
Contents

Preface to the Third Edition	xix
Preface to the Second Edition.....	xxi
Preface to the First Edition.....	xxiii
Author.....	xxv
Acronyms.....	xxvii
1 Overview of Electronic Commerce	1
1.1 Electronic Commerce and Mobile Commerce	1
1.1.1 Examples of Business-to-Business Commerce	2
1.1.2 Examples of Business-to-Consumer Commerce	3
1.1.2.1 eBay	3
1.1.2.2 Amazon	4
1.1.2.3 Stamps.com and Neopost.....	4
1.1.3 Examples of Proximity Commerce.....	4
1.1.4 Examples of Person-to-Person (Peer-to-Peer) Commerce	4
1.2 Effects of the Internet and Mobile Networks.....	5
1.3 Network Access.....	9
1.3.1 Wireline Access	9
1.3.2 Wireless Access	9
1.4 Barcodes	10
1.5 Smart Cards	13
1.6 Parties in Electronic Commerce.....	15
1.6.1 Banks	16
1.6.2 Payment Intermediaries.....	16
1.6.2.1 Aggregators.....	17
1.6.2.2 Gateways.....	17
1.6.2.3 Payment Processors	17
1.6.2.4 Certification Authorities and Trusted Service Managers.....	17
1.6.3 Providers and Manufacturers	17
1.7 Security.....	18
1.7.1 Loss of Control	18
1.7.2 Loss of Confidentiality.....	18
1.7.3 Loss of Service.....	18
1.8 Summary.....	18
Questions	19
2 Money and Payment Systems	21
2.1 Mechanisms of Classical Money.....	21
2.2 Payment Instruments	23
2.2.1 Cash	24
2.2.2 Checks	26
2.2.3 Credit Transfers.....	29
2.2.4 Direct Debit.....	32
2.2.5 Interbank Transfers	32
2.2.6 Bills of Exchange.....	32
2.2.7 Payment Cards	33

2.3	Types of Dematerialized Monies	40
2.3.1	Electronic Money	40
2.3.2	Virtual Money	40
2.3.3	Digital Money	41
2.4	Purses, Holders, and Wallets.....	41
2.4.1	Electronic Purses and Electronic Token (Jeton) Holders.....	41
2.4.2	Virtual Purses and Virtual Jeton Holders	42
2.4.3	Digital Wallets.....	43
2.4.4	Diffusion of Electronic Purses	43
2.5	Transactional Properties of Dematerialized Currencies.....	44
2.5.1	Anonymity.....	45
2.5.2	Traceability.....	45
2.6	Overall Comparison of the Means of Payment	46
2.7	Practice of Dematerialized Money	47
2.7.1	Protocols of Systems of Dematerialized Money	47
2.7.2	Direct Payments to the Merchant.....	49
2.7.3	Payment via an Intermediary	49
2.8	Clearance and Settlement in Payment Systems.....	51
2.8.1	United States	53
2.8.2	United Kingdom	55
2.8.3	France.....	55
2.9	Drivers of Innovation in Banking and Payment Systems.....	56
2.9.1	Technical Developments	56
2.9.2	Business Needs.....	57
2.9.3	User Preferences.....	57
2.9.4	Legislation and Regulation	58
2.9.5	Standards	58
2.9.6	Ideology.....	59
2.10	Summary.....	59
	Questions	59
3	Algorithms and Architectures for Security	61
3.1	Security of Open Financial Networks	61
3.2	OSI Model for Cryptographic Security.....	62
3.2.1	OSI Reference Model	62
3.2.2	Security Services: Definitions and Location	62
3.3	Security Services at the Link Layer	63
3.4	Security Services at the Network Layer.....	64
3.5	Security Services at the Application Layer.....	66
3.6	Message Confidentiality	67
3.6.1	Symmetric Cryptography	67
3.6.2	Public Key Cryptography	67
3.7	Data Integrity.....	69
3.7.1	Verification of the Integrity with a One-Way Hash Function	69
3.7.2	Verification of the Integrity with Public Key Cryptography	71
3.7.3	Blind Signature.....	71
3.7.4	Verification of the Integrity with Symmetric Cryptography.....	72
3.8	Identification of the Participants.....	74
3.9	Biometric Identification	74
3.9.1	Fingerprint Recognition.....	75
3.9.2	Iris Recognition	76
3.9.3	Face Recognition	77
3.9.4	Voice Recognition	78
3.9.5	Signature Recognition.....	78

