

# CONTENTS

Preface	xiii
Acknowledgements	xvii
<b>Chapter 1</b> TCP/IP Overview	1
1.1 Some History	2
1.2 TCP/IP Protocol Architecture	4
1.2.1 Data-link Layer	4
1.2.2 Network Layer	5
1.2.2.1 Internet Protocol	5
IPv4 Datagrams Format	9
IPv4 Address Classes	11
Types of IPv4 Addresses	12
Classless Interdomain Routing	12
Private IP Addresses	15
IPv6 Datagram Format	16
IPv6 Addressing	19
1.2.2.2 Internet Control Message Protocol	20
1.2.2.3 Internet Group Management Protocol	25
1.2.3 Transport Layer	25
1.2.3.1 Transmission Control Protocol	26
TCP Header Format	26
Initializing TCP Connections	28
TCP Connection States	29
1.2.3.2 User Datagram Protocol	30
UDP Header Format	30
1.2.4 Application Layer	31
<b>Chapter 2</b> Symmetric-Key Cryptography	33
2.1 Historical Perspective	34
2.2 The Data Encryption Standard	38
2.2.1 Triple DES	46
2.3 Design of Symmetric-Key Cryptosystems	46
2.3.1 Security Issues	47
2.3.2 Implementation and Performance Issues	51
2.3.3 Mode of Operation	53

2.4	The Advanced Encryption Standard	54
2.4.1	MARS	54
2.4.2	RC6	60
2.4.3	AES (Rijndael)	63
2.4.4	Serpent	68
2.4.5	Twofish	71
2.4.6	Performance Comparison of the AES Finalists	76
2.5	Other Symmetric-Key Cryptosystems	77
<b>Chapter 3</b>	<b>Public-Key Cryptosystems</b>	<b>81</b>
3.1	RSA Cryptosystem	82
3.2	ElGamal Cryptosystem	84
3.3	Elliptic Curve Cryptography	86
3.3.1	Elliptic Curve Over $\mathbb{Z}_p$	87
3.3.2	Elliptic Curve Over $\mathbb{F}_{2^n}$	88
3.3.3	Elliptic Curve Key Pairs	91
3.3.4	Security Considerations	91
3.4	Diffie-Hellman Key Exchange	93
3.4.1	Elliptic Curve Diffie-Hellman Key Exchange Scheme	94
3.5	Digital Signature	96
3.5.1	Digital Signature Algorithm	99
3.5.2	RSA Signature Scheme	100
3.5.3	Elliptic Curve Digital Signature Algorithm	101
3.6	Symmetric-Key vs Public-Key Cryptosystems	103
<b>Chapter 4</b>	<b>Hash Functions and MAC</b>	<b>105</b>
4.1	MD5 Hash Function	106
4.2	Secure Hash Algorithm (SHA-1)	109
4.3	RIPEMD-160	111
4.4	Tiger	114
4.5	Comparative Analysis	116
4.6	HMAC	117
<b>Chapter 5</b>	<b>Public-Key Infrastructure</b>	<b>119</b>
5.1	X.509 Certificates	121
5.1.1	X.509 Certificate Format	123
5.1.2	X.509 Extensions	126
5.1.3	Qualified Certificates	133

5.1.4	Qualified Certificate Extensions	134
5.1.5	Certificate Revocation List	137
5.1.6	CRL Extensions	138
5.1.7	CRL Entry Extensions	140
5.1.8	Online Certificate Status Protocol	141
5.1.9	X.509 Trust Model	145
5.2	PGP Certificates	150
5.2.1	PGP Certificate Format	150
5.2.2	Revocation of PGP Certificates	151
5.2.3	PGP Trust Model	152
5.3	Other PKI Issues	155
<b>Chapter 6</b>	<b>LDAP</b>	<b>159</b>
6.1	X.500 Directory	160
6.2	Overview of LDAP	162
6.3	LDAP/X.500 Attribute Types	164
6.4	LDAP URL Format	171
<b>Chapter 7</b>	<b>IP Security Architecture</b>	<b>175</b>
7.1	What IPSec Does	176
7.2	How IPSec Works	185
7.3	Security Association	186
7.4	Security Association Databases	186
7.4.1	Security Policy Database	187
7.4.2	Security Association Database	188
<b>Chapter 8</b>	<b>Authentication Header</b>	<b>191</b>
8.1	Authentication Header Format	193
8.2	AH Modes of Operation	195
8.2.1	AH Transport Mode	195
8.2.2	AH Tunnel Mode	199
8.3	Integrity Check Value Computation	200
8.4	AH Processing	204
<b>Chapter 9</b>	<b>Encapsulating Security Payload</b>	<b>207</b>
9.1	ESP Packet Format	209
9.2	ESP Modes	211
9.2.1	ESP Transport Mode	211

