



Beginning

Cryptography with Java™

David Hook



Contents

Acknowledgments	ix
Introduction	xxvii
Chapter 1: The JCA and the JCE	1
Basic Architecture	1
Provider Signing	4
Jurisdiction Policy Files	4
Installing the Unrestricted Policy Files	4
Troubleshooting Other Issues	7
How Do You Know the Policy Files Really Behave as Sun Says They Do?	7
Installing the Bouncy Castle Provider	7
Installing by Configuring the Java Runtime	8
Install the JAR File Containing the Provider	8
Enable the Provider by Adding It to the java.security File	8
Installing During Execution	10
How Provider Precedence Works	10
Examining the Capabilities of a Provider	12
Summary	13
Exercises	14
Chapter 2: Symmetric Key Cryptography	15
A First Example	15
A Basic Utility Class	16
The SecretKeySpec Class	19
The Cipher Class	19
Cipher.getInstance()	19
Cipher.init()	20
Cipher.update()	20
Cipher.doFinal()	20
Symmetric Block Cipher Padding	21
PKCS #5/PKCS #7 Padding	21
Other Padding Mechanisms	24

Symmetric Block Cipher Modes	24
ECB Mode	25
CBC Mode	26
Inline IVs	28
Creating an IV	30
Random IVs	31
Creating a SecureRandom Object	31
Pseudorandom IVs	32
A Look at Cipher Parameter Objects	34
The AlgorithmParameters Class	34
CTS Mode: A Special Case of CBC	34
Streaming Symmetric Block Cipher Modes	35
CTR Mode	35
OFB Mode	37
CFB Mode	38
Symmetric Stream Ciphers	39
Generating Random Keys	40
The Key Interface	42
Key.getAlgorithm()	42
Key.getEncoded()	42
Key.getFormat()	42
The KeyGenerator Class	42
KeyGenerator.getInstance()	43
KeyGenerator.init()	43
KeyGenerator.generateKey()	43
Password-Based Encryption	43
Basic PBE	44
The Password	45
The Salt	45
The Iteration Count	45
PBE in the JCE	45
The PBEPParameterSpec Class	48
The PBEKeySpec Class	48
The SecretKeyFactory Class	48
Key Wrapping	50
Doing Cipher-Based I/O	52
Summary	55
Exercises	55

Chapter 3: Message Digests, MACs, and HMACs	57
Getting Started	57
The Problem of Tampering	60
Message Digests	62
The MessageDigest Class	64
MessageDigest.update()	65
MessageDigest.digest()	65
MessageDigest.isEqual()	65
Tampering with the Digest	66
MACs Based on Digests — the HMAC	68
The Mac Class	71
Mac.init()	71
Mac.update()	71
Mac.doFinal()	71
MACs Based on Symmetric Ciphers	72
Digests in Pseudorandom Functions	73
PBE Key Generation	74
Mask Generation	77
Doing Digest-Based I/O	79
Summary	81
Exercises	82
Chapter 4: Asymmetric Key Cryptography	83
Getting Started	84
The PublicKey and PrivateKey Interfaces	85
The RSA Algorithm	85
The KeyFactory Class	88
RSAPublicKeySpec and RSAPublicKey	88
RSAPrivateKeySpec and RSAPrivateKey	89
Creating Random RSA Keys	89
The KeyPair Class	90
The KeyPairGenerator Class	91
The RSAKeyGenParameterSpec Class	91
Improving RSA Performance	91
Chinese Remainder Theorem	92
RSAPrivateCrtKeySpec and RSAPrivateCrtKey	92
Multi Prime Chinese Remainder Theorem	93

