

OBSAH

Předmluva	3
1. Úvod do kryptografie	5
1.1 Historie vývoje kryptografie	5
1.2 Informační bezpečnost a úkoly soudobé kryptografie.....	6
1.2.1 Cíle kryptografie.....	8
1.2.2 Hodnocení kryptografických prostředků.....	9
1.3 Kryptografický pohled na matematické funkce.....	10
1.3.1 Injekce, surjekce, bijekce, jednosměrnost (s tajnou informací).....	11
1.3.1.1 Funkce injektivní 1-1, surjektivní onto a bijektivní	13
1.3.1.2 Funkce jednosměrná	14
1.3.1.3 Funkce jednosměrná s tajnou informací	15
1.3.2 Permutace.....	16
1.3.3 Involuce	17
1.4 Základní termíny a pojmy	18
1.4.1 Definiční obory šifer a obory jejich hodnot	18
1.4.2 Šifrovací a dešifrovací transformace	18
1.4.3 Proces utajení.....	19
1.4.4 Účastníci komunikace	20
1.4.5 Kanály	21
1.4.6 Zabezpečení	21
1.4.7 Informační bezpečnost v obecném pojetí	22
1.4.8 Kryptologie	23
1.5 Šifry symetrického klíče	23
1.5.1 Stručný popis blokových a proudových šifer	23
1.5.2 Substituční a transpoziční šifry	25
1.5.2.1 Monoalfabetická substituční šifra	25
1.5.2.2 Homofonní substituční šifra	26
1.5.2.3 Šifra dělené morseovky	26
1.5.2.4 Polyalfabetické substituční šifry	29
1.5.2.5 Transpoziční šifry	30
1.5.3 Kompozice šifer	30
1.5.3.1 Kompozice funkcí	30
1.5.3.2 Kompozice a involuce	30
1.5.3.3 Kombinované šifry	31
1.5.4 Proudové šifry	32
1.5.4.1 Vernamova šifra	33
1.5.5 Prostor klíčů	33
1.6 Digitální podpis	34
1.6.1 Názvosloví a značení	34
1.6.2 Podpisová procedura	34
1.6.3 Verifikační procedura	35
1.6.4 Žádané vlastnosti podpisových a verifikačních funkcí	35
1.7 Autentizace a identifikace	36

1.7.1	Identifikace	37
1.7.2	Autentizace původu dat	37
1.8	Kryptografie veřejného klíče	38
1.8.1	Šifrování veřejným klíčem	38
1.8.2	Autentizace entit v kryptosystémech veřejného klíče	40
1.8.3	Digitální podpis z reverzibilní šifry veřejného klíče.....	41
1.8.3.1	Konstrukce digitálního podpisového schématu	41
1.8.4	Digitální podpisy v praxi	42
1.8.4.1	Řešení sporů	43
1.8.4.2	Požadavky na řešení sporných podpisů	43
1.8.5	Porovnání symetrické a asymetrické kryptografie	43
1.8.5.1	Výhody kryptografie symetrického klíče	43
1.8.5.2	Nevýhody kryptografie symetrického klíče	44
1.8.5.3	Výhody kryptografie veřejného klíče	44
1.8.5.4	Nevýhody šifrování veřejným klíčem	44
1.8.5.5	Závěrečné srovnání	45
1.9	Hašé funkce	46
1.10	Protokoly a mechanismy	47
1.10.1	Protokol, mechanismus, algoritmus	47
1.10.2	Selhání protokolů a mechanismů	47
1.11	Zavádění, správa a potvrzování klíčů	49
1.11.1	Metodologie bezpečné distribuce klíčů	49
1.11.2	Manažment klíčů řešený symetrickou kryptografií.....	50
1.11.3	Manažment klíčů řešený technikou veřejného klíče.....	51
1.11.4	Důvěryhodná třetí strana	53
1.11.5	Certifikáty veřejných klíčů	53
1.12	Pseudonáhodná čísla a posloupnosti	54
1.13	Útoky na šifry a protokoly. Modely hodnocení bezpečnosti	56
1.13.1	Pasivní a aktivní útok	56
1.13.2	Luštění šifrových systémů	56
1.13.3	Útoky proti protokolům	57
1.13.4	Modely pro hodnocení bezpečnosti	57
1.13.4.1	Absolutní (nepodmíněná bezpečnost)	58
1.13.4.2	Teoretická (teorie složitosti) bezpečnost	58
1.13.4.3	Dokazatelná bezpečnost	58
1.13.4.4	Výpočetní bezpečnost	59
1.13.4.5	Ad hoc bezpečnost	59
1.13.5	Perspektivy výpočetní bezpečnosti	59
1.13.6	Jak velké je skutečně velké?	60
1.14	Poznámky a podpůrné reference k 1. kapitole	61
2.	Matematické základy kryptografie	66
2.1	Teorie pravděpodobnosti	66
2.1.1	Základní definice	66

