

INDEX

A

- abbreviation ciphers, 10, 273–283, 395
 - breaking, 278–279
 - challenges, 281
 - detection, 275–278
 - success stories, 279–281
 - unsolved cryptograms, 282–283
- ACA. *See* American Cryptogram Association
- acrostic, 311
- Action Line, 279
- Adams, Douglas, 154
- additional encryption methods, 303–328
- additive list, 141
- Adelaide, Australia, 282
- Adirondack Enigma* (Farnsworth), 110
- AEIOU (Habsburg motto), 102
- AES, 12, 14, 331, 373
- “AF is short on water,” 141
- Agony Column Codes & Ciphers, The* (Palmer aka Gaffney), 5, 27, 194, 217, 295
- Akemi, Tachibana, 60
- Akins, Tyler, 13, 54
- Aleardi, Aleardo, 210
- Algorithmic Cryptanalysis* (Joux), 373
- Alice and Bob (placeholder names), 5
- Allies (wartime), 250, 312, 325, 328
- almanacs, 290
- alphabets, nonstandard, 34, 195, 314, 317, 323, 353, 400
- Amagiri* (Japanese warship), 250
- American Black Chamber, The* (Yardley), 26, 192, 375
- American Cryptogram Association (ACA), 11, 34, 52, 151, 220, 376, 395
 - convention, 377
 - members, 342, 344, 364, 382
 - publications, 4, 377
 - puzzles, 49
- American Revolutionary War, 288–289, 311
- America’s Most Wanted*, 109
- Amsterdam, 232
- anagram. *See* transposition ciphers
- anagramming, multiple, 182, 184, 202, 208, 235, 237
 - codebreaking tricks, 187
- “Analyzing Spanish Civil War Ciphers by Combining Combinatorial and Statistical Methods” (Sanguino), 305
- Anderson, Deb (Desch), 326
- anonymous codebreaker, 267
- anonymous message, 176
- Antal, Eugen, 371, 376
- apple tree, 309
- Applied Cryptanalysis: Breaking Ciphers in the Real World* (Stamp and Low), 373
- Arctic expedition, 139
- Aristocrat ciphers, 34, 48, 52, 89, 104, 154, 395
- Arlington National Cemetery, 313–315
- Arnold, Benedict, 288
- Arnsberg, Germany, 75
- ASCII code, 315, 395, 398
- Ask Metafilter website, 279
- Aston, Philip, 188–192
- astronomy code, 126–127
- Atlanta, Georgia, 378
- Auer, Leopold, 101
- Aurebesh writing system, 46
- Australia, 170, 282, 346, 366
 - coastwatchers, 250–251, 312
- Austria, 101–102, 372