Contents

RSA Padding Mechanisms	93
PKCS #1 V1.5 Padding	94
OAEP Padding	96
Wrapping RSA Keys	101
Secret Key Exchange	103
Key Agreement	106
The Diffie-Hellman Algorithm	106
The DHPParameterSpec Class	109
Specification Objects for Diffie-Hellman Keys	109
Interfaces for Diffie-Hellman Keys	110
Diffie-Hellman with Elliptic Curve	110
ECField, ECFieldFp, and ECFieldF2m	112
The EllipticCurve Class	113
The ECPoint Class	113
The ECParameterSpec Class	113
The ECGenParameterSpec Class	114
Elliptic Curve Cryptography Before JDK 1.5	115
Diffie-Hellman for More Than Two Parties	115
The El Gamal Algorithm	116
The AlgorithmParameterGenerator Class	118
AlgorithmParameterGenerator.init()	118
AlgorithmParameterGenerator.generateParameters()	118
The DHGenParameterSpec Class	120
Digital Signatures	121
The Signature Class	121
Using the Signature Class in Signature Creation Mode	121
Using the Signature Class in Signature Verification Mode	122
Signature.setParameter() and Signature.getParameters()	122
The Digital Signature Algorithm	122
Regular DSA	123
Elliptic Curve DSA	127
RSA-Based Signature Algorithms	128
PKCS #1 1.5 Signatures	129
PSS Signatures	130
Summary	132
Exercises	133
Chapter 5: Object Description in Cryptography Using ASN.1	135
What Is ASN.1?	135
Getting Started	136

Basic ASN.1 Syntax	136
Comment Syntax	137
Object Identifiers	137
The Module Structure	138
ASN.1 Types	140
Simple Types	140
Bit String Types	141
Character String Types	142
Structured Types	143
Type Annotations	144
Tagging	144
EXPLICIT Tagging	146
IMPLICIT Tagging	147
AUTOMATIC Tagging	148
CHOICE	148
CLASS	149
Encoding Rules	150
BER Encoding	150
The Primitive Definite-Length Method	151
The Constructed Definite-Length Method	151
The Constructed Indefinite-Length Method	152
DER Encoding	152
The Bouncy Castle ASN.1 API	153
Creating the Basic ASN.1 Types	154
Dealing with Tagging	155
Defining Your Own Objects	156
Analyzing an Unknown Encoded Object	162
Using ASN.1 in Java: Some Real Examples	164
Some Basic ASN.1 Structures	164
The AlgorithmIdentifier Structure	164
The Attribute Structure	165
Encoding an IV	165
Inside a PKCS #1 V1.5 Signature	166
Encoding PSS Signature Parameters	169
Encoding Public and Private Keys	171
The X509EncodedKeySpec Class	171
The PKCS8EncodedKeySpec Class	174
The EncryptedPrivateKeyInfo Class	176
Summary	181
Exercises	182

Chapter 6: Distinguished Names and Certificates	183
Getting Started	184
Distinguished Names	184
The X500Principal Class	186
X500Principal.getEncoded()	186
X500Principal.getName()	186
Public Key Certificates	187
The Certificate Class	187
Certificate.getType()	187
Certificate.getPublicKey()	188
Certificate.verify()	188
Certificate.getEncoded()	188
X.509 Certificates	188
The X509Certificate Class	189
X509Certificate.getTBSCertificate()	189
X509Certificate.getVersion()	190
X509Certificate.getSerialNumber()	190
X509Certificate.getIssuerX500Principal()	191
X509Certificate.getNotBefore() and X509Certificate.getNotAfter()	191
X509Certificate.checkValidity()	192
X509Certificate.getSubjectX500Principal()	192
X509Certificate.getIssuerUniqueID()	192
X509Certificate.getSubjectUniqueID()	192
X509Certificate.getSignature()	193
X509Certificate.getSigAlgOID(), and X509Certificate.getSigAlgParams()	193
X509Certificate.getSigAlgName()	193
X.509 Extensions	195
The X509Extension Interface	196
X509Extension.getCriticalExtensionsOIDs()	197
X509Extension.getExtensionValue()	197
X509Extension.getNonCriticalExtensionOIDs()	197
X509Extension.hasUnsupportedCriticalExtension()	197
Extensions Supported Directly by X509Certificate	198
X509Certificate.getKeyUsage()	198
X509Certificate.getSubjectAlternativeNames()	199
X509Certificate.getIssuerAlternativeNames()	200
X509Certificate.getBasicConstraints()	200
X509Certificate.getExtendedKeyUsage()	200
Reading and Writing Certificates	204
The CertificateFactory Class	204
CertificateFactory.generateCertificate()	204
CertificateFactory.generateCertificates()	204

