

OBSAH

PŘEDMLUVA

1

1. PROBLÉM INFORMAČNÍ BEZPEČNOSTI

7

1.1 Úvod

7

1.2 Charakter nežádoucího průniku do systému informatiky

8

1.3 Druhy narušení bezpečnosti

9

1.4 Zranitelná místa informační bezpečnosti

10

1.5 Lidé v počítačové kriminalitě

15

1.6 Metody obrany

18

2. ÚVOD DO KRYPTOLOGIE

22

2.1 Terminologie

22

2.2 Steganografie

31

2.3 Substituční a transpoziční šifry

32

2.4 Operace mod 2 (XOR)

36

2.5 Jednorázový heslář (heslář pro jedno použití)

37

2.6 Počítačové algoritmy

40

2.7 Odkazy

40

3. SUBSTITUČNÍ A TRANSPOZIČNÍ ŠIFRY

42

3.1 Reprezentace znaků

42

3.2 Monoalfabetické (substituční) šifry

43

3.3 Polyalfabetické substituční šifry

52

3.4 Transpozice (Permutace)

68

3.5 Proudové a blokové šifry

76

3.6 Charakteristiky „dobrých“ šifer

79

3.7 Odkazy

80

4. MATEMATICKÉ ZÁKLADY KRYPTOLOGIE

81

4.1 Teorie informace

81

4.2 Teorie složitosti

86

4.3 Teorie čísel

93

4.4 Rozklady

108

4.5 Generování prvočísel

111

4.6 Diskrétní logaritmy v konečném tělese

112

4.7 Odkazy

117

5. ŠIFROVACÍ NORMA DES	121
5.1 Úvod	121
5.2 Popis DES	121
5.3 Bezpečnost DES	132
5.4 Diferenční a lineární kryptoanalýza	138
5.5 Reálná kritéria návrhu	140
5.6 Varianty algoritmu DES	141
5.7 Bezpečnost současného DES	146
5.8 Odkazy	147
6. ALGORITMY VEŘEJNÉHO KLÍČE	151
6.1 Úvod	151
6.2 Zavazadlový algoritmus	152
6.3 RSA	156
6.4 Pohlig-Hellmanův systém	164
6.5 Rabinův systém	165
6.6 El Gamalův systém	167
6.7 Mc Elliceův systém	169
6.8 Kryptosystémy založené na eliptických křivkách	170
6.9 LUC systém	171
6.10 Kryptosystémy veřejného klíče řešené jako konečné automaty	172
6.11 Odkazy	173
7. BEZPEČNOST POČÍTAČOVÝCH SÍTÍ	179
7.1 Porovnání počítačové sítě s výpočetním systémem	179
7.2 Bezpečnostní problémy počítačových sítí	179
7.3 Šifrování v sítích	189
7.4 Kontrola přístupu	192
7.5 Autentizace uživatelů	204
7.6 Ohrožení aktivními uzly	206
7.7 Sledování provozu	211
7.8 Datová integrita	213
7.9 Lokální sítě LAN (Local Area Networks)	215
7.10 Shrnutí bezpečnostních problémů počítačových sítí	219
7.11 Odkazy	220
8. KVANTOVÉ POČÍTAČE A KVANTOVÁ KRYPTOGRAFIE	221
8.1 Úvod	221
8.2 Kvantová mechanika	222
8.3 Kvantovaná informace	223
8.4 Kvantové počítání	224
8.5 Mnohačasticové kvantové stavy	227

8.6 Kvantová kryptografie	229
8.7 Odkazy	232
9. RIZIKOVÁ ANALÝZA A PLÁNOVÁNÍ BEZPEČNOSTNÍCH OPATŘENÍ	233
9.1 Úvod	233
9.2 Riziková analýza	233
9.3 Plán bezpečnostních opatření	244
9.4 Shrnutí problematiky plánování bezpečnostních opatření	249
9.5 Odkazy	249
10. OCHRANA INFORMACÍ A NORMY	251
10.1 Úvod	251
10.2 Historie	251
10.3 Současný stav v normalizaci	253
10.4 Normalizační činnost ISO	257
10.5 Další mezinárodní normalizační organizace	269
10.6 Problematika hodnocení zabezpečených informačních systémů	271
10.7 Shrnutí	295
10.8 Odkazy	296