

## Obsah

<b>Proč tato publikace vznikla .....</b>	<b>8</b>
Co najdete v části o šifrování .....	8
Co najdete v části o biometrikách .....	8
<b>Podpora knihy na webu .....</b>	<b>9</b>
<b>Poděkování .....</b>	<b>10</b>
<b>Vítejte ve světě tajemství .....</b>	<b>12</b>
Trocha motivace na začátek .....	12
Kryptografie + kryptoanalýza = kryptologie .....	12
<b>Různé pohledy na kryptosystémy .....</b>	<b>16</b>
Substituční a transpoziční šifry .....	16
<b>Historické milníky ve světě šifer .....</b>	<b>23</b>
Kryptologie za světových válek .....	23
Vynález počítače .....	34
Kvantová teorie .....	38
<b>Současná kryptografie .....</b>	<b>42</b>
DES .....	42
Shamirův algoritmus .....	46
Diffie-Hellman protokol .....	47
RSA .....	49
PGP .....	52
Hašovací funkce .....	55
<b>Autentizační protokoly .....</b>	<b>57</b>
Co je autentizace .....	57
Protokoly typu výzva-odpověď .....	58
SSL protokol .....	61
Kerberos .....	65
SET .....	67
Možné útoky na autentizační protokoly .....	67
<b>Infrastruktura veřejných klíčů .....</b>	<b>68</b>
Složky PKI .....	68
Procedury PKI .....	69
Certifikáty a webové prohlížeče .....	71
Vytvoření vlastního testovacího certifikátu .....	76



# Šifrování a biometrika aneb tajemné bity a dotyky

<b>Praktické šifrování .....</b>	<b>77</b>
Steganografický software .....	77
Hašovací software .....	80
Šifrování dat na disku .....	82
Šifrování s GPG .....	88
<b>Bezpečnost hesel .....</b>	<b>93</b>
Jak si zvolit bezpečné heslo .....	93
Programy pro generování hesel .....	94
Programy pro rekonstrukci hesel .....	96
Sniffing .....	110
<b>Základy biometrik .....</b>	<b>118</b>
Co jsou biometriky .....	118
Proces práce s biometrikami .....	120
<b>Biometriky ruky .....</b>	<b>123</b>
Otisk prstu .....	123
Geometrie ruky .....	130
Dynamika podpisu .....	131
Dynamika stisku kláves .....	132
Další technologie .....	133
<b>Biometriky hlavy .....</b>	<b>135</b>
Oční duhovka .....	135
Oční sítnice .....	138
Rozpoznání obličeje .....	139
Ověřování hlasu .....	140
<b>Další biometriky .....</b>	<b>141</b>
DNA .....	141
Dynamika pohybu myši .....	148
Ucho .....	148
<b>Shrnutí biometrik .....</b>	<b>149</b>
<b>Slovníček pojmů .....</b>	<b>152</b>
<b>Přílohy .....</b>	<b>155</b>
Příkazy programu GPG .....	155
<b>Závěr .....</b>	<b>162</b>
<b>Zdroje použitých obrázků .....</b>	<b>163</b>