Certification Requests	208
Writing a Simple Certificate Authority	214
Certificate Paths and Stores	219
The CertPath Class	219
CertPath.getType()	220
CertPath.getCertificates()	220
CertPath.getEncoded()	220
CertPath.getEncodings()	220
The CertStore Class	221
The X509CertSelector Class	222
X509CertSelector.setCertificate()	222
X509CertSelector.setIssuer()	222
X509CertSelector.setSerialNumber()	223
X509CertSelector.setSubject()	223
Summary	224
Exercises	225
Chapter 7: Certificate Revocation and Path Validation	227
Getting Started	228
Certificate Revocation Lists	230
The CRL Class	231
CRL.getType()	231
CRL.isRevoked()	231
X.509 Certificate Revocation Lists	232
The X509CRL Class	233
X509CRL.getTBSCertList()	233
X509CRL.getVersion()	234
X509CRL.getIssuerX500Principal()	234
X509CRL.getThisUpdate() and X509CRL.getNextUpdate()	234
X509CRL.getRevokedCertificates()	235
X509CRL.getRevokedCertificate()	235
X509CRL.getSignature()	235
X509CRL.getSigAlgOID(), and X509CRL.getSigAlgParams()	235
X509CRL.getSigAlgName()	235
X509CRL.verify()	235
X509CRL.getEncoded()	236
The X509CRLEntry Class	236
X509CRLEntry.getCertificateIssuer()	236
X509CRLEntry.getRevocationDate()	236
X509CRLEntry.getSerialNumber()	236
X509CRLEntry.hasExtensions()	236

Contents

X.509 CRL Entry Extensions	237
The ReasonCode Extension	237
The HoldInstructionCode Extension	237
The InvalidityDate Extension	238
The CertificateIssuer Extension	238
X.509 CRL Extensions	238
The AuthorityKeyIdentifier Extension	239
The IssuerAlternativeName Extension	239
The CRLNumber Extension	239
The DeltaCRLIndicator Extension	239
The IssuingDistributionPoint Extension	239
The FreshestCRL Extension	240
Reading CRLs using the CertificateFactory Class	243
CertificateFactory.generateCRL()	243
CertificateFactory.generateCRLs()	243
The X509CRLSelector Class	245
X509CRLSelector.addIssuer() and X509CRLSelector.addIssuerName()	245
X509CRLSelector.setDateAndTime()	246
X509CRLSelector.setMaxCRL() and X509CRLSelector.setMinCRL()	246
Online Certificate Status Protocol	248
The CertificateID Class	248
CertificateID.getHashAlgOID()	249
CertificateID.getIssuerNameHash()	249
CertificateID.getIssuerKeyHash()	249
CertificateID.getSerialNumber()	249
The OCSPReq Class	249
OCSPReq.getTBSRequest()	250
OCSPReq.getVersion()	250
OCSPReq.getRequestorName()	250
OCSPReq.getRequestList()	250
OCSPReq.isSigned()	251
OCSPReq.getSignature() and OCSPReq.getSignatureAlgOID()	251
OCSPReq.getCertificates()	251
OCSP Request Extensions	251
The Nonce Extension	251
The Acceptable Response Types Extension	252
The Service Locator Extension	252
The OCSPResp Class	255
The BasicOCSPResp Class	256
BasicOCSPResp.getTBSResponseData()	256
BasicOCSPResponse.getVersion()	257
BasicOCSPResponse.getResponderID()	257

