# CONTENTS IN DETAIL

## ACKNOWLEDGMENTS

## INTRODUCTION

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

## 1 ENCRYPTION

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

## 2 PASSWORDS

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
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passwords in Authentication Systems</td>
<td>26</td>
</tr>
<tr>
<td>The Dangers of Password Tables</td>
<td>26</td>
</tr>
<tr>
<td>Hashing Passwords</td>
<td>27</td>
</tr>
<tr>
<td>Dictionary Attacks</td>
<td>28</td>
</tr>
<tr>
<td>Hash Tables</td>
<td>29</td>
</tr>
<tr>
<td>Hash Chaining</td>
<td>29</td>
</tr>
<tr>
<td>Iterative Hashing</td>
<td>32</td>
</tr>
<tr>
<td>Salting Passwords</td>
<td>34</td>
</tr>
<tr>
<td>Are Password Tables Safe?</td>
<td>35</td>
</tr>
<tr>
<td>Password Storage Services</td>
<td>35</td>
</tr>
<tr>
<td>A Final Thought</td>
<td>36</td>
</tr>
<tr>
<td>3 WEB SECURITY</td>
<td>37</td>
</tr>
<tr>
<td>How Public-Key Cryptography Solves the Shared Key Problem</td>
<td>38</td>
</tr>
<tr>
<td>Math Tools for Public-Key Cryptography</td>
<td>38</td>
</tr>
<tr>
<td>Invertible Functions</td>
<td>39</td>
</tr>
<tr>
<td>One-Way Functions</td>
<td>39</td>
</tr>
<tr>
<td>Trapdoor Functions</td>
<td>40</td>
</tr>
<tr>
<td>The RSA Encryption Method</td>
<td>42</td>
</tr>
<tr>
<td>Creating the Keys</td>
<td>42</td>
</tr>
<tr>
<td>Encrypting Data with RSA</td>
<td>44</td>
</tr>
<tr>
<td>RSA Effectiveness</td>
<td>45</td>
</tr>
<tr>
<td>RSA Use in the Real World</td>
<td>47</td>
</tr>
<tr>
<td>RSA for Authentication</td>
<td>49</td>
</tr>
<tr>
<td>Security on the Web: HTTPS</td>
<td>52</td>
</tr>
<tr>
<td>Handshaking</td>
<td>52</td>
</tr>
<tr>
<td>Transmitting Data Under HTTPS</td>
<td>54</td>
</tr>
<tr>
<td>The Shared Key Problem Solved?</td>
<td>55</td>
</tr>
<tr>
<td>4 MOVIE CGI</td>
<td>57</td>
</tr>
<tr>
<td>Software for Traditional Animation</td>
<td>59</td>
</tr>
<tr>
<td>How Digital Images Work</td>
<td>59</td>
</tr>
<tr>
<td>How Colors Are Defined</td>
<td>60</td>
</tr>
<tr>
<td>How Software Makes Cel Animations</td>
<td>61</td>
</tr>
<tr>
<td>From Cel Animation Software to Rendered 2D Graphics</td>
<td>69</td>
</tr>
<tr>
<td>Software for 3D CGI</td>
<td>69</td>
</tr>
<tr>
<td>How 3D Scenes Are Described</td>
<td>70</td>
</tr>
<tr>
<td>The Virtual Camera</td>
<td>71</td>
</tr>
<tr>
<td>Direct Lighting</td>
<td>71</td>
</tr>
<tr>
<td>Global Illumination</td>
<td>76</td>
</tr>
<tr>
<td>How Light Is Traced</td>
<td>77</td>
</tr>
<tr>
<td>Full-Scene Anti-Aliasing</td>
<td>80</td>
</tr>
<tr>
<td>Combining the Real and the Fake</td>
<td>81</td>
</tr>
<tr>
<td>The Ideal of Movie-Quality Rendering</td>
<td>82</td>
</tr>
</tbody>
</table>
## 5 GAME GRAPHICS

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

## 6 DATA COMPRESSION

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run-Length Encoding</td>
<td>117</td>
</tr>
<tr>
<td>Dictionary Compression</td>
<td>118</td>
</tr>
<tr>
<td>The Basic Method</td>
<td>118</td>
</tr>
<tr>
<td>Huffman Encoding</td>
<td>120</td>
</tr>
<tr>
<td>Reorganizing Data for Better Compression</td>
<td>121</td>
</tr>
<tr>
<td>Predictive Encoding</td>
<td>121</td>
</tr>
<tr>
<td>Quantization</td>
<td>123</td>
</tr>
<tr>
<td>JPEG Images</td>
<td>123</td>
</tr>
<tr>
<td>A Different Way to Store Colors</td>
<td>124</td>
</tr>
<tr>
<td>The Discrete Cosine Transform</td>
<td>125</td>
</tr>
<tr>
<td>The DCT for Two Dimensions</td>
<td>128</td>
</tr>
<tr>
<td>Compressing the Results</td>
<td>132</td>
</tr>
<tr>
<td>JPEG Picture Quality</td>
<td>135</td>
</tr>
<tr>
<td>Compressing High-Definition Video</td>
<td>136</td>
</tr>
<tr>
<td>Temporal Redundancy</td>
<td>138</td>
</tr>
<tr>
<td>MPEG-2 Video Compression</td>
<td>138</td>
</tr>
<tr>
<td>Video Quality with Temporal Compression</td>
<td>142</td>
</tr>
<tr>
<td>The Present and Future of Video Compression</td>
<td>143</td>
</tr>
</tbody>
</table>
Contents in Detail

7

SEARCH

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

8

CONCURRENCY

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

9

MAP ROUTES

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

INDEX ................................................................................ 191