

# **Cryptography** **for Internet** **and Database** **Applications**

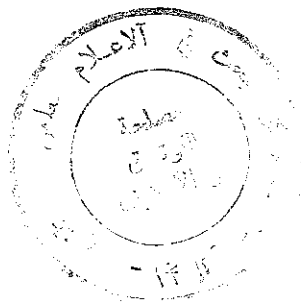


**Developing Secret and  
Public Key Techniques with Java™**

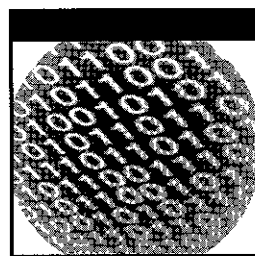
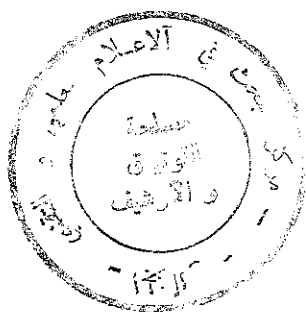
**Nick Galbreath**

IST 2837

# **Cryptography for Internet and Database Applications**







# Cryptography for Internet and Database Applications

**Developing Secret and Public Key  
Techniques with Java™**

Nick Galbreath



Wiley Publishing, Inc.

Publisher: Bob Ipsen  
Editor: Carol A. Long  
Developmental Editor: Adaobi Obi  
Managing Editor: Micheline Frederick  
New Media Editor: Brian Snapp  
Text Design & Composition: Wiley Composition Services

Designations used by companies to distinguish their products are often claimed as trademarks. In all instances where Wiley Publishing, Inc., is aware of a claim, the product names appear in initial capital or ALL CAPITAL LETTERS. Readers, however, should contact the appropriate companies for more complete information regarding trademarks and registration.

This book is printed on acid-free paper. ☺

Copyright © 2002 by Nicholas Galbreath. All rights reserved.

**Published by Wiley Publishing, Inc., Indianapolis, Indiana**

Published simultaneously in Canada

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470. Requests to the Publisher for permission should be addressed to the Legal Department, Wiley Publishing, Inc., 10475 Crosspointe Blvd., Indianapolis, IN 46256, (317) 572-3447, fax (317) 572-4447, E-mail: permcoordinator@wiley.com.

**Limit of Liability/Disclaimer of Warranty:** While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

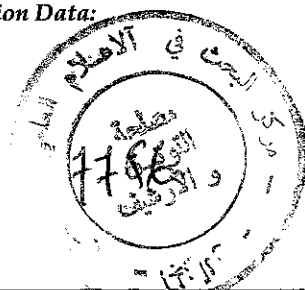
Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

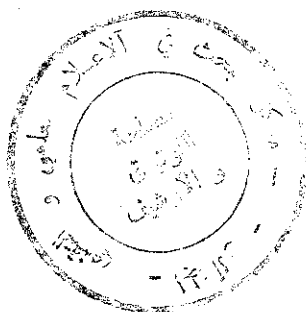
**Library of Congress Cataloging-in-Publication Data:**

ISBN: 0-471-21029-3

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1





# Contents

<b>Preface</b>	<b>xiii</b>
<b>Introduction</b>	<b>xv</b>
<b>Chapter 1 Bits and Bytes</b>	<b>1</b>
General Operations	1
Number Bases	2
Bits and Bytes	3
Signed Bytes	4
Bitwise Operators	4
Complementation or Bitwise NOT	6
Bitwise AND	6
Bitwise OR	7
Bitwise Exclusive OR (XOR)	8
Left-Shift	8
Right-Shift	9
Special Operations and Abbreviations	10
Packed Words	11
Integers and Endian Notation	12
Java Numerics	13
Basic Types	14
Type Conversion	15
Unsigned to Signed Conversions	17
Overflow	17
Arrays	18
Numeric Classes	20