BasicOCSPResponse.getProducedAt()	257
BasicOCSPResponse.getResponses()	257
OCSP Response Extensions	258
The CRL References Extension	258
The Archive Cutoff Extensions	258
X.509 CRL Entry Extensions	259
Certificate Path Validation	264
The TrustAnchor Class	264
The PKIXParameters Class	265
PKIXParameters.addCertStore() and PKIXParameters.setCertStores()	266
PKIXParameters.setDate()	266
PKIXParameters.setTargetCertConstraints()	266
PKIXParameters.setRevocationEnabled()	266
The CertPathValidator Class	266
CertPathValidator.getDefaultType()	267
CertPathValidator.getAlgorithm()	267
CertPathValidator.validate()	267
The PKIXCertPathValidatorResult Class	267
The PKIXCertPathChecker Class	270
PKIXCertPathChecker.init()	270
PKIXCertPathChecker.isForwardCheckingSupported()	271
PKIXCertPathChecker.getSupportedExtensions()	271
PKIXCertPathChecker.check()	271
Building a Valid Path from a CertStore	275
The CertPathBuilder Class	275
The PKIXBuilderParameters Class	275
Summary	278
Exercises	279
Chapter 8: Key and Certificate Management Using Keystores	281
Getting Started	281
The KeyStore Class	283
Keystore Types	284
Standard JDK Keystore Types	284
Bouncy Castle Keystore Types	284
The Basic KeyStore API	285
KeyStore.aliases()	285
KeyStore.containsAlias()	285
KeyStore.deleteEntry()	285
KeyStore.getCertificate()	285
KeyStore.getCertificateAlias()	285

Contents

KeyStore.getCertificateChain()	286
KeyStore.getCreationDate()	286
KeyStore.getKey()	286
KeyStore.getType()	286
KeyStore.isCertificateEntry()	286
KeyStore.isKeyEntry()	286
KeyStore.load()	286
KeyStore.setCertificateEntry()	287
KeyStore.setKeyEntry()	287
KeyStore.size()	287
KeyStore.store()	287
KeyStore Nested Classes and Interfaces	290
The KeyStore.ProtectionParameter Interface	290
KeyStore.CallbackHandlerProtection	291
KeyStore.PasswordProtection	291
The KeyStore.Entry Interface	291
KeyStore.getEntry()	291
KeyStore.setEntry()	291
KeyStore.entryInstanceOf()	292
KeyStore.PrivateKeyEntry	292
KeyStore.SecretKeyEntry	292
KeyStore.TrustedCertificateEntry	292
The KeyStore.Builder Class	295
KeyStore.Builder.getKeyStore()	295
KeyStore.Builder.getProtectionParameter()	295
KeyStore.Builder.newInstance()	295
The KeyStore.LoadStoreParameter Interface	297
The PKCS #12 Format	298
Using PKCS #12 with the KeyStore API	300
The Keytool	304
Keytool Commands	304
General Command Options	304
Commands and Their Options	305
The JVM's CA Keystore	307
Some Keytool Experiments	308
Generating Some Sample Keystore Files	308
Jarsigning and Java Policy	312
The Jarsigner	312
Java Policy Files	312
Summary	313
Exercises	314

Chapter 9: CMS and S/MIME	315
Getting Started	315
Cryptographic Message Syntax	318
Basic CMS	318
The Data Content Type	319
The CMSProcessable Interface	320
CMS Signed-Data	320
ASN.1 Structure	321
The DigestAlgorithms Field	322
The EncapContentInfo Field	322
The Certificates and Crls Fields	322
The SignerInfos Field	323
The Version Field	325
The SignerInformation Class	325
SignerInformation.getDigestAlgOID()	325
SignerInformation.getDigestAlgParams()	325
SignerInformation.getEncryptionAlgOID()	326
SignerInformation.getEncryptionAlgParams()	326
SignerInformation.getSID()	326
SignerInformation.getSignature()	326
SignerInformation.getSignedAttributes()	326
SignerInformation.getUnsignedAttributes()	326
SignerInformation.verify()	326
SignerInformation.replaceUnsignedAttributes()	327
The SignerInformationStore Class	327
SignerInformationStore.get()	327
SignerInformationStore.getSigners()	327
SignerInformationStore.size()	327
The CMSSignedData Class	327
CMSSignedData.getCertificatesAndCRLs()	328
CMSSignedData.getEncoded()	328
CMSSignedData.getSignedContent()	328
CMSSignedData.getSignedContentOID()	328
CMSSignedData.getSignerInfos()	328
CMSSignedData.replaceSigners()	328
CMS Enveloped-Data	332
ASN.1 Structure	333
The OriginatorInfo Field	333
The RecipientInfos Field	333
The EncryptedContentInfo Field	334
The UnprotectedAttrs Field	335
The Version Field	335

