

Obsah

1. ÚVOD	10
2. ÚVOD DO KRYPTOLOGIE	12
2.1 DEFINICE, ZÁKLADNÍ TERMÍNY A ZKRATKY POUŽÍVANÉ V KRYPTOLOGII.....	12
2.2 PRAVIDLA A ZÁSADY KRYPTOLOGIE	16
2.3 TYPOLOGIE ŠIFROVACÍCH ALGORITMŮ	19
3. HISTORIE KRYPTOLOGIE	21
3.1.1 <i>Starověká kryptologie</i>	21
3.1.2 <i>Středověká kryptologie</i>	22
3.1.3 <i>Kryptologie dvacátého století</i>	22
3.2 MODERNÍ KRYPTOLOGIE.....	24
3.3 HISTORIE – SHRUTÍ	26
4. MATEMATICKÉ ZÁKLADY KRYPTOLOGIE	29
4.1 ALGORITMIZACE V KRYPTOGRAFII	29
4.2 TEORIE ČÍSEL.....	30
4.2.1 <i>Modulární aritmetika</i>	30
4.2.2 <i>Inverze</i>	31
4.2.3 <i>Prvočísla</i>	32
4.2.3.1 Generování náhodných a pseudonáhodných čísel	33
4.2.3.2 Testy na prvočíslnost.....	34
4.2.4 <i>Euklidův algoritmus /69/</i>	36
4.2.5 <i>Úloha faktorizace</i>	37
4.2.6 <i>Úloha diskrétního logaritmu</i>	37
4.2.7 <i>Malá Fermatova věta</i>	37
4.2.8 <i>Teorie Feistelových sítí</i>	38
4.2.9 <i>Čínská věta o zbytcích</i>	38
4.3 KLÍČE	39
5. KLASICKÉ KRYPTOGRAFICKÉ SYSTÉMY	41
5.1 SUBSTITUČNÍ ŠIFRY	41
5.1.1 <i>Monoalfabetická substituční šifra</i>	41
5.1.1.1 Monoalfabetické šifry založené na klíčovacích frázích.....	43
5.1.1.2 Césarovská šifra	44
5.1.2 <i>Homofonní substituční šifra</i>	46
5.1.3 <i>Polygramová substituční šifra</i>	47
5.1.4 <i>Polyalfabetické šifry</i>	47
5.1.4.1 Obecné Vigenérovské šifry	48

5.1.5	<i>Hillova šifra</i>	49
5.1.6	<i>Steganografie</i>	50
5.1.6.1	Typy steganografie a techniky pro steganografii	51
5.1.6.2	Příklady oblastí využití steganografie	58
5.1.6.3	Stegoanalýza	59
5.1.7	<i>Vernamova šifra</i>	59
5.1.8	<i>Transpozice</i>	61
6.	MODERNÍ ŠIFROVACÍ ALGORITMY	63
6.1	SYMETRICKÁ A ASYMETRICKÁ KRYPTOGRAFIE	63
6.2	SYMETRICKÁ KRYPTOGRAFIE	65
6.2.1	<i>Kryptosystémy Feistelova typu</i>	67
6.2.2	<i>DES</i>	69
6.2.2.1	Pokusy zesílit DES	71
6.2.3	<i>IDEA (International Data Encryption Algorithm)</i>	73
6.2.4	<i>GOST</i>	75
6.2.5	<i>Šifra AES (RIJNDAEL)</i>	76
6.2.5.1	Notace a konvence	76
6.2.5.2	Matematické základy šifry Rijndael	77
6.2.5.3	Proces šifrování	78
6.2.5.4	Implementace a rychlost	84
6.2.5.5	Bezpečnost algoritmu	86
6.2.5.6	Celkové zhodnocení AES	90
6.2.6	<i>Shrnutí pro symetrické šifrování</i>	90
6.3	ASYMETRICKÁ KRYPTOGRAFIE	90
6.3.1	<i>Kryptografie s veřejným klíčem</i>	91
6.3.2	<i>Zavazadlový algoritmus</i>	95
6.3.3	<i>Algoritmus RSA</i>	97
6.3.3.1	Tvorba klíčů	97
6.3.3.2	Postup šifrování	99
6.3.3.3	RSA a PKCS#1	100
6.3.3.4	RSA prakticky – bezpečnost, rychlost, normalizace	102
6.3.4	<i>EL GAMAL</i>	103
6.3.5	<i>SKIPJACK a KEA</i>	105
6.4	KRYPTOGRAFICKÉ STANDARDY	106
6.4.1	<i>Nový standard AES pro symetrickou kryptografii</i>	106
6.4.2	<i>NESSIE</i>	108
6.4.3	<i>Normy PKCS</i>	109
7.	KRYPTOANALÝZA	110
7.1	ÚTOKY PROTI ŠIFRÁM	111
7.2	ÚTOKY PROTI KLASICKÝM ŠIFRÁM	112

