Table of Contents

Introduction xi

Chapter 1: Fundamentals of Cyber Law 1

1.1 History of Internet 2
1.2 Introduction to Indian Cyber Law 2
Need for Cyber Laws 3
Jurisprudence of Cyber Law 3
1.3 Objective and Scope of the IT Act 2000 4
1.4 Uncitral Model Law 5
1.5 ISP Guideline 9
1.6 Intellectual property issues 13
1.7 Overview of Intellectual property related legislation in India 13
Rationale behind Intellectual Property 14
Underlying premises of IP 15
Balancing the Rights of the Owner of the IP and the Society 15
Enforcement of IPRS 15
IP and Constitution of India 16
1.8 Patent 16
The Patent System 17
Patentable Invention? 17
Nonpatentable 17
Procedure for Obtaining Patent 18
1.9 Copyright 19
1.10 Trademark law 22
1.11 Law related to semiconductor layout and design 23
Summary 24
Exercises 25
Review Questions 25
Sample Examination Questions 25

Chapter 2: E – Commerce 31

2.1 E-Commerce and its Models 32
The B2C E-Commerce 33
The B2B E-Commerce 33
The C2C E-Commerce 34
The C2B E-Commerce 34
The B2G E-Commerce 35
The G2B E-Commerce 35
The C2G E-Commerce 35
The G2C E-commerce 35
The G2E E-Commerce 36
The B2E E-Commerce 36
2.2 Generations of E-commerce 36
2.3 Advantages of E-commerce 37
E-Government 38
E-Banking 40
E-Tailing 41
2.4 EDI 43
Standards of EDI 44
Transmission Modes of EDI 44
2.5 E-Cash and E-Payment Scheme 46
E-Cash 46

Electronic payment systems 48
2.6 Business Transactions on Web or E-Transaction 49
2.7 Credit/Debit/Smart Cards 50
2.8 E-Commerce in India 51
Scope of E-Commerce in India 51
Key Factors to Attract Indian Online Customer 52
Obstacles in the Way of E-commerce in India 53
E-Commerce and the Government of India 53
2.9 Recent Trends in Shopping 54
2.10 Mobile Commerce 54
2.11 E-Marketplace Technology 56
Problem Definition 56
Research Process 57
Identifying Factors to Enter E-marketplace 57
Specifying Guidelines to Enter E-Marketplace 59
2.12 E-Agreement 59
2.13 Legal Recognition of Electronic and Digital Records 60
Legal Recognition of Digital Signatures 60
Use of Electronic Records and Digital Signatures 60
2.14 Virtual Organisation 61
Characteristics of a Virtual Organisation 61
Advantages of a Virtual Organisation 62
Disadvantages of Virtual Organisation 62
Summary 63
Exercises 63
Review Questions 63
Sample Examination Questions 64

Chapter 3: Security in E-Commerce 65

3.1 E-Commerce Issues of privacy 65
3.2 Security Threats to E – Commerce 66
3.3 Physical Security 67
Incidents of Physical Security Violations 68
Disaster and Controls 68
Basic Tenets of Physical Security 70
Challenges in Ensuring Physical Security 71
Physical Entry Controls 72
Steps to Perform after Physical Security Breach 73
3.4 Spyware Technology 73
Lock Down USB Ports 74
DeviceLock 74
Tracking Device 74
3.5 Access Control 75
Biometrics 75
Benefits, Criteria for selection of Biometrics 77
Interoperability Issues 78
Economic and Social Aspects 79
Legal Challenges 80
3.6 Digital Signatures 81
Requirements of Digital Signature System 81
Components of Digital Signature 82
Technical issues 82
Legal issues 83
Electronic Records 83
Digital Certificates 84
Applications of Digital Signatures 85

3.7 Certificate Issuance ... 85
Cardholder Certificates ... 86
Trader Certificates ... 86
Acquirer and Issuer Certificates ... 86
Summary ... 87
Exercises ... 87
Review Questions ... 87
Sample Examination Questions ... 88

Chapter 4: Investigation and Ethics ... 89
4.1 Cybercrime ... 90
4.2 Cyber/Resource Theft ... 90
4.3 Types of cyber crimes/frauds ... 91
4.4 Cyber frauds in India ... 92
4.5 Cyber jurisdiction ... 93
4.6 Dealing with cybercrime in various countries ... 93
4.7 Ethical issues in data and software privacy ... 94
Plagiarism ... 94
Pornography ... 94
Tampering computer documents /System hacking ... 94
Data privacy and protection ... 95
Software Piracy ... 96
Social Engineering and Phishing ... 96
Types of Social Engineering ... 97
Exploring Methods of Phishing ... 98
4.8 Issues in ethical hacking ... 100
4.9 Internet security threats ... 101
Hacking and Cracking ... 102
Malicious code ... 102
Viruses ... 103
Worms ... 105
Trojan Horses ... 105
4.10 Certifying authorities ... 109
Needs of certifying authority and power ... 109
Appointment ... 110
Function of controller ... 110
Generation ... 111
Suspension and Revocation of Certifying Authorities ... 112
4.11 Cyber crime forensic ... 112
Summary ... 113
Exercises ... 114
Review Questions ... 114
Sample Examination Questions ... 114