Contents

The RecipientInformation Class	335
RecipientInformation.getContent()	336
RecipientInformation.getKeyEncryptionAlgOID()	336
RecipientInformation.getKeyEncryptionAlgorithmParameters()	336
RecipientInformation.getKeyEncryptionAlgParams()	336
RecipientInformation.getRID()	336
The KeyTransRecipientInformation Class	336
The RecipientInformationStore Class	337
RecipientInformationStore.get()	337
RecipientInformationStore.getRecipients()	337
RecipientInformationStore.size()	337
The CMSEnvelopedData Class	337
CMSEnvelopedData.getEncoded()	338
CMSEnvelopedData.getEncryptionAlgOID()	338
CMSEnvelopedData.getEncryptionAlgorithmParameters()	338
CMSEnvelopedData.getEncryptionAlgParams()	338
CMSEnvelopedData.getRecipientInfos()	338
CMSEnvelopedData.getUnprotectedAttributes()	338
The KEKRecipientInformation Class	342
Data Compression in CMS	345
ASN.1 Structure	345
The CMSCompressedData Class	345
CMSCompressedData.getContent()	345
CMSCompressedData.getEncoded()	345
Secure/Multipurpose Internet Mail Extensions (S/MIME)	347
The CMSProcessableBodyPart Class	348
The SMIMEUtil Class	348
SMIMEUtil.toMimeBodyPart()	348
SMIMEUtil.createIssuerAndSerialNumberFor()	348
S/MIME Signed Messages	348
The CMSProcessableBodyPartInbound Class	349
The CMSProcessableBodyPartOutbound Class	349
The SMIMESigned Class	349
SMIMESigned.getContent()	350
SMIMESigned.getContentAsMimeMessage()	350
SMIMESigned.getContentWithSignature()	350
S/MIME Enveloped Messages	354
The SMIMEEnveloped Class	355
Combining Signing with Encryption	357
S/MIME Compressed Messages	361
The SMIMECompressed Class	361
Summary	363
Exercises	364

Chapter 10: SSL and TLS	365
The SSL and TLS Protocols	365
Getting Started	366
A Basic SSL Client and Server	369
The SSLSocketFactory Class	370
SSLSocketFactory.createSocket()	370
SSLSocketFactory.getDefault()	370
SSLSocketFactory.getDefaultCipherSuites()	370
SSLSocketFactory.getSupportedCipherSuites()	370
The SSLServerSocketFactory Class	370
SSLServerSocketFactory.createServerSocket()	371
SSLServerSocketFactory.getDefault()	371
SSLServerSocketFactory.getDefaultCipherSuites() and SSLServerSocketFactory.getSupportedCipherSuites()	371
The SSLSocket Class	371
SSLSocket.setEnabledCipherSuites()	371
SSLSocket.setEnabledProtocols()	372
SSLSocket.setEnableSessionCreation()	372
SSLSocket.setUseClientMode()	372
SSLSocket.startHandshake()	372
The SSLServerSocket Class	373
SSLServerSocket.setEnabledCipherSuites()	373
SSLServerSocket.setEnabledProtocols()	373
SSLServerSocket.setEnableSessionCreation()	373
SSLServerSocket.setUseClientMode()	373
The HandshakeCompletedListener Interface	377
Client-Side Authentication	378
SSLServerSocket Configuration	379
SSLServerSocket.setNeedClientAuth()	379
SSLServerSocket.setWantClientAuth()	379
Server-Mode SSLSocket Configuration	379
The setNeedClientAuth() Method	379
The setWantClientAuth() Method	379
The SSLContext Class	379
SSLContext.init()	380
SSLContext.getClientSessionContext()	380
SSLContext.getProtocol()	380
SSLContext.getServerSessionContext()	381
SSLContext.getServerSocketFactory()	381
SSLContext.getSocketFactory()	381