- 3.9.6 Keystroke Recognition 79
- 3.9.7 Hand Geometry 79
- 3.9.8 Retinal Recognition 79
- 3.9.9 Additional Standards 79
- 3.9.10 Summary and Evaluation 80
- 3.10 Authentication of the Participants 81
- 3.11 Access Control 82
- 3.12 Denial of Service 83
- 3.13 Nonrepudiation 85
 - 3.13.1 Time Stamping and Sequence Numbers 85
- 3.14 Secure Management of Cryptographic Keys 86
 - 3.14.1 Production and Storage 86
 - 3.14.2 Distribution 86
 - 3.14.3 Utilization, Withdrawal, and Replacement 86
 - 3.14.4 Key Revocation 87
 - 3.14.5 Deletion, Backup, and Archiving 87
 - 3.14.6 A Comparison between Symmetric and Public Key Cryptography 87
- 3.15 Exchange of Secret Keys: Kerberos 87
 - 3.15.1 Message (1): Request of a Session Ticket 88
 - 3.15.2 Message (2): Acquisition of a Session Ticket 88
 - 3.15.3 Message (3): Request of a Service Ticket 89
 - 3.15.4 Message (4): Acquisition of the Service Ticket 89
 - 3.15.5 Message (5): Service Request 89
 - 3.15.6 Message (6): Optional Response of the Server 89
- 3.16 Public Key Kerberos 90
 - 3.16.1 Where to Find Kerberos? 90
- 3.17 Exchange of Public Keys 90
 - 3.17.1 The Diffie–Hellman Exchange 90
 - 3.17.2 Internet Security Association and Key Management Protocol 91
- 3.18 Certificate Management 92
 - 3.18.1 Basic Operation 94
 - 3.18.2 Description of an X.509 Certificate 94
 - 3.18.3 Attribute Certificates 95
 - 3.18.4 Certification Path 95
 - 3.18.5 Hierarchical Certification Path 97
 - 3.18.6 Distributed Trust Model 98
 - 3.18.7 Certificate Classes 98
 - 3.18.8 Certificate Revocation 99
 - 3.18.9 Archival 99
 - 3.18.10 Recovery 100
 - 3.18.11 Banking Applications 100
- 3.19 Authentication 100
 - 3.19.1 Procedures for Strong Authentication 100
 - 3.19.1.1 One-Way Authentication 100
 - 3.19.1.2 Two-Way Authentication 101
 - 3.19.1.3 Three-Way Authentication 101
- 3.20 Security Cracks 101
 - 3.20.1 Problems with Certificates 102
 - 3.20.2 Underground Markets for Passwords 102
 - 3.20.3 Encryption Loopholes 103
 - 3.20.4 Phishing, Spoofing, and Pharming 104
- 3.21 Summary 106
- 3A Appendix: Principles of Symmetric Encryption 106
 - 3A.1 Block Encryption Modes of Operation 106

