

<b>Unit</b>	<b>Contents</b>	<b>Page No</b>
<b>Part A</b>		
<b>1</b>	<b>Planning for Security</b>	<b>1</b>
	1.1. Introduction	1
	1.2. Information Security Policy, Standards, and Practices	2
	1.3. Information Security Blueprints	13
	1.4. Planning for Security-Hybrid Framework	24
	1.5. Contingency Planning	34
<b>2</b>	<b>Security Technology-1</b>	<b>49</b>
	2.1. Introduction	49
	2.2. Physical Design	49
	2.3. Protecting Remote Connections	78
<b>3</b>	<b>Security Technology-2</b>	<b>86</b>
	3.1. Introduction	86
	3.2. Intrusion Detection Systems (IDSs)	87
	3.3. Honey Pots, Honey Nets, and Padded Cell system	123
	3.4. Scanning and Analysis Tools	127
	3.5. Access Control Devices	140
<b>4</b>	<b>Cryptography</b>	<b>147</b>
	4.1. Introduction	147
	4.2. A Short History of Cryptology	148
	4.3. Principles of Cryptography	151
	4.4. Cryptography Tools	175
	4.5. Attacks on Cryptosystems	179

## Part B

<b>5</b>	<b>Introduction to Network Security, Authentication</b>	<b>182</b>
	5.1. The OSI Security Architecture	182
	5.2. Security Attacks	183
	5.3. Security Services	186
	5.4. A Model for Network Security	189
	5.5. Internet Standards and the Internet Society	191
<b>6</b>	<b>Electronic Mail Security</b>	<b>214</b>
	6.1. Pretty Good Service (PGP)	214
	6.2. S/MIME (Secure/Multipurpose Internet Mail Extension)	229
<b>7</b>	<b>IP Security</b>	<b>245</b>
	7.1. IP Security Overview	245
	7.2. IP Security Architecture	247
	7.3. Authentication Header	252
	7.4. Encapsulating Security Payload	257
	7.5. Combining Security Associations	262
	7.6. Basic Combinations of Security Associations	264
	7.7. Key Management	265
<b>8</b>	<b>Web Security</b>	<b>274</b>
	8.1. Web Security Considerations	274
	8.2. Secure Socket Layer and Transport Layer Security	276
	8.3. Secure Electronic Transaction	292