.3	Distribúcia tajných kľúčov	173
9	AUTENTIZÁCIA POUŽÍVATEĽOV A AUTORIZÁCIA DÁT	176
9.1	Šifrovanie správy.....	177
9.2	Autentizačný kód správy MAC	179
9.2.1	Vlastnosti a realizácia MAC.....	181
9.3	Hašovacie funkcie	182
9.3.1	Vlastnosti hašovacích funkcií.....	184
9.3.2	Realizácia hašovacích funkcií	185
9.3.3	Bezpečnosť MAC a hašovacích funkcií	186
10	VYBRANÉ TYPY HAŠOVACÍCH FUNKCIÍ.....	188
10.1	Algoritmus MD5	188
10.2	Kompresná funkcia MD5	190
10.3	Algoritmy skupiny hašovacích funkcií SHA.....	192
10.4	Kompresná funkcia SHA-1.....	194
10.5	Skupina hašovacích funkcií SHA-3.....	197
10.6	Algoritmus RIPEMD-160.....	197
10.7	Kompresná funkcia RIPEMD-160.....	200
10.8	Algoritmus HMAC.....	202
11	ELEKTRONICKÉ A DIGITÁLNE PODPISY	207
11.1	Elektronické podpisy	207
11.2	Digitálne podpisy	208
11.3	Priame digitálne podpisy	209
11.4	Verifikované digitálne podpisy	210
11.5	Štandardy pre digitálne podpisy	212
11.5.1	Algoritmus digitálneho podpisu El Gamal	214
11.5.2	Algoritmus DSA.....	215
11.5.3	Digitálne podpisy na báze eliptických kriviek	217
11.6	Hodnotenie bezpečnosti kryptografických algoritmov.....	220
12	INFORMAČNÁ A SIEŤOVÁ BEZPEČNOSŤ	224
12.1	Komponenty informačnej bezpečnosti	224
12.2	Základné pojmy a definície	225
12.3	Sieťová bezpečnosť	229
12.3.1	Komponenty sieťovej bezpečnosti	230
12.3.2	Prístupová bezpečnosť.....	231
12.3.3	Komunikačná bezpečnosť	232

12.3.4	Systemová bezpečnosť	234
12.3.4.1	Firewally	234
12.3.4.2	Útočníci a systémy na ich detekciu	235
12.3.4.3	Škodlivý softvér	237
12.4	Architektúra bezpečnosti ICT	240
12.4.1	Štandardizácia architektúry bezpečnosti ICT	241
12.5	Architektúra bezpečnosti na báze odporúčania X.800	242
12.5.1	Služby bezpečnosti	242
12.5.2	Mechanizmy bezpečnosti	244
12.5.3	Útoky na bezpečnosť	245
12.5.3.1	Pasívne útoky na bezpečnosť	246
12.5.3.2	Aktívne útoky na bezpečnosť	246
12.6	Architektúra bezpečnosti na báze odporúčania X.805	247
12.6.1	Komponenty bezpečnosti	247
12.6.2	Vrstvy bezpečnosti	248
12.6.3	Roviny bezpečnosti	249
12.6.4	Ohrozenia bezpečnosti	249
13	BEZPEČNOSŤ V ARCHITEKTÚRE TCP/ IP	251
13.1	Architektúra TCP/IP	251
13.2	Protokol IPv4	252
13.3	Protokol IPv6	253
13.3.1	Rozšírenie hlavičiek	254
13.4	Bezpečnosť komunikácie na úrovni IP protokolu	255
13.5	Bezpečnostná asociácia	256
13.5.1	Parametre SA	257
13.5.1.1	Režimy IPsec	258
13.5.1.2	Rozširujúca hlavička AH	258
13.5.1.3	Rozširujúca hlavička ESP	260
13.6	Manažment kľúčov v IPsec	261
13.6.1	Protokol OKD	262
13.6.2	Protokol ISAKMP	263
14	BEZPEČNOSŤ PRENOSU DÁT V TRANSPORTNEJ VRSTVE PROTOKOLU TCP/IP	265
14.1	Architektúra protokolu SSL	266
14.2	SSL Record protocol	267
14.3	Change Cipher Spec Protocol	269
14.4	Alert protokol	270
14.5	Handshake protokol	271
14.5.1	Fáza 1 – definovanie parametrov bezpečnosti	272
14.5.2	Fáza 2 – autentizácia servra a výmena kľúčov	274
14.5.3	Fáza 3 – autentizácia klienta a výmena kľúčov	275
14.5.4	Fáza 4 – Kompletizácia spojenia	275
14.6	Výpočet kryptografických parametrov protokolu SSL	276
14.7	Protokol TLS	276
14.7.1	Formát fragmentu v TLS	277
14.7.2	Výpočet MAC	277
14.7.3	Pseudonáhodná funkcia	277
14.7.4	Výstražné správy	278
14.7.5	Šifrovacie súbory	278
14.7.6	Typy certifikátov klienta	278
14.7.7	Výpočet kryptografických parametrov	278
14.7.8	Výplň	278

