

[For more information about this title, click here.](#)

Contents

Preface	xv
Acknowledgments	xvii
About the Reviewer	xix
 Chapter 1 Introduction	 1
 Chapter 2 Security Primer	 5
Encryption	6
Symmetric Ciphers (The Nature of the Crank)	7
Triple-DES	8
Padding and Feedback Modes	9
AES	14
Symmetric Key Generation (The Nature of the Key)	15
Symmetric Encryption	15
Asymmetric Ciphers	16
Introduction to the RSA Algorithm	17
Asymmetric Encryption with RSA	19
RSA Algorithm Details	20
Case 1: "The Engineer"	21
Case 2: "The Theoretician"	22
RSA Logistics	22
RSA Problems	25
Digital Envelopes	28
Key Agreement	29
Diffie-Hellman Key Agreement Logistics	30
Digital Signature Basics	32
Hash Functions	33
RSA Signature Scheme	34
DSA Signature Scheme	36
HMAC Authentication	37
Prelude to Trust and Standardization	39
Raw Cryptographic Objects	39
Cryptographic Standards	40
Trust, Certificates, and Path Validation	46
Path Validation	50
Path Validation State Machine	51
Authorization	54
Additional Information	54
Chapter Summary	54

Chapter 3	XML Primer	57
	What Is XML?	58
	Meta-Language and Paradigm Shift	58
	Elements, Attributes, and Documents	62
	The URI	69
	Namespaces in XML	70
	More Markup	74
	More Semantics: The Document Prolog	75
	Document Type Definition (DTD)	78
	Processing XML	84
	The Document Object Model (DOM)	84
	The XPath Data Model	94
	Document Order	96
	XPath Node Set	104
	More on XPath	104
	Chapter Summary	104
Chapter 4	Introduction to XML Digital Signatures	107
	XML Signature Basics	108
	XML Signatures and Raw Digital Signatures	114
	XML Signature Types	120
	XML Signature Syntax and Examples	121
	XML Signature Syntax	122
	Chapter Summary	144
Chapter 5	Introduction to XML Digital Signatures Part 2	147
	XML Signature Processing	147
	The <Reference> Element	148
	Core Generation	152
	The URI Attribute: Additional Features	163
	Signature Transforms	170
	Chapter Summary	191
Chapter 6	XML Signature Examples	193
	XML Signature Examples and Frequently Asked Questions	193
	Scenario 1	194
	Proposed Solution	194
	Scenario 2	194

Proposed Solution	195
Scenario 3	196
Proposed Solution	196
Scenario 4	199
Proposed Solution	199
Scenario 5	201
Proposed Solution 1	201
Proposed Solution 2	203
Scenario 6	204
Proposed Solution	204
Scenario 7	206
Proposed Solution	207
Scenario 8	208
Proposed Solution	208
Scenario 9	209
Proposed Solution	209
Scenario 10	211
Proposed Solution	211
Scenario 11	214
Proposed Solution	214
Scenario 12	214
Proposed Solution	215
Scenario 13	221
Proposed Solution	221
Scenario 14	223
Proposed Solution	223
Chapter Summary	225
Chapter 7 Introduction to XML Encryption	227
XML Encryption Basics and Syntax	228
XML Encryption Use Cases	229
The <EncryptedData> Element: Details	234
The <ds:KeyInfo> Element	244
Plaintext Replacement	263
XML Encryption Processing Rules	265
The Application	266
The Encryptor	266
The Decryptor	266
The Encryptor: Process	267

The Decryptor: Process	269
XML Encryption: Other Issues	271
Security Considerations	275
Chapter Summary	277
Chapter 8 XML Signature Implementation: RSA BSAFE® Cert-J	279
RSA BSAFE Cert-J: Class Diagrams and Code Examples	280
Syntax and Processing Revisited	280
XMLSignature	281
Reference and Transformer	285
KeyInfo	290
Manifest	307
The <Object> Element	313
Signature Processing	316
More on Manifest	321
Additional Classes	322
RSA BSAFE Cert-J: Specialized Code Samples	324
Enveloping Arbitrary Binary Data	324
Custom Transformations	326
XPath Tester	329
Chapter Summary	330
Chapter 9 XML Key Management Specification and the Proliferation of Web Services	333
XKMS Basics	334
Validation, Verification, and Trust	334
XKMS Components	335
X-KISS: Tier 1	336
Syntax of the Locate Message	338
X-KISS: Tier 2	340
Syntax of the Validate Message	343
X-KRSS	345
Key Registration	345
Key Registration Message Syntax	347
Key Revocation	351
Security Considerations	351
Chapter Summary	354

Appendix	355
Additional Resources	355
Exclusive Canonicalization	355
XML Encryption: A List of Supported Algorithms	358
References	360
Template Signing FAQs for RSA BSAFE Cert-J	363
Index	365