7.2.1	<i>Frekvenční analýza</i>	113
7.2.2	<i>Zjištění a využití koeficientu koincidence</i>	114
7.2.3	<i>Jednoduchá polyalfabetická šifra</i>	116
7.3	ÚTOK HRUBOU SILOU	117
7.3.1	<i>Útok hrubou silou – symetrická kryptografie</i>	117
7.3.2	<i>Možná řešení pro útok hrubou silou</i>	117
7.3.2.1	Kvantové počítače	117
7.3.2.2	DNA computing	119
7.3.2.3	Počítačové viry	120
7.3.2.4	Paralelní počítače na Internetu	121
7.3.2.5	Čínská loterie.....	121
7.3.2.6	Biotechnologie	121
7.3.3	<i>Termodynamické hranice pro útok hrubou silou</i>	121
7.3.4	<i>Útok hrubou silou – kryptografie s veřejným klíčem</i>	122
7.3.4.1	Srovnání bezpečnosti symetrické kryptografie a kryptografie s veřejným klíčem	122
7.3.5	<i>Útoky na RSA</i>	123
7.3.5.1	Útok na RSA se znalostí podepsaného šifrovaného textu .	123
7.3.5.2	Útok na RSA se společným modulem n	124
7.3.5.3	Podpis podvrženého dokumentu	124
7.3.5.4	Záměna zpráv	125
7.3.6	<i>Zesilování šifrování</i>	125
7.3.6.1	Dvojitě šifrování.....	125
7.3.6.2	Trojitě šifrování.....	126
8.	HAŠOVACÍ FUNKCE	127
8.1	KONCEPCE.....	127
8.2	HAŠOVACÍ FUNKCE – VLASTNOSTI A PODSTATA	130
8.3	VYBRANÉ HAŠOVACÍ FUNKCE.....	133
8.3.1	<i>RIPMD-x</i>	133
8.3.2	<i>SHA-1</i>	133
9.	KRYPTOGRAFICKÉ PROTOKOLY	134
9.1.1	<i>Protokoly pro bezpečnou komunikaci na počítačových sítích</i> 134	
9.1.1.1	Protokol S-HTTP	134
9.1.1.2	Protokol SSL	135
9.1.2	<i>Modelové útoky proti kryptografickým protokolům</i>	137
9.1.3	<i>Oblivious transfer</i>	138
9.1.4	<i>Kryptografický protokol pro výpočet průměrného platu</i>	139
9.1.5	<i>Protokol pro bezpečné volby</i>	139
9.1.5.1	Protokol bez centrální autority	139
9.1.5.2	Protokol se dvěma centrálními autoritami	141

9.1.6	<i>Protokoly pro elektronický obchod a bezpečnou komunikaci</i>	142
9.1.6.1	Podepisování kontraktů	142
9.1.6.2	Elektronická potvrzovaná pošta	143
9.1.6.3	Podpisy naslepo	143
9.1.6.4	Autentizované platby	144
9.1.6.5	Protokol pro digitální podpisy	146
9.1.6.6	Komunikace se symetrickou kryptografií	147
10.	ELEKTRONICKÝ PODPIS	148
10.1	TEORETICKÉ ZÁKLADY ELEKTRONICKÉHO PODPISU	149
10.1.1	<i>Vlastnosti digitálního podpisu</i>	<i>150</i>
10.1.2	<i>Bezpečnost digitálního podpisu</i>	<i>151</i>
10.1.3	<i>Kryptografie a digitální podpis</i>	<i>151</i>
10.1.4	<i>Specifika elektronického podpisu</i>	<i>154</i>
10.1.4.1	Vztah vlastnoručního a digitálního podpisu	154
10.1.4.2	Certifikáty, certifikační autority /37, 76/	154
10.2	LEGISLATIVA	158
10.2.1	<i>Právní úprava elektronického podpisu v České republice</i>	<i>158</i>
10.2.1.1	Vymezení některých termínů v zákoně	159
10.2.1.2	Zákon o elektronickém podpisu v praxi	162
10.2.1.3	Vyhlášky k Zákonu o elektronickém podpisu	163
10.2.2	<i>Aktivita Evropské Unie v oblasti elektronických podpisů</i>	<i>163</i>
10.2.3	<i>Normy ISO pro elektronický podpis</i>	<i>165</i>
10.3	ELEKTRONICKÝ PODPIS V PRAXI /35/	168
11.	NOVÉ POSTUPY KRYPTOGRRAFIE	172
11.1	KRYPTOGRRAFIE A KOMPRESSE DAT – FRAKTÁLY	172
11.1.1	<i>Afinní transformace v R</i>	<i>172</i>
11.1.2	<i>Afinní transformace v R^2</i>	<i>172</i>
11.1.3	<i>Fraktální šifrování</i>	<i>173</i>
11.2	ŠIFROVÁNÍ POMOCÍ NEURONOVÝCH SÍTÍ	173
11.3	KRYPTOLOGIE – ZÁVĚRY	174
12.	OTÁZKY A ÚKOLY – SOUHRNNÝ TEST, SHRUTÍ	175
13.	STUDIJNÍ LITERATURA A DALŠÍ ZDROJE INFORMACÍ	176
14.	PŘÍLOHY	181