2.1.2	Podmíněná pravděpodobnost	67
2.1.3	Náhodné proměnné	67
2.1.4	Binomické rozdělení	68
2.1.5	Útoky paradoxem společných narozenin	69
2.1.6	Modely náhodných zobrazení	71
2.2	Teorie informace	73
2.2.1	Entropie	73
2.2.2	Vzájemná informace	74
2.3	Teorie složitosti	75
2.3.1	Základní definice	75
2.3.2	Asymptotický zápis	76
2.3.3	Třídy složitosti	77
2.3.4	Nahodilostní algoritmy	81
2.4	Teorie čísel	82
2.4.1	Celá čísla	82
2.4.2	Algoritmy pro celá čísla $\mathbb{Z}$	85
2.4.3	Celá čísla modulo n	86
2.4.4	Algoritmy pro celá čísla modulo $\mathbb{Z}_n$	91
2.4.5	Symbol Legendreuv a Jacobyho	93
2.4.6	Blumova celá čísla	96
2.5	Abstraktní algebra	96
2.5.1	Grupy	97
2.5.2	Okruhy	98
2.5.3	Pole (Tělesa)	99
2.5.4	Okruhy polynomů	99
2.5.5	Vektorové prostory	101
2.6	Konečná pole (Tělesa)	103
2.6.1	Základní vlastnosti	103
2.6.2	Euclídův algoritmus pro polynomy	104
2.6.3	Aritmetika polynomů	106
2.7	Poznámky a podpůrné reference ke 2. kapitole	110
3.	Kryptografické protokoly	111
3.1	Stavební bloky kryptografických protokolů	111
3.1.1	Úvod k protokolům	111
3.1.1.1	Účel protokolů	112
3.1.1.2	Účastníci protokolů	113
3.1.1.3	Arbitrážní protokoly	113
3.1.1.4	Protokoly s účastí smírčího soudce	115
3.1.1.5	Vnitřně chráněné protokoly	117
3.1.1.6	Útoky proti protokolům	117
3.1.2	Využití symetrické kryptografie pro komunikaci	118
3.1.3	Jednosměrné funkce	120
3.1.4	Jednosměrné haše funkce	121

3.1.4.1	Autentizační kódy zpráv	122
3.1.5	Využití kryptografie veřejného klíče pro komunikaci.....	122
3.1.5.1	Hybridní kryptosystémy	123
3.1.5.2	Merklovy hádanky	124
3.1.6	Digitální podpisy	125
3.1.6.1	Užití symetrické kryptografie s arbitrem pro podpis.....	126
3.1.6.2	Užití kryptografie veřejného klíče pro podpis	128
3.1.6.3	Užití časových známek pro podpis	128
3.1.6.4	Využití asymetrické kryptografie s hašovací funkcí pro podpis	129
3.1.6.5	Algoritmy a terminologie	130
3.1.6.6	Násobné podpisy	130
3.1.6.7	Nepopíratelné digitální podpisy	131
3.1.6.8	Aplikace digitálních podpisů	132
3.1.7	Digitální podpisy s šifrováním	132
3.1.7.1	Zpětné odeslání zprávy jako potvrzení příjmu	133
3.1.7.2	Odvrácení útoku založeném na zpětném odeslání zprávy	134
3.1.7.3	Útoky proti kryptografii veřejného klíče	135
3.1.8	Tvorba náhodných a pseudonáhodných posloupností	135
3.1.8.1	Pseudonáhodné posloupnosti	136
3.1.8.2	Kryptograficky bezpečné pseudonáhodné posloupnosti	137
3.1.8.3	Skutečně náhodné posloupnosti	137
3.2	Základní kryptografické protokoly	138
3.2.1	Výměna klíčů	138
3.2.1.1	Výměna klíčů pomocí symetrické kryptografie	138
3.2.1.2	Výměna klíčů pomocí veřejné kryptografie	139
3.2.1.3	Útok narušitele zastupováním	139
3.2.1.4	Vnitřně zabezpečený protokol	140
3.2.1.5	Výměna klíče s digitálním podpisem	141
3.2.1.6	Přenos klíče a zprávy	142
3.2.1.7	Hromadné rozeslání klíče a zprávy	142
3.2.2	Autentizace	143
3.2.2.1	Autentizace pomocí jednosměrných funkcí	143
3.2.2.2	Slovníkový útok a náhodný řetězec připojený k heslu	143
3.2.2.3	Autentizační program jištěný jednosměrnou funkcí	144
3.2.2.4	Autentizace využívající kryptografii veřejného klíče	145
3.2.2.5	Vzájemná autentizace a vnitřně zabezpečený protokol	146
3.2.2.6	Dva symetrické identifikační kryptografické protokoly	147
3.2.2.7	Autentizace zprávy	148
3.2.3	Autentizace a výměna klíčů	148
3.2.3.1	Další protokoly	157
3.2.3.2	Z čeho se poučit?	157
3.2.4	Analýza protokolů pro autentizaci a výměnu klíčů	157
3.2.5	Asymetrická kryptografie mnoha klíčů	161

