

# Obsah

<b>Poděkování</b> .....	7
<b>1 Úvod</b> .....	9
<b>2 Historie</b> .....	13
2.1 Starověk .....	13
3.1 Středověk a raný novověk .....	14
2.3 Devatenácté století .....	15
2.4 Legendy, poklady a stará písmena .....	16
2.5 První světová válka .....	17
2.6 Druhá světová válka .....	18
2.7 Současnost .....	21
2.8 Výhled do budoucna .....	24
2.9 Přehled historie šifrování .....	25
<b>3 Šifrovací hry</b> .....	27
3.1 Výzvy .....	27
3.2 Drobné šifrovací hry .....	30
3.3 Velké šifrovací hry .....	31
3.4 Základní principy velkých her .....	32
3.5 Komunita hráčů .....	35
3.6 Přehled velkých her .....	36
3.7 Popis hry: Tmou 7 .....	41
<b>4 Organizace šifrovacích her</b> .....	53
4.1 Organizace drobných her .....	53
4.2 Příprava šifer .....	54
4.3 Zabezpečení hry .....	57
4.4 Příklady chyb a problémů .....	60
<b>5 Základy</b> .....	65
5.1 Pojmy .....	65
5.2 Kódování .....	67
5.3 Matematické základy .....	70
<b>6 Klasické šifry</b> .....	73
6.1 Jednoduché substituce .....	73
6.2 Polyalfabetická substituce .....	74
6.3 Polygrafické substituce .....	76
6.4 Další substituce .....	79
6.5 Jednoduché transpoziční systémy .....	80

6.6	Transpozice dle klíče a mřížky	81
6.7	Produktové šifry	82
<b>7</b>	<b>Skrývání a nekonvenční metody</b>	<b>85</b>
7.1	Neviditelné inkousty	85
7.2	Skrytí celé zprávy	86
7.3	Skrývání v textu	87
7.4	Morseovka	88
7.5	Grafické šifry	90
7.6	Víceúrovňové šifry	92
7.7	Nepřímé informace	94
<b>8</b>	<b>Moderní šifry</b>	<b>95</b>
8.1	Pojmy	95
8.2	Symetrické šifry	96
8.3	Veřejná výměna klíčů	98
8.4	Šifry s veřejným klíčem	100
8.5	Digitální steganografie	101
<b>9</b>	<b>Kryptoanalýza klasických šifer</b>	<b>103</b>
9.1	Charakteristiky češtiny	104
9.2	Rozluštění Caesarovy šifry	104
9.3	Rozluštění monoalfabetické substituce	105
9.4	Rozluštění polyalfabetické substituce	107
9.5	Rozluštění šifry Playfair	109
9.6	Rozluštění transpozice dle klíče	112
9.7	Rozluštění transpoziční mřížky	113
9.8	Nepřímé útoky	115
<b>10</b>	<b>Luštění šifer při hrách</b>	<b>117</b>
10.1	Základní otázky	117
10.2	Analýzy a pozorování	118
10.3	Luštění v terénu	120
10.4	Příklady z her	122
<b>11</b>	<b>Příklady</b>	<b>129</b>
11.1	Příklady	130
11.2	Nápovědy	160
11.3	Řešení	166
11.4	Rejstřík příkladů	184
	<b>Literatura a odkazy</b>	<b>185</b>
<b>A</b>	<b>Slovníček</b>	<b>189</b>
<b>B</b>	<b>Přílohy</b>	<b>193</b>