Booleans and BitFields	21
Chars	22
Working with Bytes	22
Sign Problems	22
Conversion of Integral Types to Byte Arrays	24
Converting to Hex Strings	25
BigInteger	28
Creating and Converting	29
BigInteger and Cryptography	31
Secret Methods in BigInteger	31
<b>Chapter 2 Secret Key Cryptography</b>	<b>35</b>
Symmetric Block Ciphers	35
Cipher Properties	36
Security Properties	36
Brute-Force Attacks	37
Other Attacks	37
Common Block Ciphers	39
Data Encryption Standard (DES)	39
Triple DES	40
Blowfish	41
IDEA	43
RC5	43
Rijndael and the Advanced Encryption Standard (AES)	44
Twofish	46
RC6	47
Ciphers You Shouldn't Use	47
Password XOR Schemes	47
Classical Cryptography	48
ROT 13	49
Padding	49
Fixed-Value Padding	49
Random Padding	50
PKCS Padding	50
Modes of Operations	51
Initialization Vectors	51
Electronic Codebook Mode (ECB)	53
Cipher Block Chaining Mode (CBC)	54
Cipher Feedback Mode (CFB)	56
Output Feedback Mode (OFB)	58
Counter Mode (CTR)	60
Propagating CBC (PCBC) Mode	60
Key Wrapping	61
Triple DES KEY Wrapping	61
AES Key Wrapping	62
Turning Passwords into Keys	63

Hashes	64
Cryptographic Hashes	65
Collisions	66
Attacks	67
Algorithms	69
The MD Family	71
The SHA Family	71
The RIPE-MD Family	72
Hash Standards and Practices	73
Hashed Message Authentication Codes (HMACs)	74
The Standard HMAC	74
Legacy Concatenation Schemes	75
HMAC Standards and Practices	76
Summary	76
<b>Chapter 3    Public Key Cryptography</b>	<b>77</b>
Public Key Ciphers	77
Other Systems	79
Digital Signatures	79
Key Agreements	79
Zero-Knowledge Schemes	79
Secret Sharing	80
Public Key Security Classification	80
Fundamental Mathematics	82
Prime Numbers	82
The Distribution of Prime Numbers	83
Prime Testing	84
Probabilistic Tests	85
Sequence-Based Tests	87
Elementary Number Theory	88
Modular Arithmetic	88
Additive Groups	89
Multiplicative Groups	89
Fields	90
Rings	90
Orders and Generators	90
Public Key Encryption and Major PKCS Categories	91
RSA and Integer Factorization	92
Factoring	92
The RSA Problem	94
The Algorithm	94
Message Representation and OAEP	96
In Practice and Standards	98
Choice of Parameters	98
Discrete Logarithm Systems	100
Underlying Mathematics	100
The Algorithm	103
Standards and Practice	106

Elliptic Curves	106
Underlying Mathematics: Elliptic Curves	106
The Algorithm	110
Standards and Practice	112
Other Public Key Cryptographic Systems	112
Rabin Cryptosystem	112
NTRU	114
Summary	115
<b>Chapter 4 Random Numbers</b>	<b>117</b>
Randomness and Security	119
Testing for Randomness	120
FIPS 140-2 Requirements	121
Pseudorandom Number Generators	122
Cryptographic PRNG	123
SHA-1 PRNG	123
Cipher-CBC or ANSI X9.17	123
FIPS 186	123
Blum-Blum-Shub	124
Stream Ciphers	125
One-Time Pads	125
RC4 or ArcFour	125
Using Randomness	126
Generating Random Numbers for Gaming	126
Generating Random Numbers in a Range	127
Shuffling	129
Generating Random Permutations	131
Small Permutations	131
Large Fixed Permutations	132
Random Sampling	133
Accessing Entropy	134
OS Services	134
Win32 CryptoAPI CryptGenRandom	135
/dev/random and friends	135
Userland Services	136
Entropy Generating Daemon (EGD)	137
PRNGD	141
Yarrow and EGADS	141
TrueRand Library	141
Remote Services	142
RAND Corporation	143
HotBits	143
Random.org	143
LavaRnd	144
Java and Random Numbers	144
Random and SecureRandom	144
java.util.random	145
java.security.SecureRandom	146