Contents

The KeyManagerFactory Class	381
KeyManagerFactory.init()	381
KeyManagerFactory.getAlgorithm()	382
KeyManagerFactory.getDefaultAlgorithm()	382
KeyManagerFactory.getKeyManagers()	382
The TrustManagerFactory Class	386
TrustManagerFactory.init()	386
TrustManagerFactory.getAlgorithm()	386
TrustManagerFactory.getDefaultAlgorithm()	386
TrustManagerFactory.getTrustManagers()	387
Managing SSL Session Information	389
The SSLSession Interface	389
SSLSession.getCipherSuite()	389
SSLSession.getCreationTime()	389
SSLSession.getId()	390
SSLSession.getLastAccessedTime()	390
SSLSession.getLocalCertificates()	390
SSLSession.getLocalPrincipal()	390
SSLSession.getPeerCertificates()	390
SSLSession.getPeerHost()	390
SSLSession.getPeerPort()	390
SSLSession.getPeerPrincipal()	390
SSLSession.getProtocol()	391
SSLSession.getSessionContext()	391
SSLSession.invalidate()	391
SSLSession.isValid()	391
SSLSession.putValue()	391
Dealing with HTTPS	394
The HttpsURLConnection Class	394
HttpsURLConnection.getCipherSuite()	395
HttpsURLConnection.getHostnameVerifier()	395
HttpsURLConnection.getLocalCertificates()	395
HttpsURLConnection.getLocalPrincipal()	395
HttpsURLConnection.getPeerPrincipal()	395
HttpsURLConnection.getServerCertificates()	396
HttpsURLConnection.getSSLSocketFactory()	396
HttpsURLConnection.setDefaultSSLSocketFactory()	396
HttpsURLConnection.setDefaultHostnameVerifier()	396
The HostnameVerifier Interface	396
Summary	401
Exercises	402

Appendix A: Solutions to Exercises	403
Chapter 1 Solutions	403
Chapter 2 Solutions	403
Chapter 3 Solutions	404
Chapter 4 Solutions	405
Chapter 5 Solutions	406
Chapter 6 Solutions	407
Chapter 7 Solutions	408
Chapter 8 Solutions	409
Chapter 9 Solutions	412
Chapter 10 Solutions	415
Appendix B: Algorithms Provided by the Bouncy Castle Provider	417
Asymmetric Ciphers	417
Certificate Path Validation	417
Key Agreement Algorithms	417
Key Stores	418
MAC Algorithms	418
Signature Algorithms	418
Message Digests	418
Symmetric Block Ciphers	418
Symmetric Stream Ciphers	419
Appendix C: Using the Bouncy Castle API for Elliptic Curve	421
Elliptic Curve Interfaces	421
The ECKey Interface	421
The ECPrivateKey Interface	422
The ECPublicKey Interface	422
The ECPointEncoder Interface	422
Elliptic Curve Classes	422
The ECNamedCurveParameterSpec Class	422
The ECNamedCurveSpec Class	423
The ECParameterSpec Class	423
The ECPrivateKeySpec Class	423
The ECPublicKeySpec Class	423

Contents

Appendix D: Bibliography and Further Reading	425
ASN.1 Standards	425
IETF Working Group Charter Pages	425
NIST Publications	426
PKCS Standards	426
RFCs	427
Other Useful Standards	428
Useful References	428
Useful Web Links	429
Index	431