

CONTENTS IN DETAIL

PREFACE

xix

1

HOW CAN I BREAK AN ENCRYPTED MESSAGE? AND OTHER INTRODUCTORY QUESTIONS

1

What is this book about?	3
Which technical terms do I need to know?	4
How can I break an encrypted text?	5
How do I know what kind of encryption I am dealing with?	7
I have found an encrypted text in the attic; can you decipher it for me?	10
I have encrypted a text myself; can you break it?	11
I have invented a new encryption method; can you take a look at it?	12
I have solved a famous unsolved cryptogram; what should I do?	12
What tools do I need for codebreaking?	13
How can I encrypt my files and email?	14
I have a comment on this book; what should I do?	14
Who contributed to this book?	14

2

THE CAESAR CIPHER

17

How the Caesar cipher works	18
How to detect a Caesar cipher	20
How to break a Caesar cipher	22
Success stories	23
A prison inmate's cipher	23
A spy's encrypted sheet	25
An encrypted journal from the movie <i>The Prestige</i>	26
Challenges	26
Herbert Yardley's first challenge	26
A series of newspaper advertisements from 1900	27

3

SIMPLE SUBSTITUTION CIPHERS

29

How simple substitution ciphers work	31
How to detect a simple substitution cipher	34
Example of a cipher that is not a simple substitution cipher	36
Index-of-coincidence technique	37
How to break a simple substitution cipher	38
Performing a frequency analysis	39
Guessing frequent words	39
Guessing words with unusual letter patterns	40

Success stories	41
How Gary Klivans broke a prison inmate's code	41
How Kent Boklan broke encrypted diary entries from the Civil War	43
Beatrix Potter's diary	44
Challenges	46
A prison code	46
A postcard	46
Another postcard	47
The Friedmans' wedding centennial nickel	47
An Aristocrat from the ACA	48
Unsolved cryptograms	48
An encrypted newspaper ad from 1888	48
The Zodiac Celebrity Cypher	49
The Furlong postcard	50

4

SIMPLE SUBSTITUTION CIPHERS WITHOUT SPACES BETWEEN WORDS: PATRISTOCRATS

51

How a Patristocrat, a simple substitution cipher without spaces, works	52
How to detect a Patristocrat	53
How to break a Patristocrat	54
Frequency analysis using digraphs	54
Word guessing	57
Success stories	57
A prison message	57
The Cheltenham Number Stone	59
Challenges	60
Rudyard Kipling's encrypted message	60
NSA's second Monday Challenge	61
Unsolved cryptograms	61
The Dorabella cryptogram	61
The Chinese gold bars mystery	62
James Hampton's notebook	63

5

SIMPLE SUBSTITUTION CIPHERS IN NON-ENGLISH LANGUAGES

65

Detecting the language used	67
How to break a non-English simple substitution cipher	69
Frequency analysis and word guessing	70
Word pattern guessing	70
Success stories	72
A girl's pigpen cipher (Spanish)	72
The La Buse cryptogram (French)	73
A postcard with a love message (German)	75
A Mafia message (Italian)	77
Challenges	78
An encrypted postcard	78
The third NSA Monday Challenge	78
Christlieb Funk's challenge cryptogram	79

Unsolved cryptograms	80
The Voynich manuscript	80
The cigarette case cryptogram	81
NSA's fourth Monday Challenge	82
The Moustier altar inscriptions	83

6 HOMOPHONIC CIPHERS 85

How homophonic ciphers work	88
How to detect a homophonic cipher	89
How to break a homophonic cipher	91
Success stories	95
The first Zodiac message (Z408)	95
The Zodiac Killer's second message (Z340)	96
Ferdinand III's letters	101
A postcard from Hawaii	104
Challenges	105
A message to the Zodiac Killer	105
Edgar Allan Poe's second challenge	106
Unsolved cryptograms	107
Beale Papers #1 and #3	107
The Zodiac Killer's third message (Z13)	109
The Zodiac Killer's fourth message (Z32)	109
The Scorpion cryptograms	109
Henry Debosnys's messages	110

7 CODES AND NOMENCLATORS 113

Codes	115
Nomenclators	118
Terminology	120
The history of codes and nomenclators	120
Superencryption of codes and nomenclators	123
How to detect a code or nomenclator	124
How to break a code or nomenclator	126
Finding the nomenclator table or codebook	126
Exploiting weaknesses of codes and nomenclators	129
Solving codes and nomenclators with cribs	133
Success stories	133
A telegram sent to Tel Aviv	133
Encrypted messages by Mary, Queen of Scots	134
Collinson's search expedition	138
The Japanese JN-25 code	140
Challenges	142
The Mount Everest telegram	142
Unsolved cryptograms	143
The silk dress cryptogram	143
The train station robbery cryptogram	144
A Pollaky newspaper advertisement	145
Lord Manchester's letter	145

8

POLYALPHABETIC CIPHERS

147

How a polyalphabetic cipher works	148
Vigenère cipher	149
Other polyalphabetic ciphers	150
One-time pad	151
How to detect a polyalphabetic cipher	152
How to break a polyalphabetic cipher	153
Word guessing	153
Checking for repeating patterns (Kasiski's method)	155
Using the index of coincidence	157
Dictionary attacks	159
Tobias Schrödel's method	159
Other Vigenère breaking methods	160
How to break a one-time pad	160
Success stories	161
The Diana Dors message	161
Kryptos 1 and 2	163
The Cyrillic Projector	165
Thouless's second cryptogram from the crypt	169
The Smithy Code	171
Challenges	173
The Schooling challenge	173
A German radio message from the Second World War	173
Unsolved cryptograms	174
Wood's cryptogram from the crypt	174