15	BEZDRÔTOVÉ SIETE	279
15.1	Klasifikácia bezdrôtových sietí	279
15.1.1	Dosah bezdrôtových sietí	279
15.1.2	Podpora mobility	280
15.1.3	Typ prenášaných signálov	280
15.2	Bezpečnosť sietí WPAN.....	282
15.2.1	Technológia Bluetooth	282
15.2.2	Bezpečnosť technológie Bluetooth.....	284
15.2.3	Kľúče v štandarde Bluetooth	285
15.2.4	Generovanie kľúčov	286
15.2.5	Kryptografické algoritmy Bluetooth	290
15.2.5.1	Šifra SAFER+	290
15.2.6	Algoritmy Bluetooth na báze SAFER+	293
15.2.6.1	Autentizačný algoritmus E_1	293
15.2.6.2	Kryptografické algoritmy E_{22} a E_{21}	295
15.2.6.3	Kryptografický algoritmus E_3	296
15.2.7	Mechanizmy bezpečnosti v Bluetooth.....	297
15.3	Bezdrôtové siete WLAN	300
15.3.1	Štandardy pre WLAN.....	303
15.4	Bezpečnosť sietí WLAN	303
15.4.1	Protokol WEP.....	303
15.4.2	WEP autentizácia	304
15.4.3	WEP šifrovanie.....	304
15.4.4	Hodnotenia protokolu WEP	305
15.4.5	Protokol WPA	306
15.4.6	Protokol TKIP	306
15.4.7	Generovanie paketového kľúča	307
15.4.8	Zabezpečenie integrity pomocou MIC	308
15.4.8.1	Riadenie prístupu na báze štandardu 802.1x	308
15.4.9	Štandard 802.11i (WPA2)	309
15.5	Bezpečnosť bezdrôtových sietí WiMAX	311
15.5.1	Štandardné skupiny 802.16	311
15.5.2	Bezpečnosť v štandardoch WiMAX.....	312
15.5.3	Autentizácia v štandardoch WiMAX	312
15.5.4	Šifrovanie dát	313
15.5.4.1	AES v režime CCM.....	313
15.5.5	Bezpečnostné asociácie	314
15.5.6	Manažment súkromných kľúčov	315
15.5.6.1	Protokol PKM verzia 1.....	316
15.5.6.2	Protokol PKM verzia 2.....	316
15.5.6.3	Odvodenie autorizačného kľúča AK	317
15.6	Mobilné siete WWAN.....	317
15.6.1	Generácie mobilných WWAN	317
15.7	Bezpečnosť v sieťach GSM (GPRS).....	318
15.7.1	Autentizácia používateľa.....	319
15.8	Šifrovanie dát v GSM (GPRS)	320
15.8.1	Bezpečnosť mobilných 3G sietí	321
15.8.2	Autentizácia a dohoda o kľúčoch v 3GPP	321
15.8.3	Šifrovanie a integrita dát v 3GPP	322
15.8.4	Bloková šifra KASUMI.....	322
15.8.5	Šifrovanie blokovou šifrou KASUMI	323
15.8.6	Generovanie kľúčov	326
15.8.7	Šifrovacia funkcia f_8	326
15.8.8	Funkcia na výpočet integrity dát f_9	328

15.8.9 Bezpečnosť signalizácie v 3GPP.....	330
ZOZNAM POUŽITEJ LITERATÚRY	331
SLOVNÍK ZÁKLADNÝCH POJMOV	334
REGISTER	342
ABECEDNÝ ZOZNAM SKRATIEK	350

15.8.9 Bezpečnosť signalizácie v 3GPP

Práca, v podstatke bolo usporiadanie spravy zbraňu napráť vo vnútornej oblasti a v diplomacii, vedľa civilizácie a vývoj nových technológií sa vyznačujú aplikáciou moderných postupov, ktoré sa využívajú v každodennom živote.

Kryptografia sa stala modernou vedou a matematickým nástrojom na ochranu súkromia, na bezpečnosť elektronických systémov a na bezpečnosť elektronickej komunikácie. Významnou aplikáciou kryptografie je oblasť informačnej a sietovej bezpečnosti, oblasť ochrany autorských práv a autentifikácie elektronickej dokumentácie.

Uvedené vzťahy v oblasti kryptografie a komunikačnej bezpečnosti boli motiváciou, ktorý viedol k napísaniu tejto publikácie, ktorá predstavuje úvod do uvedenej problematiky. Zároveň slúži ako úvod v tejto oblasti, pričom je potrebné pripomenúť, že uvedené obsah sa vyznačuje dynamickým charakterom, ktorý je súvisiaci vývojom informačných a komunikačných technológií a rozvojom globálnej informačnej spoločnosti.

Prvá kapitola zahŕňa úvod do problematiky a vysvetľuje pojmy steganografia, kryptografia a informačná bezpečnosť.

Problematika klasických kryptografických systémov a šifrov je venovaná druhej kapitole.

Tretia kapitola je venovaná základným operáciám z oblasti matematiky, najmä aritmetickým operáciám ako sú grupy, konečné pole, eliptické krivky a predstava modulárnej aritmetiky.

Princípy moderných kryptografických systémov sú uvedené a analyzované v štvartej kapitole.

Problematika symetrických šifrov je predmetom piatej kapitoly, pričom dôraz je položený na moderné symetrické šifry (DES, 3DES, AES). Zahŕňa aj problematiku generovania náhodných čísel, ktoré majú v kryptografii veľký význam.

Šiesta kapitola predstavuje prehľad základných poznatkov z elementárnej teórie čísel s dôrazom na ich využitie v kryptografii s verejným kľúčom.

Kryptografia s verejným kľúčom je predmetom siedmej kapitoly. Sú tu opísané základné algoritmy s verejným kľúčom (Diffie-Hellman, El Gamal, RSA), pričom osobitná pozornosť je venovaná aj kryptografii na báze eliptických kriviek.

Manažment kľúčov v kryptografii s verejným kľúčom je venovaná ôsma kapitola. Sú tu uvedené problémy súvisiace s distribúciou verejných aj tajných kľúčov, ako aj s certifikáciou verejných kľúčov.

Deväta kapitola je venovaná problematike autentizácie používateľov a autentizácie dát s využitím šifrovania a hašovacích funkcií.

Výberné typy hašovacích funkcií sú opísané v desiatej kapitole.