Předmluva vydavatele 7

Úvod 15

1 Základy kryptografie 19
1.1 Utajovací kryptosystémy 20
1.2 Autentizační kryptosystémy 22
1.3 Generátory nepředvídatelných čísel 24
1.4 Hešovací funkce 25
1.5 Diffie-Hellmanova funkce 26
1.6 Odvozovací funkce 28
1.7 Kryptografické proměnné 29
1.8 Ustavení klíčů 30

2 Přenosové systémy 35
2.1 IP sítě 35
2.2 Kryptografie v IP sítích 37
2.3 Integrované symetrické kryptosystémy 39
2.4 Kryptografie v aplikační vrstvě 40
2.4.1 Zabezpečení elektronické pošty 40
2.4.2 Protokol IKE 42
2.4.3 Protokol DNSsec 45
2.5 Kryptografie v transportní vrstvě 48
2.5.1 Protokol TLS 48
2.5.2 Protokol SSH 51
2.6 Kryptografie v síťové vrstvě 53
2.6.1 Komplex IPsec 53
2.6.2 Anonymizační síť Tor 58
2.7 Kryptografie v linkové vrstvě 68
2.7.1 Komplex WPA 69
2.7.2 Protokol MACsec 75

3 Přístupové systémy 81
3.1 Architektura přístupových systémů 81
3.2 Autentizace 84
3.3 Autentizační protokoly 87
3.3.1 Autentizace BAA a DAA 87
3.3.2 Protokol EAP 88
3.3.3 Protokol Kerberos 90
3.3.4 Protokol OpenID Connect 93
3.4 Autorizační protokoly 96
3.4.1 Protokol OAuth 96

3.5 Přístupové protokoly 99
3.5.1 Protokol RADIUS 99
3.5.2 Systémy elektronické kontroly vstupu 100

4 Platební systémy 105
4.1 Internetové bankovnictví 105
4.2 Protokol 3D Secure 106
4.3 Síť Bitcoin 109
4.4 Platební karty 117

Literatura 127