3A.2	Examples of Symmetric Block Encryption Algorithms	112
3A.2.1	DES and Triple DES.....	112
3A.2.2	AES	113
3A.2.3	RC4	114
3A.2.4	New European Schemes for Signature, Integrity, and Encryption	114
3A.2.5	eSTREAM	114
3A.2.6	IDEA.....	115
3A.2.7	SKIPJACK	115
3B	Appendix: Principles of Public Key Encryption.....	115
3B.1	RSA.....	115
3B.1.1	Chosen-Ciphertext Attacks.....	115
3B.1.2	Practical Considerations.....	116
3B.2	Public Key Cryptography Standards	116
3B.3	PGP and OpenPGP	117
3B.4	Elliptic Curve Cryptography.....	117
3C	Appendix: Principles of the Digital Signature Algorithm and the Elliptic Curve Digital Signature Algorithm	118
	Questions	119
4	Business-to-Business Commerce.....	121
4.1	Drivers for Business-to-Business Electronic Commerce	121
4.1.1	Progress in Telecommunications and Information Processing	121
4.1.2	Globalization	121
4.1.3	Quest for Organizational Agility	122
4.1.4	Personalization of Products and Services	122
4.1.5	The Legal Environment and Regulatory Compliance	122
4.2	Four Stages of Systems Integration	123
4.2.1	Interconnectivity	123
4.2.2	Functional Interoperability	123
4.2.3	Semantic Interoperability	124
4.2.4	Optimization and Innovation	124
4.3	Overview of Business-to-Business Commerce	124
4.4	Short History of Business-to-Business Electronic Commerce.....	126
4.5	Examples of Business-to-Business Electronic Commerce.....	126
4.5.1	Banking Applications.....	126
4.5.2	Aeronautical Applications.....	127
4.5.3	Applications in the Automotive Industry	127
4.5.4	Other Industries.....	128
4.6	Evolution of Business-to-Business Electronic Commerce.....	128
4.7	Implementation of Business-to-Business Electronic Commerce.....	129
4.8	X12 and EDIFACT	130
4.8.1	Definitions.....	131
4.8.2	ANSI X12	131
4.8.3	EDIFACT.....	132
4.8.3.1	UNB/UNZ and UIB/UIZ Segments	132
4.8.3.2	UNH/UNT Segments.....	133
4.8.3.3	The UNS Segment	133
4.8.3.4	UNG/UNE Segments.....	133
4.8.3.5	UNO/UNP Segments.....	133
4.8.3.6	Structure of an Interchange.....	134
4.8.3.7	A Partial List of EDIFACT Messages.....	134
4.8.3.8	Interactive EDIFACT	134
4.8.4	Structural Comparison between X12 and EDIFACT	135

- 4.9 EDI Messaging..... 135
 - 4.9.1 X.400..... 135
 - 4.9.2 The Internet (SMTP/MIME)..... 136
- 4.10 The Security of EDI..... 137
 - 4.10.1 X12 Security 137
 - 4.10.2 EDIFACT Security..... 137
 - 4.10.2.1 Security of EDIFACT Documents Using In-Band Segments 138
 - 4.10.2.2 Security of EDIFACT Documents with Out-of-Band Segments: The AUTACK Message..... 140
 - 4.10.3 Protection of EDI Messages in Internet Mail 142
 - 4.10.4 Protocol Stacks for EDI Messaging 142
- 4.11 Integration of XML and Traditional EDI 143
 - 4.11.1 BizTalk® 143
 - 4.11.2 xCBL..... 144
 - 4.11.3 UBL 144
- 4.12 New Architectures for Business-to-Business Electronic Commerce..... 144
- 4.13 Electronic Business (Using) Extensible Markup Language 146
 - 4.13.1 Architecture of ebXML 146
 - 4.13.2 Business Scenarios 146
 - 4.13.3 Core Components 147
 - 4.13.4 Registry and Repository 148
 - 4.13.5 CPPA 148
 - 4.13.6 Message Service Specification..... 148
 - 4.13.7 ebXML Operations..... 148
- 4.14 Web Services 149
 - 4.14.1 Web Services Standards..... 150
 - 4.14.2 Web Services Description Language 151
 - 4.14.3 Universal Description, Discovery, and Integration 151
 - 4.14.4 Simple Object Access Protocol 151
 - 4.14.5 Security..... 151
 - 4.14.6 Standardization of Web Services..... 153
- 4.15 Relation of EDI with Electronic Funds Transfer..... 153
 - 4.15.1 Funds Transfer with EDIFACT 155
 - 4.15.2 Fund Transfers with X12..... 156
 - 4.15.3 Financial Dialects of XML 156
 - 4.15.4 Electronic Billing..... 157
 - 4.15.5 An Example for EDI Integration with Business Processes 158
- 4.16 Summary 159
- Questions 160

