

# CONTENTS IN DETAIL

<b>ACKNOWLEDGMENTS</b>	<b>xiii</b>
------------------------	-------------

<b>INTRODUCTION</b>	<b>xv</b>
---------------------	-----------

Who This Book Is For . . . . .	xvi
Topics Covered . . . . .	xvi
Behind the Magic . . . . .	xvii

<b>1</b>	
<b>ENCRYPTION</b>	<b>1</b>

The Goal of Encryption . . . . .	2
Transposition: Same Data, Different Order . . . . .	2
Cipher Keys . . . . .	4
Attacking the Encryption . . . . .	5
Substitution: Replacing Data . . . . .	6
Varying the Substitution Pattern . . . . .	7
Key Expansion . . . . .	9
The Advanced Encryption Standard . . . . .	9
Binary Basics . . . . .	10
AES Encryption: The Big Picture . . . . .	12
Key Expansion in AES . . . . .	13
AES Encryption Rounds . . . . .	14
Block Chaining . . . . .	15
Why AES Is Secure . . . . .	16
Possible AES Attacks . . . . .	17
The Limits of Private-Key Encryption . . . . .	18

<b>2</b>	
<b>PASSWORDS</b>	<b>19</b>

Transforming a Password into a Number . . . . .	20
Properties of Good Hash Functions . . . . .	20
The MD5 Hash Function . . . . .	21
Encoding the Password . . . . .	21
Bitwise Operations . . . . .	22
MD5 Hashing Rounds . . . . .	24
Meeting the Criteria of a Good Hash Function . . . . .	25
Digital Signatures . . . . .	25
The Problem of Identity . . . . .	26
Collision Attacks . . . . .	26

Passwords in Authentication Systems . . . . .	26
The Dangers of Password Tables . . . . .	26
Hashing Passwords . . . . .	27
Dictionary Attacks . . . . .	28
Hash Tables . . . . .	29
Hash Chaining . . . . .	29
Iterative Hashing . . . . .	32
Salting Passwords . . . . .	34
Are Password Tables Safe? . . . . .	35
Password Storage Services . . . . .	35
A Final Thought . . . . .	36

### **3**

## **WEB SECURITY** **37**

How Public-Key Cryptography Solves the Shared Key Problem . . . . .	38
Math Tools for Public-Key Cryptography . . . . .	38
Invertible Functions . . . . .	39
One-Way Functions . . . . .	39
Trapdoor Functions . . . . .	40
The RSA Encryption Method . . . . .	42
Creating the Keys . . . . .	42
Encrypting Data with RSA . . . . .	44
RSA Effectiveness . . . . .	45
RSA Use in the Real World . . . . .	47
RSA for Authentication . . . . .	49
Security on the Web: HTTPS . . . . .	52
Handshaking . . . . .	52
Transmitting Data Under HTTPS . . . . .	54
The Shared Key Problem Solved? . . . . .	55

### **4**

## **MOVIE CGI** **57**

Software for Traditional Animation . . . . .	59
How Digital Images Work . . . . .	59
How Colors Are Defined . . . . .	60
How Software Makes Cel Animations . . . . .	61
From Cel Animation Software to Rendered 2D Graphics . . . . .	69
Software for 3D CGI . . . . .	69
How 3D Scenes Are Described . . . . .	70
The Virtual Camera . . . . .	71
Direct Lighting . . . . .	71
Global Illumination . . . . .	76
How Light Is Traced . . . . .	77
Full-Scene Anti-Aliasing . . . . .	80
Combining the Real and the Fake . . . . .	81
The Ideal of Movie-Quality Rendering . . . . .	82

<b>5</b>	<b>GAME GRAPHICS</b>	<b>85</b>
	Hardware for Real-Time Graphics . . . . .	86
	Why Games Don't Ray Trace . . . . .	87
	All Lines and No Curves . . . . .	87
	Projection Without Ray Tracing . . . . .	88
	Rendering Triangles . . . . .	89
	The Painter's Algorithm . . . . .	90
	Depth Buffering . . . . .	91
	Real-Time Lighting . . . . .	92
	Shadows . . . . .	94
	Ambient Light and Ambient Occlusion . . . . .	96
	Texture Mapping . . . . .	97
	Nearest-Neighbor Sampling . . . . .	99
	Bilinear Filtering . . . . .	101
	Mipmaps . . . . .	102
	Trilinear Filtering . . . . .	102
	Reflections . . . . .	103
	Faking Curves . . . . .	105
	Distant Impostors . . . . .	105
	Bump Mapping . . . . .	106
	Tessellation . . . . .	107
	Anti-Aliasing in Real Time . . . . .	108
	Supersampling . . . . .	109
	Multisampling . . . . .	110
	Post-Process Anti-Aliasing . . . . .	111
	The Rendering Budget . . . . .	113
	What's Next for Game Graphics . . . . .	113

<b>6</b>	<b>DATA COMPRESSION</b>	<b>115</b>
	Run-Length Encoding . . . . .	117
	Dictionary Compression . . . . .	118
	The Basic Method . . . . .	118
	Huffman Encoding . . . . .	120
	Reorganizing Data for Better Compression . . . . .	121
	Predictive Encoding . . . . .	121
	Quantization . . . . .	123
	JPEG Images . . . . .	123
	A Different Way to Store Colors . . . . .	124
	The Discrete Cosine Transform . . . . .	125
	The DCT for Two Dimensions . . . . .	128
	Compressing the Results . . . . .	132
	JPEG Picture Quality . . . . .	135
	Compressing High-Definition Video . . . . .	136
	Temporal Redundancy . . . . .	138
	MPEG-2 Video Compression . . . . .	138
	Video Quality with Temporal Compression . . . . .	142
	The Present and Future of Video Compression . . . . .	143

<b>7</b>		
<b>SEARCH</b>		<b>145</b>
Defining the Search Problem . . . . .		146
Putting Data in Order . . . . .		146
Selection Sort . . . . .		146
Quicksort . . . . .		147
Binary Search . . . . .		151
Indexing . . . . .		152
Hashing . . . . .		154
Web Search . . . . .		157
Ranking Results . . . . .		158
Using the Index Effectively . . . . .		159
What's Next for Web Search . . . . .		160
<b>8</b>		
<b>CONCURRENCY</b>		<b>161</b>
Why Concurrency Is Needed . . . . .		162
Performance . . . . .		162
Multiuser Environments . . . . .		162
Multitasking . . . . .		162
How Concurrency Can Fail . . . . .		163
Making Concurrency Safe . . . . .		166
Read-Only Data . . . . .		166
Transaction-Based Processing . . . . .		166
Semaphores . . . . .		167
The Problem of Indefinite Waits . . . . .		169
Orderly Queues . . . . .		170
Starvation from Circular Waits . . . . .		170
Performance Issues of Semaphores . . . . .		172
What's Next for Concurrency . . . . .		174
<b>9</b>		
<b>MAP ROUTES</b>		<b>175</b>
What a Map Looks Like to Software . . . . .		176
Best-First Search . . . . .		178
Reusing Prior Search Results . . . . .		181
Finding All the Best Routes at Once . . . . .		183
Floyd's Algorithm . . . . .		183
Storing Route Directions . . . . .		186
The Future of Routing . . . . .		189
<b>INDEX</b>		<b>191</b>