Chapter 5: Information Security ... 115
5.1 Information Systems ... 116
Computer Literacy and IS Literacy ... 117
IS Components ... 117
Trends in IS ... 119
Classification of IS ... 120
Framework of IS in an Organisation ... 122
IS and Business Organisation ... 122
Human Body as an Information System ... 123
IS Failures and Causes ... 124
5.2 Developing Information System ... 125
Waterfall Model ... 125
Prototyping Approach ... 127

Evolutionary Model 128
Spiral Model 128
Incremental Model 129
Role of Security in Internet and Web Services 129
Securing Web Services 130
5.3 Principles of Information Security 130
5.4 An Overview of Information Security Management System (ISMS) 131
Benefits of ISMS 132
5.5 Classification of Threats and Attacks 132
5.6 Security Implication for Organisations 133
Monitoring the Network 133
Understanding Intrusion Detection Systems 134
5.7 Information Classification and their Roles 135
Visibility 135
Findability 135
Security 135
Compliance 136
Roles and Responsibilities of Information Authority 136
Roles and Responsibilities of the Information Custodian / Steward 136
Roles and Responsibilities of the Information User 137
5.8 Some other terms in Information Security 137
Access control 137
Authentication of Hosts 138
Vulnerability 140
5.9 Stages of Vulnerability Management 141
Summary 143
Exercises 143
Review Questions 143
Sample Examination Questions 144

Chapter 6: Cryptography 145

6.1 Understanding Cryptography and Encryption 146
Private Key Encryption 146
Public Key Encryption 147
Secret-Key Encryption 147
6.2 Understanding Cryptographic Algorithms 148
MD5 149
SHA 149
RC4 149
RC5 149
Blowfish 149
6.3 Understanding Cryptanalysis 150
6.4 Describing Code Breaking Methodologies 150
6.5 Describing Cryptographic Attacks 151
6.6 Firewalls 151
Types of Firewall Techniques 153
How to Identify a Firewall 154
6.7 Issues in Documents Security 155
6.8 Basic concepts of Network Security 155
Sniffing 156
Sniffing Objectives 156
Protecting from Sniffing Attacks 156
6.9 Perimeters of Network protection and Network attack 157
Scoping an Attack 158
Enumerating Network 158
Querying Registrar 159

Querying Domain 160
Querying Network 160
Interrogating DNS 160
Exploring Network Reconnaissance 161
6.10 Common Attacks 162
Wiretaps 162
Eavesdropping 163
Portscan 164
6.11 Need of Intrusion Monitoring and Detection 165
Network-based IDS 166
Host-based IDS 170
6.12 Honeypot 173
Types of Honeypots 174
Placement of Honeypots 174
6.13 VPN 176
Insecure Storage of AuthenticationCredentials by VPN Clients 177
VPN Fingerprinting 177
Username Enumeration Vulnerabilities 177
Offline Password Cracking 178
Lack of Account Lockout 178
Denial of Service Attacks 178
Benefits 178
Use of Tunnelling with VPN 179
Authentication Mechanism 179
Types of VPN 180
Security Concerns in VPN 182
Summary 182
Exercises 183
Review Questions 183
Sample Examination Questions 183

Chapter 7: Networking 185

7.1 Concept of Networking 186
Need of Networking 187
Basic Components of Networks 187
Exploring the Types of Networks 188
Network Topologies 191
Advantages of Networking 195
Disadvantages of Computer Networks 197
7.2 IP Addressing and Subnetting 198
Classification of IP Addresses 199
Class A 200
Class B 200
Class C 200
Class D 200
Class E 200
Subnetting 200
7.3 Domain Name System(DNS) 201
Name Space 202
Domain Name Space 202
Concepts used in a Domain Name System 203
7.4 Protocol 205
Bootp 206
DHCP 206
HTTP 207
TCP/IP 207
Physical Layer 208

Data Link Layer 208
Network Layer 209
Transport Layer 209
SMTP and POP3 210
7.5 Services 210
Active Directory service(ADS) 211
Internet information services(IIS) 211
Windows Server Update Services (WSUS) 213
7.6 Network Address Translation (NAT) 213
Static NAT (SNAT) 214
Dynamic NAT (DNAT) 214
7.7 Server 214
Exchange Server 214
Connection oriented server 215
7.8 Internet Security and Acceleration (ISA) 215
Editions of ISA Server 215
7.9 Wireless network 216
Basics of Wireless Networking 217
Availability 217
Speed 217
Security 217
Hardware Requirements for a Wireless Network 217
Types of Wireless Networks 218
Application of Wireless Networks 219
Wireless Local Area Network 219
Wireless Wide Area Network 219
Wireless Pan Area Network 219
Bluetooth 219
Infrared Wireless Technology 221
IEEE 802.15 222
Mobile IP 223
7.10 Ethernet 223
7.11 Fiber Distributed Data Interface(FDDI) 224
7.12 Client Server Model 225
Socket Interface 226
Connectionless Iterative Server 227
7.13 Concurrency 227
7.14 Byte ordering 228
7.15 Network Socket 229
Socket states and the client-server model 229
Address Domain and Socket Types 229
Socket system calls 230
7.16 Zigbee 231
7.17 RAN 231
7.18 MANET 231
Types of MANET 232
Summary 232
Exercises 233
Review Questions 233
Sample Examination Questions 234

Examination Questions 235

Index 239