

Contents

About the Authors	<i>ix</i>
About the Technical Reviewers	<i>xi</i>
Acknowledgments	<i>xiii</i>
Introduction	<i>xv</i>

Chapter 1 The Basics of Cryptography and Security1

The Essence of Cryptography	<i>1</i>
Basic Terminology	<i>2</i>
Creating Digital Signatures	<i>17</i>
Certificates Defined	<i>18</i>
Cryptography versus Security	<i>19</i>
Summary	<i>22</i>

Chapter 2 Using the .NET Cryptography Classes23

Working with the System.Security.Cryptography Namespace	<i>23</i>
Understanding Hash-Based Classes	<i>24</i>
Cryptographic Streaming	<i>30</i>
Investigating Random Number Generation Classes	<i>32</i>
Creating Keys	<i>36</i>
Working with the System.Security.Cryptography.X509Certificates Namespace ..	<i>52</i>
Exploring Serialized Objects and Cryptography	<i>54</i>
Summary	<i>67</i>

Chapter 3 XML Encryption and Signatures69

Locking Down XML	<i>69</i>
Understanding the Relationships between .NET, Cryptography, and XML	<i>80</i>
Summary	<i>91</i>

Chapter 4 Code Access Security	93
Understanding Code Access Security	93
Covering the Essentials	94
Managing Permissions	110
Creating Custom Permissions	136
Examining .NET and Operation System Security	155
Summary	158
Chapter 5 Role Access Security	159
Using .NET Class Definitions	159
Understanding Identity Permission Attributes	166
Exploring Impersonation	170
Summary	183
Chapter 6 Remoting and Security	185
Remoting Overview	185
Network Security Simplified	195
Understanding Authentication, Authorization, and Impersonation	198
Summary	224
Chapter 7 ASP.NET Web Application Security	225
ASP.NET and IIS Considerations	225
Configuring Security	229
Exploring ASP.NET	233
Summary	252
Chapter 8 Passport	253
Passport Fundamentals	253
Sample Application—Exploring Passport	283
Summary	287

Chapter 9 Protecting Code	289
Decompiling Assemblies	289
Preventing Decompilation	292
Summary	298
 Index	 299