- 5 Transport Layer Security and Secure Sockets Layer..... 161**
 - 5.1 Architecture of SSL/TLS..... 161
 - 5.2 SSL/TLS Security Services 161
 - 5.2.1 Authentication..... 162
 - 5.2.2 Confidentiality 163
 - 5.2.3 Integrity..... 164
 - 5.2.4 Summary of Security Algorithms..... 164
 - 5.2.5 TLS Cryptographic Vulnerabilities 164
 - 5.2.5.1 Initialization Vector Attack (BEAST Attack)..... 165
 - 5.2.5.2 The RC4 Statistical Bias Attack..... 165
 - 5.2.5.3 Forging X.509 Certificates 165
 - 5.3 SSL/TLS Subprotocols..... 165
 - 5.3.1 SSL/TLS Exchanges..... 166

5.3.2	State Variables of an SSL/TLS Session.....	166
5.3.3	State Variables for an SSL/TLS Connection.....	167
5.3.4	Synopsis of Parameters Computation.....	167
5.3.5	The Handshake Protocol	168
5.3.5.1	General Operation.....	168
5.3.5.2	Opening a New Session	168
5.3.5.3	Authentication of the Server.....	171
5.3.5.4	Exchange of Secrets.....	172
5.3.5.5	Key Derivation for SSL	172
5.3.5.6	Key Derivation for TLS.....	173
5.3.5.7	Exchange Verification	174
5.3.5.8	Verification and Confirmation by the Server	174
5.3.6	The ChangeCipherSpec Protocol.....	175
5.3.7	Record Protocol	175
5.3.8	Connection Establishment.....	176
5.3.9	Renegotiation or Rehandshake.....	178
5.3.10	The Alert Protocol.....	181
5.3.10.1	The Bleichenbacher Attack	182
5.3.10.2	Padding Attacks	183
5.3.11	Denial-of-Service Attacks	183
5.4	Performance of SSL/TLS.....	185
5.5	Implementation Pitfalls	185
5.6	Summary	187
	Questions	188
6	Wireless Transport Layer Security.....	189
6.1	Architecture.....	189
6.2	From TLS to WTLS.....	189
6.2.1	Identifiers and Certificates	190
6.2.2	Cryptographic Algorithms.....	191
6.2.3	Handshake Messages and Exchanges	192
6.2.4	Calculation of Secrets.....	193
6.2.4.1	Computation of the PreMasterSecret	193
6.2.4.2	Computation of MasterSecret.....	193
6.2.5	Alert Messages	194
6.3	Operational Constraints.....	194
6.3.1	Positioning of the WAP/Web Gateway.....	194
6.3.2	ITLS.....	196
6.3.3	NAETEA.....	196
6.4	WAP 2.0 and TLS Extensions	198
6.5	WAP Browsers	199
6.6	Summary.....	199
	Questions	201
7	The SET Protocol	203
7.1	SET Architecture	203
7.2	Security Services of SET.....	204
7.2.1	Cryptographic Algorithms.....	205
7.2.2	Dual Signature	207
7.3	Certification	208
7.3.1	Certificate Management.....	208
7.3.2	Registration of the Participants	209
7.3.2.1	Cardholder Registration.....	209
7.3.2.2	Merchant's Registration.....	212

- 7.4 Purchasing Transaction..... 213
 - 7.4.1 SET Payment Messages..... 213
 - 7.4.2 Transaction Progress..... 213
 - 7.4.2.1 Initialization..... 213
 - 7.4.2.2 Order Information and Payment Instructions..... 214
 - 7.4.2.3 Authorization Request..... 216
 - 7.4.2.4 Granting Authorization..... 218
 - 7.4.2.5 Capture..... 220
- 7.5 Optional Procedures..... 220
- 7.6 Efforts to Promote SETs..... 221
 - 7.6.1 SET Reference Implementation (SETFEF) and Conformance Tests..... 221
 - 7.6.2 SETs and Integrated Circuit Cards..... 221
 - 7.6.3 Hybrid TLS/SET Architecture..... 222
 - 7.6.3.1 3D SET..... 222
 - 7.6.3.2 SET Fácil..... 223
- 7.7 SET versus TLS/SSL..... 223
- 7.8 Summary..... 224
- Questions..... 225