9

COMPLETE COLUMNAR TRANSPOSITION CIPHERS

175

How complete columnar transposition ciphers work	176
How to detect a complete columnar transposition cipher	179
How to break a complete columnar transposition cipher	179
The arrange-and-read method	180
Vowel frequencies and multiple anagramming	182
Success stories	188
Donald Hill's diary	188
The Pablo Waberski spy case	192
Challenges	193
The Lampedusa message	193
The Friedmans' love messages	194
An encrypted "agony" ad	194
Yardley's eleventh ciphergram	195
Edgar Allan Poe's first challenge	195
An IRA message	196

10

INCOMPLETE COLUMNAR TRANSPOSITION CIPHERS

197

How an incomplete columnar transposition cipher works	198
How to detect an incomplete columnar transposition cipher	201
How to break an incomplete columnar transposition cipher	201

Success stories	206
Kryptos K3	206
Antonio Marzi's radio messages	209
Challenges	216
Yet another IRA message	216
The Double Columnar Transposition Reloaded challenge	216
Unsolved cryptograms	216
The Catokwacopa ad series	216

11 **TURNING GRILLE TRANSPOSITION CIPHERS** **219**

How turning grille encryption works	221
How to detect a turning grille encryption	223
How to break a turning grille encryption	223
Success stories	227
Paolo Bonavoglia's turning grille solution	227
André Langie's turning grille solution	229
Karl de Leeuw's turning grille solution	232
The Mathias Sandorf cryptogram	234
Challenges	239
The Friedmans' Christmas card	239
Jew-Lee and Bill's Cryptocablegram	240
A MysteryTwister challenge	241
A Kerckhoffs cryptogram	241

12 **DIGRAPH SUBSTITUTION** **243**

How general digraph substitution works	244
How the Playfair cipher works	245
How to detect a general digraph substitution	248
How to detect a Playfair cipher	250
How to break a digraph substitution	252
Frequency analysis	253
Dictionary attacks	253
Manual attacks	253
Success stories	267
Thouless's first message	267
Thouless's third message	268
Challenges	270
The cryptogram in National Treasure: Book of Secrets	270
Unsolved cryptograms	270
The world record digraph challenge	270
The world record Playfair challenge	270

13 **ABBREVIATION CIPHERS** **273**

How abbreviation ciphers work	274
How to detect an abbreviation cipher	275
How to break an abbreviation cipher	278
Success stories	279
Emil Snyder's booklet	279

Challenges	281
A birthday card	281
Unsolved cryptograms	282
The Tamám Shud mystery	282
Two unsolved postcards	283

14

DICTIONARY CODES AND BOOK CIPHERS **285**

How dictionary codes and book ciphers work	286
How to detect a dictionary code or book cipher	289
How to break a dictionary code or book cipher.	290
Identifying the book or dictionary	290
Reconstructing the dictionary	290
Treating a book cipher like a simple substitution cipher	293
Success stories	294
The FIDES ads.	294
Nicholas Trist’s key book	295
How William Friedman broke a Hindu conspiracy encryption	296
A dictionary code message sent to Robert E. Lee.	298
Challenges	299
Dan Brown’s book cipher challenge	299
A dictionary code challenge.	300
Unsolved cryptograms	301
Two encrypted newspaper advertisements from 1873	301

15

ADDITIONAL ENCRYPTION METHODS **303**

Cipher tools.	304
Voice encryption	305
Code talking	306
Shorthand (stenography).	307
Hidden messages (steganography).	309
Success story: How Elonka found a hidden message on a tombstone.	313
Success story: Deciphering Steganographia	315
Success story: Mysterious Stranger message.	320
Challenge: Another steganographic message by the Friedmans	321
Cipher machines	322

16

SOLVING CIPHERS WITH HILL CLIMBING **329**

Solving simple substitution ciphers with hill climbing	331
Simulated annealing	336
Success story: Bart Wenmeckers’s solution to the Baring-Gould cryptogram	337
Success story: The Florida murder case cryptogram.	338
Solving a homophonic cipher with simulated annealing	340
Success story: Dhavare, Low, and Stamp’s Zodiac Killer solutions	340
Solving a Vigenère cipher with hill climbing	341
Success story: Jim Gillogly’s solution to IRA Vigenère cryptograms	342
Solving a columnar transposition with hill climbing.	343
Success story: Jim Gillogly’s solution to IRA transposition cryptograms	344

Success story: Richard Bean's solution to the last unsolved IRA cryptogram . . .	346
Success story: George Lasry's solution of the double columnar transposition challenge	348
Solving a turning grille cipher with hill climbing	349
Success story: Bart Wenmeckers's solution to a turning grille cryptogram	350
Success story: Armin Krauss's solution to a turning grille challenge	352
Solving a general digraph substitution with hill climbing	353
Success story: Some digraph challenges	353
Solving a Playfair cipher with hill climbing	354
Success story: Dan Girard's solution to the Cheltenham Letter Stone	355
Success story: Playfair world records	356
Solving machine ciphers with hill climbing	358
Success story: Breaking original Enigma messages	358

17
WHAT NEXT? 361

More unsolved cryptograms	362
The fourth Kryptos message (K4)	362
The Rubin cryptogram	363
Ricky McCormick's encrypted notes	364
The carrier pigeon message from World War II.	364
The encrypted NKRYPT pillars.	366
Even more unsolved cryptograms	370
Codebreaking tools	371
Other books about codebreaking.	371
Websites about codebreaking	375
Journals and newsletters	377
Events	377

A
KRYPTOS 379

B
USEFUL LANGUAGE STATISTICS 389

C
GLOSSARY 395

D
MORSE CODE 403

E
FIGURE SOURCES 405

F
REFERENCES 417

INDEX 447