Developer Issues	148
Reseeding	148
Collecting Entropy	150
An Entropy Pool Implementation	150
Basic System State	151
Thread Schemes	153
Reading External Sources	156
Application Events	156
User Events	157
<b>Chapter 5 Java Cryptography</b>	<b>159</b>
Organization	160
Providers and Engine Classes	161
Parameters, Keys, and Certificates	162
Error Handling	163
Providers	164
Standard Names	165
Standard Sun and SunJCE Providers	168
Other Providers	169
Initializing Providers	170
Writing Your Own Provider	171
Core Engine Classes	171
MessageDigest	171
Digest Streams	172
MAC	173
SecureRandom	174
Ciphers	177
Additional Cipher-Related Objects	180
Signatures	183
SignedObject	184
Key Agreement Protocols	184
Parameters, Keys, and Certificates	185
Algorithm Parameters	186
AlgorithmParameters	186
AlgorithmParameterGenerators	188
Keys	189
Secret Keys	192
Public/Private Keys	195
Encoding and Encrypting Keys	197
Summary	202
<b>Chapter 6 Small Message Encoding and Encryption</b>	<b>203</b>
Preprocessing	203
Converting Digits into Bytes	203
7-bit to 8-bit Compression	205
General Compression and java.util.zip.Deflate	206
Adding Check and Parity Bits	207

Small Message Encryption	209
Single-Block Encryption	210
$n$ -Block Encryption	210
Very Small Message Encryption	211
XOR Tables	211
Small Codebooks	211
RC5-16/16	212
Small Message Encoding	212
Encoding for Customer-Usable Data	213
Capacity and Range	213
Selecting a Base Representation	214
Selecting Base Alphabets	215
Mixed Bases and Alphabets	221
Adding Check Digits	221
Encoding for Machines and Customer-Visible Applications	230
Base 64	230
Base 85	234
Base 128 and Java Source Encoding	237
<b>Chapter 7 Application and Data Architecture</b>	<b>241</b>
Database Architecture for Encrypted Data	241
Selecting a Cipher	243
Secret or Public?	243
Cipher Selection	244
Data	245
Passwords	245
Challenges and Responses	246
Payment, Credit Card, and Other Account Numbers	247
Social Security Number (U.S.)	250
Birthdates and Birthdays	250
Last Name	251
Searching, Indexing, and Constraints	251
Removing Randomness	252
Deterministic Key Selection	252
Indexing and Hashing	253
Uniqueness Constraints	254
Asymmetric Data Usages	255
Null Values and Database Applications	256
Secure Memory Management in Java	258
Smart Array Classes	259
Char Arrays	262
Using SecureRandom	263
Secret Key Management	263
Secret Key Data	264
Key Generation	266
Key Encryption	266
Storage	267

Key Access and Distribution	268
Using Keys with Ciphers and MACs	269
Passwords	272
Startup Passwords	272
Member Names and Passwords	274
Selecting Passwords	274
Member Login, Success and Failure	275
Changing Passwords and Challenges	276
Web-Based Password Entry	276
Generating New Passwords	277
Member Names	278
Logging	278
Embedded-Encryption Logging	279
Fully Encrypted Log Files	279
Public Key Logging	281
Split Log Files	281
Network-Based Logs	282
Cryptographic Tokens and Applications	282
Token Design	282
Expirations and Time Quantization	283
Creating the Security Bits	285
URL Tokens	285
Tamper-Evident URLs	285
Protecting Static Content	286
A Simple URL MAC Implementation	287
Fast Query String Parsing	290
URL Encryption	296
Very Short URLs	296
Cookie Tokens	297
Detecting Cookie Capability	297
Cookies and Authentication	297
Tokens for Access Control	298
Buy-on-Demand Systems	299
Multiple Key Systems	299
Trials and Expirations	300
Decimal and Monetary Computations	300
Doubles and Floats	300
BigDecimal	301
Rounding	302
BigDecimal and Mathematics	303
BigDecimal Alternatives and Wrappers	304
Usage and Storage	304

<b>Appendix A Java Cryptography Class Reference</b>	<b>305</b>
---	------------

<b>References</b>	<b>367</b>
-------------------	------------

<b>Index</b>	<b>381</b>
--------------	------------