- 8 Payments with Magnetic Stripe Cards..... 227**
 - 8.1 Point-of-Sale Transactions..... 227
 - 8.2 Communication Standards for Card Transactions..... 230
 - 8.3 Security of Point-of-Sale Transactions..... 231
 - 8.3.1 PCI Standards..... 231
 - 8.3.2 Point-to-Point Encryption..... 232
 - 8.3.3 Point-of-Sale Fraud..... 232
 - 8.4 Internet Transactions..... 233
 - 8.4.1 Screening for Risks..... 234
 - 8.4.2 Online Security Code..... 235
 - 8.4.3 Perishable Card Numbers..... 235
 - 8.4.4 One-Time Passwords..... 236
 - 8.4.5 Online Fraud in North America..... 237
 - 8.5 3-D Secure..... 238
 - 8.5.1 Enrollment..... 239
 - 8.5.2 Purchase and Payment Protocol..... 240
 - 8.5.3 Clearance and Settlement..... 241
 - 8.5.4 Security..... 241
 - 8.5.5 Evaluation..... 242
 - 8.6 Migration to EMV..... 243
 - 8.7 Summary..... 244
 - Questions..... 245

- 9 Secure Payments with Integrated Circuit Cards..... 247**
 - 9.1 Description of Integrated Circuit Cards..... 247
 - 9.1.1 Memory Types..... 247
 - 9.1.2 Processing Capabilities..... 248
 - 9.1.3 Operating Systems..... 248
 - 9.1.4 Integrated Circuit Cards with Contacts..... 248
 - 9.1.5 Contactless Integrated Circuit Cards..... 249
 - 9.2 Integration of Smart Cards with Computer Systems..... 249
 - 9.2.1 OpenCard Framework..... 250
 - 9.2.2 PC/SC..... 250
 - 9.2.3 Movement for the Use of Smart Cards in a Linux Environment..... 251
 - 9.2.4 Financial Transactional IC Card Reader (FINREAD)..... 251

9.3	Standards for Integrated Circuit Cards	252
9.3.1	ISO Standards for Integrated Circuit Cards	252
9.3.2	ISO Standards for Contactless Cards	253
9.3.2.1	Anticollision Protocols	253
9.3.2.2	Type A Anticollision Protocol	254
9.3.2.3	Type B Anticollision Protocol	254
9.3.3	RFID Standards	254
9.3.3.1	ISO Standards	255
9.3.3.2	EPCglobal®	255
9.3.3.3	Open Specifications	257
9.3.3.4	Privacy Concerns	257
9.3.4	Near-Field Communication Standards	257
9.3.5	File System of Integrated Circuits Cards	258
9.3.5.1	Swedish Electronic Identity Card	259
9.3.5.2	Subscriber Identity Module of GSM Terminals	259
9.4	Multiapplication Smart Cards	261
9.4.1	Management of Applications in Multiapplication Cards	261
9.4.1.1	Secondary Applications Controlled by the Primary Application	261
9.4.1.2	Federation of Several Applications under a Central Authority	261
9.4.1.3	Independent Multiapplications	262
9.4.2	Java Virtual Machine	263
9.5	Security of Integrated Circuit Cards	263
9.5.1	Security during Production	263
9.5.2	Physical Security of the Card during Usage	265
9.5.3	Logical Security of the Card during Usage	265
9.5.3.1	Authentication with Symmetric Encryption	266
9.5.3.2	Authentication with Public Key Encryption	266
9.6	Payment Applications of Integrated Circuit Cards	267
9.6.1	Historical Smart Card of French Banks	267
9.6.2	Speedpass	268
9.6.3	Toll Collection Systems	268
9.6.3.1	Subscription	268
9.6.3.2	Virtual Purse	268
9.6.3.3	Security	269
9.6.3.4	Interoperability	269
9.7	EMV® Card	269
9.7.1	EMV Cryptography	270
9.7.1.1	Static Data Authentication	270
9.7.1.2	Dynamic Data Authentication	271
9.7.1.3	Combined Dynamic Data Authentication	271
9.7.2	EMV Operation	272
9.7.2.1	Offline Authorization	272
9.7.2.2	Online Authorization	274
9.7.3	EMV Limitations	276
9.7.4	EMV Tokenization	276
9.7.5	Other Attacks on EMV	277
9.7.5.1	Attacks Due to Backward Compatibility	277
9.7.5.2	Man-in-the-Middle Attacks	278
9.7.5.3	Relay Attacks	278
9.8	General Consideration on the Security of Smart Cards	280
9.8.1	Physical (Destructive) Attacks	280
9.8.2	Logical (Noninvasive) Attacks	280
9.8.3	Attacks against the Chip-Reader Communication Channel	280