- Austrian army, 228
 Awesome Con, 378
 AZDecrypt software, 98, 340, 371
- B**
- backward writing, 177, 238, 339
 Bacon, Francis, 314, 321
 Baconian cipher, 314, 322
 Baigent, Michael, 171
 Bales, Mike, 167
 bankruptcy, 163
 Banyuwangi, Indonesia, 140
 Baring-Gould, Sabine, 331, 337
 Baring-Gould cryptogram, 336
Basic Cryptanalysis (US Army Field Manual), 372
Battle of Wits (Budiansky), 326
 battleship, 173, 250, 312
 Baudot code, 327, 396
 Bauer, Craig, 62, 159, 328, 364, 370, 373
 Bauer, Friedrich, 373
 Baumann, Christian, 31, 371
 Beale, Thomas J., 86, 107
 Beale ciphers, xix, 288–289, 362, 387
 Paper #1, 107
 Paper #2, 86
 Paper #3, 107
 Bean, Richard, 170, 346
 “Because it’s there!”, 142
 Bedford County, Virginia, xix, xxi, 86
 beer barrel cork, 134
 Beinecke Rare Book & Manuscript Library, 66, 80
 Belfield, Richard, 370
 Belgium, 83, 340, 353
 Bellaso, Giovan Battista, 149
 Benthin Sanguino, Luis Alberto, 305
 BERLIN (*Kryptos* hint), 362
 Bhattacharjee, Yudhijit, 26
 Bible, 318
 Bibliothèque nationale de France (BnF), 136
 Biermann, Norbert, 135–136, 138, 301, 353
 Bigram challenges, 270, 353
 binary arithmetic, 398
 binary code, 152, 305, 315, 398
 Bion’s gadgets, 371
 Birmingham, England, 327
 birthday cards, 224, 281
 Bisno, Peter, xxii, 63
 Biwy (nickname), 194
Black Beauty (Sewell), 269
 Blackstone, William, 288
 Blaine, David, 320
 Bletchley Park, 30, 141, 325, 359
 blog challenges, 248, 270–271, 300, 352, 356
 Blue code, 326
 Boklan, Kent D., 43
 Bollig, Randall, 167
 bomba kryptologiczna, 325
 Bombe, 326
 Bonavoglia, Paolo, 120, 133, 227, 350, 376
 book ciphers, 88, 90, 124, 287, 289–290, 293, 296, 299, 301–302
 books, recommended, 372
 Borden, Alfred, 26
 Borges, Raymond, 47
 Borrás, José, 287, 296
 Bosbach, Thomas, 68, 298
 Brandt, Willy, 348
 breaking an encryption, 4, 5–7
Breaking German Navy Ciphers (Hörenberg project), 359
Breaking German Wehrmacht Ciphers (Weierud project), 359
 Briden, Jeff, 321
 Briere, Bill, 47, 149, 240
 Brisbane, Australia, 170, 346
 British codebreakers, 114, 140, 325.
 See also Bletchley Park
 British Library, 295
 British Royal Air Force, 366
 British Tabulating Machine Company, 326
 Bromley, UK, 283
 Brooks comet, 129
 Brown, Dan, xx, 171, 299, 318
 Broza, Gil, 106
 Brucia, Charlie, 338
 brute force, 22–23, 25, 340
 Budiansky, Stephen, 326
 Buford’s Tavern, xix, 87
 Burr, Aaron, 289

C

- C-35 encryption machine, 323
- Caesar cipher, 18–22, 115, 396, 400–401
 - breaking, 22–23
 - detection, 20
 - NKRYPT* sculpture, xxii, 366–370
 - other language, 78
 - part of other cipher types, 149–150, 156–157, 164
- Cage, Nicolas, 306
- cake, 178
- calculators, 188
- Call of Duty: Black Ops III* computer game, 38
- Canada, 306
- Canberra, Australia, 366
- Can You Crack the Enigma Code?* (Belfield), 370
- Cardan grille, 311
- carrier pigeons, 234, 364
- Carter, Howard, 209, 386
- celebrity ciphers, 49
- cell phones, 305
- cemeteries, 31, 313
- Cenerentola, 21
- Central Intelligence Agency (CIA), 36, 148, 163, 362, 379–381
- challenges. *See also Kryptos*; metapuzzle
 - abbreviation cipher, 281
 - Bigram, 270, 353
 - blog, 248, 270–271, 300, 352, 356
 - book cipher, 299
 - Caesar cipher, 27
 - ciphergrams (Yardley), 26–27, 195
 - code, 142
 - complete columnar transposition cipher, 193–196
 - DCT, 216, 348
 - dictionary code, 300
 - digraph substitution, 353
 - double columnar transposition, 216, 348–349
 - Friedman, Elizabeth and William, 315, 322
 - Funk, Christlieb Benedict, 79
 - homophonic cipher, 105
 - incomplete columnar transposition cipher, 216
 - non-English cryptograms, 65–83
 - NSA Monday Challenges, 53–57, 61, 78, 82–83
 - Playfair, 270, 356
 - Poe, Edgar Allan, 106, 195
 - polyalphabetic cipher, 173
 - simple substitution cipher, 47, 79, 195
 - transposition cipher, 195
 - turning grille, 239–240, 352
 - Vigenère cipher, 173
 - Zodiac, 89
- Chamberlain Observatory, Colorado, 127
- Charles I of England, xxii, 121
- Charlotte, North Carolina, 165
- Charlotte International Cryptologic Symposium, viii
- cheesecake, 177–178
- Cheltenham, UK, 59, 355
- Cheltenham *Listening Stones*, 59–60, 352–353, 355–356
- Cherokee code talkers, 306
- Chicago, Illinois, 296–297, 322
- chiffre indéchiffable, 153
- chimney, 356, 364
- Chinese gold bars mystery, 62
- Choctaw code talkers, 62–63
- Christmas cards, 221, 239
- Christmas Carol, A* (Dickens), 308
- Christmas present, 82
- Christos's *Military and Intelligence Corner*, 376
- CIA. *See* Central Intelligence Agency
- cigarette case cryptogram, 81
- Cipherbrain* blog, xxi, 11, 60, 279, 299, 375
- cipher cylinders, 304
- cipher disks, 304, 322
- The Cipher Foundation website, 371
- Ciphergrams* (Yardley), 195
- Cipher History website, 376
- cipher machine, 322, 376
- Cipher Mysteries* blog, 83, 375
- ciphers, 4, 13, 396
- cipher slides, 304, 322
- Cipher Solving Assistants website, 371
- ciphertext, 4, 396
- cipher-tool challenge, 305

