

# Obsah

Úvod .....	7
1 Z histórie šifrovania .....	13
I Základy kryptológie .....	23
2 Základy kryptografie .....	25
2.1 Základy modulárnej aritmetiky .....	25
2.2 Všeobecné pravidlá kryptológie .....	40
2.3 Abeceda textu .....	42
2.4 Definícia kryptografického systému .....	47
2.5 Klasické kryptografické systémy .....	53
3 Základy kryptoanalýzy .....	63
3.1 Modely zdroja .....	63
3.2 Model jazyka .....	67
3.3 Základné štatistické prostriedky kryptoanalýzy .....	78
3.4 Index koincidence .....	83
II Klasická kryptológia .....	93
4 Monoalfabetické šifry .....	95
4.1 Cézarovské šifry .....	95
4.2 Afinné šifry .....	103
4.3 Všeobecná monoalfabetická šifra .....	111
4.4 Hillovská šifra .....	122
5 Polyalfabetické šifry .....	135
5.1 Dĺžka kľúča .....	135
5.1.1 Kasiského metóda .....	136
5.1.2 Metóda koincidence .....	137
5.1.3 Metóda pokusov .....	141
5.2 Zistenie kľúča pre vigenèrovské šifry .....	143

<b>III Kryptológia dnes</b> .....	<b>153</b>
<b>6 Systémy s verejným kľúčom</b> .....	<b>155</b>
6.1 Binárna bitová zložitosť .....	155
6.2 Základy a aplikácie verejných kľúčovacích systémov .....	163
6.3 Architektúra VKS .....	166
<b>7 Kódovanie a šifrovanie</b> .....	<b>173</b>
7.1 Ako zabrániť pasívnemu odpočúvaniu so šumom .....	173
7.2 Ako zabrániť pasívnemu odpočúvaniu bez šumu .....	183
<b>8 Kryptosystémy Feistelovho typu</b> .....	<b>193</b>
8.1 Všeobecná schéma .....	193
8.2 Lucifer a DES .....	195
<b>9 RSA – algoritmus</b> .....	<b>199</b>
9.1 Postup pri RSA – šifrovaní .....	200
9.2 Diskusia algoritmu RSA .....	205
<b>10 Niektoré aplikácie VKS</b> .....	<b>247</b>
10.1 Hierarchický kryptosystém .....	247
10.2 Kryptosystém kolektívnej bezpečnosti .....	250
<b>Literatúra</b> .....	<b>257</b>
<b>Index</b> .....	<b>265</b>