9.8.4	Relay Attacks on Contactless Cards.....	281
9.9	Summary.....	282
	Questions.....	282
10	Mobile Payments.....	283
10.1	Reference Model for Mobile Commerce.....	283
10.1.1	Bank-Centric Model.....	284
10.1.2	Mobile Operator–Centric Model.....	284
10.1.3	Third-Party Service Provider Model.....	284
10.1.4	Collaborative Model.....	284
10.1.5	Manufacturer–Centric Model.....	285
10.2	Secure Element in Mobile Phones.....	285
10.2.1	Option 1.....	285
10.2.2	Option 2.....	286
10.2.3	Option 3.....	286
10.2.4	Option 4.....	286
10.2.5	Option 5.....	286
10.2.6	Option 6.....	286
10.2.7	Near-Field Communication Terminals.....	286
10.2.8	Java™ 2 Platform Micro Edition.....	286
10.2.9	Unauthorized Access to the Secure Element.....	287
10.2.10	User Authentication.....	287
10.3	Barcodes.....	287
10.4	Bluetooth.....	288
10.4.1	Highlights of Bluetooth History.....	289
10.4.2	Security of Bluetooth.....	290
10.5	Near-Field Communication.....	291
10.5.1	Tag Types.....	291
10.5.2	Operating Modes.....	291
10.5.3	Transaction Authorization.....	293
10.5.4	Security of NFC Communications.....	294
10.5.4.1	Spoofing of NFC Tags.....	295
10.5.4.2	Relay Attacks.....	295
10.6	Text Messages.....	296
10.6.1	Short Message Service.....	296
10.6.2	SIM Application Toolkit (STK/SAT/USIM).....	296
10.6.3	Unstructured Supplementary Service Data.....	296
10.6.4	Over-the-Air Application Provisioning.....	296
10.7	Bank-Centric Offers.....	297
10.8	Mobile Operator–Centric Offers.....	297
10.8.1	Offers in Industrialized Countries.....	297
10.8.1.1	Paieiment CB sur Mobile.....	297
10.8.1.2	QuickTap.....	297
10.8.1.3	Softcard (ISIS) Mobile Wallet.....	298
10.8.2	M-PESA.....	298
10.9	Third-Party Service Offers.....	298
10.9.1	Apple Pay and Passbook.....	298
10.9.2	Deutsche Bahn’s “Touch and Travel”.....	299
10.9.3	Google Wallet.....	299
10.9.3.1	Account Activation.....	300
10.9.3.2	Payment and Compensation.....	300
10.9.3.3	Revenue Sources.....	300
10.9.3.4	Security.....	300