- cipher tools, 13, 304–305, 322, 376, 399
- Cipher Tools website, 13, 54, 153, 371
- ciphony, 305
- Clark, Andrew, 162
- cleartext, 4, 396
- Clifton's Nouveau Dictionnaire Français*, 286
- Clinton, Henry, 289, 311
- CLOCK (*Kryptos* hint), 362
- coconut, 312
- Code 13040, 115–116
- Code Book, The* (Singh), 373
- Code Book for Young People, The* (Singh), 373
- codebooks, 4, 116, 141, 145, 289, 326
- Codebreakers, The* (Kahn), 296, 315, 373
- codebreaking, 4, 126, 396
 - books about, 371–375
 - tools, 13, 371
- codegroups, 116, 141, 396
- Code of Love, The* (Linklater), 188, 192
- codes, 4, 115, 373, 396
 - detection, 124
 - one-part, 116
 - two-part, 116
- Codes, Ciphers and Secret Writing* (Gardner), 293
- code talking, 306–307
- Cold War, 151, 167, 200, 305, 307, 310, 328, 348
- Collier, Price, 298
- Collinson, Richard, 138–140
- Collinson newspaper ads, 22, 138–140
- Colossus, 327
- columnar transposition ciphers, 176, 343, 394, 396. *See also* complete columnar transposition ciphers; incomplete columnar transposition ciphers
 - solving with hill climbing, 343–344
- Comanche code talkers, 306
- comets, 127
- Commentaries on the Laws of England* (Blackstone), 288
- complete columnar transposition ciphers, 175–187, 344
 - breaking, 179–187
 - detection, 179
- computer-based steganography, 312
- computer files and emails, encryption
 - of, 14
- copper sheets, 380
- CORAL, 326
- cork, 134
- cornfield, 364
- Cornwallis, Charles, 289
- Corr, Frank, 167
- court trials, 135, 171, 297, 338, 340
- COVID-19, *xxi*
- Cracking Code Book, The* (Singh), 373
- Cracking Codes & Cryptograms for Dummies* (Sutherland and Koltko-Rivera), 374
- Cracking Codes with Python* (Sweigart), 373
- cribs, 5, 397
 - AZDecrypt option, 98
 - dictionary code, 293
 - digraph substitution, 252
 - FIDES cryptogram, 294–295
 - incomplete columnar transposition, 201–202, 207
 - IRA cryptogram, 346
 - Kryptos*, 208
 - manual attacks, 253–267
 - mechanical ciphers, 326
 - one-time pad, 160
 - Playfair cipher, 253
 - solving codes and nomenclators, 126, 133
 - turning grille, 223
 - word guessing, 57
- criminal ciphers, 23, 41, 46, 49, 57, 95, 109–110, 144, 338, 364. *See also* Irish Republican Army; spies
- Cross Island, 251
- crossword encryption, 220
- CRRU, 25, 338, 340, 364
- Cruise Wilkins, Reginald, 74
- cryptanalysis, 4, 397
- Cryptanalysis* (Gaines), *xx*, 160, 187, 267, 372
- Cryptanalysis and Racketeering Records Unit (CRRU), 25, 338, 340, 364

