Contents

1	**Introduction – A Revolutionary Cipher**		1
	1.1	A Traitorous Doctor	1
	1.2	A Few (Vocabulary) Words About Cryptology	5
	1.3	Codes	6
	1.4	Ciphers	8
	1.5	Substitution Ciphers	8
	1.6	Transposition Ciphers	10
	References		11
2	**Cryptology Before 1500 – A Bit of Magic**		13
	2.1	Veni, Vidi, Cipher	13
	2.2	Cryptology in the Ancient World – The Greeks	14
	2.3	Cryptology in the Middle Ages – The Arab Contribution	15
	2.4	Monastic Geniuses and Poets	15
	2.5	Frequency Analysis, The First Cryptanalytic Tool	18
	References		23
3	**The Black Chambers: 1500–1776**		25
	3.1	Bacon vs. Shakespeare	25
	3.2	Crypto Brings Down a Queen: Mary, Queen of Scots	29
	3.3	Nomenclators	34
	3.4	The Black Chambers	36
	3.5	The Next Complexity – Polyalphabetic Substitutions	37
	References		42
4	**Crypto Goes to War: The American Revolution**		43
	4.1	Secret Writing and Espionage	44
	4.2	British Cipher Systems	45
	4.3	American Cipher Systems	52
	4.4	American Diplomatic Cipher Systems	57
	4.5	After the Revolution	60
	References		61

5 Crypto Goes to War: The American Civil War 1861–1865 63
5.1 Technology Goes to War 63
5.2 The Union Tries a Route 64
5.3 Crypto for the Confederates 68
5.4 Solving a Vigenère Cipher – Babbage & Kasiski 69
5.5 Solving a Vigenère – Friedman's Index of Coincidence 71
5.6 Solving a Vigenère – Finding the Key Length 76
5.7 Solving a Vigenère – Barr and Simoson 78
5.7.1 Computing the Keyword Length 78
5.7.2 Finding the Keyword 82
5.8 Conclusion 84
References 85

6 Crypto and the War to End All Wars: 1914–1919 87
6.1 The Last Gasp of the Lone Codebreaker 87
6.2 The Last "Amateur" Cipher Bureau – Room 40 88
6.3 The Americans Start from Behind 94
6.4 America Catches Up: Herbert Yardley and MI-8 95
6.5 The A.E.F. in France 96
6.6 Trench Codes 97
6.7 Ciphers in the Great War – the Playfair 100
6.8 Ciphers in the Great War – The ADFGVX Cipher 102
6.9 The Home Front – Cracking the Waberski Cipher 104
6.10 A New Beginning 113
References 114

7 The Interwar Period: 1919–1941 117
7.1 Room 40 After the War 117
7.2 The U.S.A. – Herbert O. Yardley and the Cipher Bureau 118
7.3 William Friedman and the Signal Intelligence Service 124
7.4 The Other Friedman – Elizebeth Smith Friedman 126
7.5 Agnes Meyer Driscoll, the Navy, and OP-20-G 131
References 135

8 The Rise of the Machines: 1918–1941 137
8.1 Early Cipher Machines 137
8.2 The Rotor Makes Its Appearance 138
8.3 The Enigma 142
8.4 Solving the Enigma – The Polish Mathematicians 145
8.5 SIS vs. Japan: Solving Red and Purple 146
References 150

9 Battle Against the Machines: World War II 1939–1945 151
9.1 How Does the Enigma Work? 151
9.2 Solving the Enigma – Alan, Marian, and the Bombe 154

9.3 SIGABA – Friedman and Rowlett's Triumph 157
9.4 How Does the SIGABA Work? 160
9.5 Women in Crypto During World War II 162
References 164

10 The Machines Take Over: Computer Cryptography 167
10.1 The Shoulders of Giants: Friedman, Hill, and Shannon 167
10.2 Modern Computer Cipher Algorithms – DES 169
10.2.1 How Does the DES Work? 169
10.2.2 The f() Function 171
10.2.3 The Key Scheduler 172
10.2.4 The Security of DES 173
10.3 The Advanced Encryption Standard Algorithm (AES) 175
10.4 Secure Hash Algorithms 179
10.5 Passwords and Password Hacking 181
References 184

11 Alice and Bob and Whit and Martin: Public-Key Cryptography 185
11.1 The Problem with Symmetric Ciphers 185
11.2 Enter Whit and Martin 186
11.3 The Key Exchange Problem 187
11.4 Public-Key Cryptography Appears (and GCHQ Too) 189
11.5 Authentication Is a Problem Too 191
11.6 Implementing Public-Key Cryptography – The RSA Algorithm 192
11.6.1 RSA Key Generation Example 193
11.6.2 Encrypting and Decrypting Example 193
11.7 Analysis of RSA 194
11.8 Applications of Public-Key Cryptography 194
11.9 Elliptic Curve Cryptography 196
References 201

12 Web and Mobile Device Cryptology 203
12.1 Web Security and Cryptology 203
12.2 Mobile Device Security and Cryptology 205
12.3 Wi-Fi Security and Cryptology 207
References 212

13 Cyber Weapons and Cyber Warfare 213
13.1 Cyber Attacks, Types, Players, and Definitions 213
13.2 Malware – Viruses and Worms 216
13.2.1 Computer Viruses 216
13.2.2 Computer Worms 218
13.3 Conficker 219
13.4 Stuxnet 220

13.5 Mitnick, Morris, and Zimmermann 221
13.5.1 Kevin Mitnick, the World's Most Wanted Hacker 221
13.5.2 Robert Tappan Morris and the First Worm 224
13.5.3 Phil Zimmermann and PGP 229
13.6 Playing Defense 233
Appendix: A Simple Linux Virus Program Written in C 234
References 238

14 Cryptology and the Internet of Things 241
14.1 A Day in the Life – All Your Devices Are on the Net Now 241
14.2 The Internet of Things 243
14.2.1 Internet of Things – What Is It 243
14.2.2 What Issues Are There with IoT Security? 244
14.2.3 How to Make IoT Devices More Secure 245
14.3 Security and IoT Devices – Examples 246
14.3.1 IoT Botnets – The Dyn Denial of Service Attack 246
14.3.2 Taking over Household Devices 248
14.3.3 Autonomous Vehicles and the Internet of Things 249
14.4 Conclusion 251
References 252

15 What Is Next in Cryptology? 253
15.1 Quantum Computing 253
15.1.1 What Is Quantum Computing? 254
15.1.2 So What Is the Problem for Cryptography? 256
15.2 Post-quantum Cryptography 258
15.3 Quantum Key Distribution (QKD) 259
References 262

16 Cipher Mysteries 263
16.1 The Voynich Manuscript 263
16.2 The Beale Ciphers 271
16.3 Kryptos 281
Appendix – Beale Cipher Messages #1 and #3 289
References 291

Photo and Illustration Credits 293

Index 299