10.9.4	Paybox.....	301
10.9.4.1	Purchase Payments	301
10.9.4.2	Person-to-Person Transactions	302
10.9.4.3	Business Model.....	302
10.9.4.4	Additional Privacy Measure.....	302
10.10	Collaborative Offers.....	302
10.10.1	Mobito.....	302
10.10.2	Mpass.....	302
10.10.3	Pay2Me	303
10.11	Payments from Mobile Terminals	303
10.11.1	iZettle.....	303
10.11.2	Payleven.....	303
10.11.3	Paym	304
10.11.4	Square.....	304
10.11.5	Starbucks Card Mobile.....	304
10.11.6	Zoosh	305
10.12	Summary.....	305
	Questions	305
11	Micropayments	307
11.1	Characteristics of Micropayment Systems	307
11.1.1	Prepayment.....	307
11.1.2	Offline Authorization.....	307
11.1.3	Aggregation of Transactions	308
11.1.4	Reduced Computational Intensity.....	308
11.1.5	Routing through the ACH Network	308
11.1.6	Management of Micropayments.....	308
11.2	Standardization Efforts	308
11.2.1	Common Electronic Purse Specifications	308
11.2.1.1	Authentication of the Purse by the Issuer	309
11.2.1.2	Loading of Value	309
11.2.1.3	Point-of-Sale Transactions.....	309
11.2.2	GlobalPlatform	309
11.2.3	Electronic Commerce Modeling Language	310
11.3	Electronic Purses.....	310
11.3.1	Advantis	310
11.3.2	FeliCa	311
11.3.3	GeldKarte.....	311
11.3.3.1	Registration and Loading of Value.....	311
11.3.3.2	Payment	312
11.3.3.3	Security	313
11.3.4	Proton	314
11.4	Online Micropayments	315
11.4.1	The First Generation.....	315
11.4.1.1	First Virtual.....	315
11.4.1.2	KLELine.....	316
11.4.1.3	ClickandBuy.....	316
11.4.1.4	Bankpass Web.....	317
11.4.2	The Second Generation	317
11.4.2.1	Pay per Click	317
11.4.2.2	Payment Kiosks	317
11.4.2.3	Prepaid Cards	318
11.4.2.4	Virtual Purses.....	319
11.4.3	The Third Generation.....	320

11.5	Research Projects.....	320
11.5.1	Millicent	320
11.5.1.1	Secrets	321
11.5.1.2	Description of the Scrip.....	321
11.5.1.3	Registration and Loading of Value	322
11.5.1.4	Purchase	323
11.5.1.5	Evaluation.....	323
11.5.2	NetBill.....	324
11.5.2.1	Registration and Loading of Value	325
11.5.2.2	Purchase	325
11.5.2.3	Financial Settlement	328
11.5.2.4	Evaluation.....	328
11.5.3	PayWord	328
11.5.3.1	Registration and Loading of Value	329
11.5.3.2	Purchase	329
11.5.3.3	Financial Settlement	330
11.5.3.4	Computational Load.....	331
11.5.3.5	Evaluation.....	331
11.5.4	MicroMint	331
11.5.4.1	Registration and Loading of Value	332
11.5.4.2	Purchase	332
11.5.4.3	Financial Settlement	332
11.5.4.4	Security	332
11.5.5	Evaluation of the Research Projects for Online Micropayments	333
11.6	Market Response to Micropayment Systems.....	333
11.7	Summary.....	335
	Questions	335
12	PayPal	337
12.1	Evolution of PayPal	337
12.2	Individual Accounts	338
12.2.1	Payment with Credit Cards.....	339
12.2.2	Payment with PayPal Account Balance	339
12.2.3	Payment with Bank Accounts.....	342
12.2.4	Mobile Payments.....	342
12.2.5	Fraud Prevention.....	342
12.3	Business Accounts.....	343
12.3.1	Merchant Registration.....	343
12.3.2	Hosted Services.....	344
12.3.3	Mobile Point-of-Sale Terminals.....	344
12.4	Summary.....	345
	Questions	345
13	Digital Money	347
13.1	Privacy with Cash and Digital Money.....	347
13.2	DigiCash (eCash).....	348
13.2.1	Registration.....	348
13.2.2	Loading of Value	349
13.2.3	Purchase	349
13.2.4	Financial Settlement.....	350
13.2.5	Delivery	350
13.3	Anonymity and Untraceability in DigiCash.....	350
13.3.1	Case of the Debtor (Buyer) Untraceability	350
13.3.1.1	Loading of Value	350