- Cryptiana website, 298, 376
 CryptoBooks.org, 375
 Cryptocablegram, 240
 CryptoCrack, 371
 cryptogram, 4, 397
Crypto-Gram (Schneier newsletter), 376
Cryptogram, The (ACA publication), 377
 Cryptograms & Classical Ciphers
 Facebook group, 350, 376
 “Cryptograms from the Crypt”
 (Gillogly and Harnisch), 270
Cryptographie Militaire, La
 (Kerckhoffs), 223
 cryptography, 4, 397
Cryptography (Langie), 72, 229, 267,
 290, 372
Cryptologia journal, 377
Cryptolog newsletter, 83
 cryptology, 5, 397
 Crypto Museum website, 323, 376
 CrypTool
 CrypTool 1, 159
 CrypTool 2, 13, 55, 70, 330, 354
 YouTube channel, 375
 JCrypTool, 350
 project, 13, 344, 397
 website, 375
 CryptoPrograms website, 371
 Cumberbatch, Benedict, 326
Curiosities of Olden Times (Baring-
 Gould), 331
 cyanide, 363
 Cylob cryptogram, 370
 Cypher, 274
 Cyrillic alphabet, 165, 167–168
Cyrillic Projector sculpture, 165, 375, 387
 Czech language, 393
- D**
 D’Agapeyeff cryptogram, 370
Daily Telegraph (London), 301
 Danish language, 393
Daphnis (journal), 318
 Dartmouth College, 106
 Davidsch, 299
 Davies, Donald, 327
Da Vinci Code, The (Brown), xx,
 171–172, 299
 Dawson, Mark, 161–162
 Dayton, Ohio, 326
 Dayton Codebreakers, 326
 dCode website, 13, 157
 DCT. *See* double columnar
 transposition
 D-Day, 328, 366
 Debosnys, Henry, 110–111
 decipher, 397
 Declaration of Independence (US), 86,
 288, 290
 DECODE database, 370, 376
Decoding the IRA (Gillogly and Mahon),
 342, 344, 346
Decrypted Secrets (Bauer), 373
 decryption, 4, 397
 DeepL, 377
 DEF CON, 378
De furtivis literarum notis (della Porta), 244
Demystifying the Bombe (Turing), 326
 Denslow, Ray V., 274
 DES, 331, 373
 Desch, Joseph, 326
 Design 215 Word Pattern Finder, 371
 DESPARATLY. *See* *Kryptos*: spelling errors
 Detroit, Michigan, 279
Detroit Free Press, 279
 Deutsches Museum, 30
 Devil’s Chimney, 356
 Dhavare, Amrapali, 340–341
 diaries, encrypted, 3, 43, 44, 188, 210, 304
 Dickens, Charles, 308
 dictation machines, 308
 dictionary
 attack, 253
 on double columnar
 transposition, 349
 on Playfair, 269, 354–358
 on Vigenère, 159
 codes, 285–301
 breaking, 290
 challenge, 300
 detection, 289
 example, 10
 English, 288, 290, 295, 299
 Entick’s Spelling Dictionary, 288
 Johnson’s Pocket Dictionary of the
 English Language, 295

