

Obsah

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

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