3.2.5.1	Hromadné rozesílání zpráv	162
3.2.6	Dělení utajované informace	163
3.2.7	Sdílení utajované informace	164
3.2.7.1	Sílení tajné informace s nedůvěryhodnými účastníky.....	165
3.2.7.2	Sdílení tajné informace bez arbitra T	166
3.2.7.3	Sdílení tajné informace bez zveřejnění sdílených znaků	166
3.2.7.4	Ověřitelné sdílení tajné informace	167
3.2.7.5	Sdílení tajné informace s omezením	167
3.2.7.6	Sdílení tajné informace s vyloučením nežádoucí osoby	167
3.2.8	Kryptografická ochrana databází	167
4.	Kryptografické techniky	169
4.1	Délka klíče	169
4.1.1	Délka symetrického klíče	169
4.1.1.1	Odhady časů a nákladů na útok hrubou silou	169
4.1.1.2	„Softwéroví krakeři“	171
4.1.1.3	Neuronové sítě	171
4.1.1.4	Viry	171
4.1.1.5	Čínská loterie	172
4.1.1.6	Biotechnologie	172
4.1.7	Termodynamická omezení	173
4.1.2	Délka veřejného klíče	173
4.1.2.1	Řešení NP - složitého problému technikou DNA	175
4.1.2.2	Řešení NP - složitého problému kvantovým počítačem	176
4.1.3	Porovnání délek symetrických a veřejných klíčů	176
4.1.4	Útok na hašé funkce paradoxem společných narozenin	177
4.1.5	Jak dlouhý má být klíč?.....	178
4.1.6	Závěrečné varování	178
4.2	Manažment klíčů	179
4.2.1	Generování klíčů	179
4.2.1.2	Výběr špatných klíčů	180
4.2.1.3	Náhodné klíče	181
4.2.1.4	Větná hesla	182
4.2.1.5	Norma X 9.17 pro generování klíčů	182
4.2.1.6	Generování klíčů podle ministerstva obrany USA	183
4.2.2	Nelineární prostory klíčů	183
4.2.3	Přeprava klíčů	184
4.2.3.1	Distribuce klíčů ve velkých sítích	185
4.2.4	Verifikace klíčů.....	185
4.2.4.1	Detekce chyb při přenosu klíče	185
4.2.4.2	Detekce chyb klíče při dešifrování	185
4.2.5	Používání klíčů	186
4.2.5.1	Kontrola používání klíčů	186
4.2.6	Aktualizace klíčů	187

4.2.7	Ukládání klíčů.....	187
4.2.8	Zálohování klíčů	188
4.2.9	Kompromitace klíčů	188
4.2.10	Životnost klíčů	189
4.2.11	Ničení klíčů	190
4.2.12	Manažment veřejných klíčů	190
4.2.12.1	Certifikáty veřejného klíče	190
4.2.12.2	Distribuovaný manažment klíčů	190
4.3	Typy a režimy algoritmů	191
4.3.1	Režim elektronické kódové knihy	191
4.3.1.1	Doplňování v režimu ECB	192
4.3.2	Opakování bloků	193
4.3.3	Režim řetězení šifrových bloků	195
4.3.3.1	Inicializační vektor	196
4.3.3.2	Doplňování v režimu CBC	197
4.3.3.3	Šíření chyb	198
4.3.3.4	Bezpečnostní problémy	199
4.3.4	Proudové šifry	199
4.3.5	Proudové šifry s vlastní synchronizací	201
4.3.5.1	Bezpečnostní problémy	202
4.3.6	Režim šifrové zpětné vazby	203
4.3.6.1	Inicializační vektor	203
4.3.6.2	Šíření chyb	205
4.3.7	Synchronní proudové šifry	205
4.3.7.1	Útok vkládáním	206
4.3.8	Režim výstupní zpětné vazby	207
4.3.8.1	Inicializační vektor v OFB režimu	207
4.3.8.2	Šíření chyb	207
4.3.8.3	Bezpečnostní problémy v OFB režimu	209
4.3.8.4	Proudové šifry v OFB režimu	209
4.3.9	Čítačový režim	210
4.3.9.1	Proudové šifry v čítačovém režimu	210
4.3.10	Další režimy blokových šifer	211
4.3.10.1	Režim řetězení bloků	211
4.3.10.2	Režim šířeného řetězení šifrových bloků	211
4.3.10.3	Řetězení šifrových bloků s kontrolním součtem	212
4.3.10.4	Výstupní zpětná vazba s nelineární funkcí	212
4.3.10.5	Další režimy	213
4.3.11	Volba režimu šifry	213
4.3.12	Prokládání	216
4.3.13	Vzájemné porovnání blokových a proudových šifer.....	217
4.4	Informační bezpečnost v obecném pojetí	218
Reference		221