9.2.2	ESP Tunnel Mode	214
9.3	ESP Processing	216
9.3.1	Outbound Processing	216
9.3.2	Inbound Processing	218
<b>Chapter 10</b>	<b>ISAKMP</b>	<b>221</b>
10.1	ISAKMP Header Format	222
10.2	ISAKMP Payloads Formats	225
10.2.1	Generic Payload Header	226
10.2.2	Data Attributes	226
10.2.3	Security Association Payload	229
10.2.4	Proposal Payload	232
10.2.5	Transform Payload	233
10.2.6	Key Exchange Payload	236
10.2.7	Identification Payload	237
10.2.8	Certificate Payload	238
10.2.9	Certificate Request Payload	240
10.2.10	Hash Payload	241
10.2.11	Signature Payload	242
10.2.12	Nonce Payload	242
10.2.13	Notification Payload	243
10.2.14	Delete Payload	245
10.2.15	Vendor ID Payload	246
10.3	ISAKMP Negotiation Phases	247
10.4	ISAKMP Exchange Types	247
10.4.1	Base Exchange	248
10.4.2	Identity Protection Exchange	250
10.4.3	Authentication Only Exchange	251
10.4.4	Aggressive Exchange	251
10.4.5	Informational Exchange	253
<b>Chapter 11</b>	<b>Internet Key Exchange</b>	<b>255</b>
11.1	Exchange Phases	256
11.2	Exchange Modes	256
11.2.1	Main Mode	258
11.2.2	Aggressive Mode	259
11.2.3	Quick Mode	260
11.2.4	New Group Mode	261
11.3	Generation of Keying Material	262

11.4	Oakley Groups	263
11.5	Mode Config	265
11.5.1	Configuration Method Payload and Exchange	266
11.6	DHCP Configuration of IPSec Tunnel Mode in IPv4	269
11.6.1	Description of DHCP mode config	270
11.7	XAuth	273
11.7.1	Detail of XAuth Authentication Mechanism	274
11.8	Hybrid Auth	277
11.8.1	Details of Hybrid Auth Authentication Mechanism	278
<b>Chapter 12</b>	<b>IP Compression</b>	<b>281</b>
12.1	Important Considerations	282
12.2	Compressed IP Datagram Header Structure	284
12.2.1	IPv4 Header Modification	285
12.2.2	IPv6 Header Modification	286
12.3	IPComp Association	287
<b>Chapter 13</b>	<b>VPN Solutions</b>	<b>289</b>
13.1	Scenarios For VPN Utilization	290
13.1.1	Interconnecting Branch Offices	290
13.1.2	Interconnecting Different Organizations' Intranets	293
13.1.3	Securing Remote Access Via DSL or Other Broadband Alternatives	294
13.2	Choosing a VPN Solution	295
13.3	A VPN Configuration Case Study	299
13.3.1	Configuration of the PKI Server	299
13.3.2	Configuration of the VPN Gateway	311
13.3.3	Configuration of the VPN Client	321
<b>Appendix A</b>	<b>A Reference C Implementation for AES</b>	<b>327</b>
<b>Appendix B</b>	<b>A Java Implementation of AES</b>	<b>349</b>
<b>Appendix C</b>	<b>A Reference Implementation of MD5</b>	<b>373</b>
<b>Bibliography</b>		<b>383</b>
<b>Index</b>		<b>395</b>