13.3.1.2	Purchase	351
13.3.1.3	Deposit and Settlement	351
13.3.1.4	Improvement of Protection	351
13.3.2	Case of the Creditor (Merchant) Untraceability	351
13.3.3	Mutual Untraceability	352
13.4	Splitting of Value	352
13.5	Detection of Counterfeit (Multiple Spending)	354
13.5.1	Loading of Value	354
13.5.2	Purchasing	355
13.5.3	Financial Settlement and Verification	355
13.5.4	Proof of Double Spending	355
13.6	Evaluation of DigiCash	355
	Questions	356
14	Bitcoin and Cryptocurrencies	357
14.1	Background	357
14.2	Bitcoin Protocol	359
14.2.1	Bitcoin Nodes	360
14.2.2	Bitcoin Wallets	361
14.2.3	Blockchain	363
14.2.4	Mining	364
14.2.5	Proof-of-Work Algorithm	365
14.2.6	Adjustment of the Difficulty	366
14.2.7	Hashing Race	367
14.2.8	Mining Pools	367
14.3	Operation	368
14.3.1	Getting Bitcoins	368
14.3.2	Bitcoin Address	370
14.3.3	Key Formats	371
14.3.4	Bitcoin Transaction	372
14.3.5	Orphaned Blocks	374
14.3.6	Anonymity	375
14.3.7	Point-of-Sale Applications	378
14.3.8	Double Spending	378
14.3.9	The Protocol Evolution	378
14.4	Risk Evaluation	379
14.4.1	Limited Supply	379
14.4.2	Loss, Theft, and Irreversibility	380
14.4.3	Volatility	380
14.4.4	Opacity	381
14.4.5	Lack of Independent Review	381
14.4.6	Unknown Software Risks	382
14.4.7	Energy Consumption	382
14.4.8	Regulations	383
14.5	Summary and Conclusions	384
14A	Appendix: The Crypto Anarchist Manifesto	384
14B	Appendix: Bitcoin as a Social Phenomenon	385
14B.1	Anarcho-Libertarian Response to the Social and Political Environment	386
14B.2	Bitcoin Religion	386
14C	Appendix: Other Significant Cryptocurrencies	387
14C.1	Ripple	388
14C.2	Litecoin	388
14C.3	Dash (Darkcoin)	389
14C.4	BitShares	389

14C.5 Dogecoin	390
14C.6 Stellar	390
14C.7 Nxt.....	390
14C.8 MaidSafeCoin.....	390
14C.9 Paycoin.....	391
14D Appendix: Service Offers Based on Bitcoin	391
14D.1 Bitmessage.....	391
14D.2 Bitnotar	391
14D.3 Blocktrace	391
14D.4 ChronoBit	391
14D.5 CoinSpark.....	391
14D.6 Namecoin	391
Questions	392
15 Dematerialized Checks	393
15.1 Processing of Paper Checks.....	393
15.2 Dematerialized Processing of Checks	393
15.2.1 Electronic Check Presentment (Check Truncation)	394
15.2.2 Check Imaging	395
15.2.3 ICL File Structure.....	396
15.2.4 Remote Deposit Capture.....	396
15.3 Virtual Checks.....	397
15.3.1 Representation of eChecks	397
15.3.2 Payment and Settlement with eChecks.....	398
15.4 Summary.....	402
Questions	402
16 Electronic Commerce in Society.....	403
16.1 Harmonization of Communication Interfaces.....	403
16.2 Governance of Electronic Money.....	404
16.3 Protection of Intellectual Property	405
16.4 Electronic Surveillance and Privacy.....	406
16.4.1 Disclosure of Personal Information Online.....	406
16.4.2 Data Breaches	407
16.4.3 Monetizing Personal Data	407
16.4.4 Government Spying	409
16.4.5 Technologies for Privacy Protection.....	410
16.5 Content Filtering and Censorship	411
16.6 Taxation of Electronic Commerce.....	411
16.7 Trust Promotion	412
16.8 Archives Dematerialization.....	412
16.9 Summary.....	413
Questions	414
References	415
Websites	441