- dictionary (*continued*)
- Langenscheidt's Lilliput Dictionary*
 - English-German*, 289
 - Nathan Bailey's Dictionary*, 288
 - Noah Webster, William Greenleaf*
 - Webster Dictionary*, 299
 - word list, 277
 - Diffie-Hellman, 14, 373
 - digraph, 54, 94, 192, 208, 251, 343, 354, 397
 - nonoverlapping, 249
 - overlapping, 249
 - substitution, 252, 353, 398
 - breaking, 252
 - detection, 248
 - Diné, 306
 - distributed computing, 359
 - Doppelkasten, 247
 - Dorabella cryptogram, xxii, 61–62
 - Dorking, UK, 366
 - Dors, Diana, 161
 - Double Box method, 247
 - double columnar transposition (DCT), 200, 210, 216, 398
 - challenge, 348
 - DCT Reloaded, 216, 349
 - doubled letters, 392
 - Dovenberg, Bob, 367
 - downhill step, 336
 - Doyle, Arthur Conan, 145, 290
 - Dragon Con, 378
 - drawings, 309
 - Dreadnought*, HMS, 173
 - Driscoll, Agnes Meyer, 141
 - duel, 289
 - Dunin, Elonka, iv, viii, xix–xxii, 313–315, 370, 375–378
 - Kryptos* work, 382–387
 - Dunin, Stanley, 167
 - Dunin-Schmeh substitution, 394, 398
 - Duran-Fairport cipher, 398
- E**
- EAST (*Kryptos* hint), 362
 - East Germany, 348
 - Egypt, 209
 - Eisenhower, Dwight D., 328
 - Ekhall, Magnus, 357
 - Elementary Cryptanalysis* (Sinkov), 372
 - Elgar, Edward, 62
 - Elizabeth I, 134, 138
 - elonka.com, 375, 382
 - “Elsbeth,” 194
 - “Encrypted Books List” (EBL), xxii, 80
 - English frequency mnemonic, 390
 - English language statistics, 92, 189, 277–288, 290, 299, 312, 389, 393, 394
 - Enigma, 3, 324, 330, 358, 398
 - Enigma* (movie), 326
 - Enigma* magazine, 144
 - Entick's Spelling Dictionary*, 288
 - Ernst, Thomas, 102–103, 318–320
 - Esoteric* (Oddfellows), 280–281
 - Essex County, New York, 110
 - Esslinger, Bernhard, 13, 216, 344, 354, 373
 - Estes, Lance, 382
 - Evans, Reginald, 250–251, 312
 - Evening Standard* (London), 27, 179, 194, 216–217
 - exclusive-or operation (XOR operation), 152, 398
 - Eycke, Jarl Van, 340, 353, 371
- F**
- Fabyan, George, 321
 - Facebook, 53
 - Fagone, Jason, 194, 313
 - Fagone, Peter P., 129
 - Fair Game* (movie), 370
 - Fairport Convention, 151
 - Farnsworth, Cheri, 110
 - Farsi language, 282
 - faulty cipherment, 322
 - FBI, 25, 338, 364. *See also* Cryptanalysis and Racketeering Records Unit
 - Ferdinand III (Holy Roman emperor), 101–104
 - Feynman Ciphers, 370
 - Fibonacci numbers, 172
 - FIDES cryptograms, 294–295
 - Figl, Andreas, 372
 - final letter frequencies, 93
 - Finland, Finnish language, 68–69, 392, 394

Fisher, Jackie, 172–173
 fitness function, 253, 331–357
 FitzGerald, Edward, 282
 Fleissner grille, 221. *See also* turning grille transposition ciphers
 Fleissner von Wostrowitz, Edouard, 221
 Flohansen, 279
 Flossenbürg concentration camp, 359
 Flowers, Thomas H., 327–328
 fonts, 46, 314, 318
 Fort Meade, Maryland, 377, 381
 44CON, 378
 France, 145, 398
 Franklin, Benjamin, 89
 Franklin, John, 139
 Frasnés-lez-Anvaing, Belgium, 83
 Freedom of Information Act
 Request, 382
 Freemasons, 274–276, 279
 Freemason’s cipher. *See* pigpen ciphers
 French cryptogram, 194
 French language, 72, 78, 235, 241, 277, 286, 301, 389–390, 394
 frequency analysis, 6, 88, 91, 130, 371, 398
 Friedman, Elizebeth, xxi, 194, 239–240, 313–315, 321, 326
 Friedman, William, xxi, 141, 158, 182, 194, 239–240, 296, 313–315, 326, 372
 Friedman test, 159
 Friedman tombstone, 313–315, 375
 Funk, Christlieb Benedict, 79
 Funk’s challenge, 79
 Furlong, George, 50
 Furlong, Lizzie, 50

G

Gaffney, Tony (aka Jean Palmer), 5, 20, 48, 194, 217, 295
 Gaines, Helen Fouché, 123, 160, 187, 267, 372
 gang codes, 23, 41
 Gardner, Martin, 293
 Garlick, Ryan, 13
 Gasa, Biuku, 250, 312
 GCHQ, Cheltenham, UK, 59, 180–181, 355

gelignite (explosive), 346
 Gelsenkirchen, Germany, xix
 General Wang, 62
 geocaching, 3, 19, 91, 384
 George C. Marshall Research Library, xxi, 313
 German language, 68, 82, 192, 228, 232, 277, 310, 351, 389–390, 392, 394
 Germany, 30, 114, 359, 366
 army, 228, 247, 327
 chancellor, 348
 U-boats, 325
Germany and the Germans (Collier), 298
 ghosts, 315
 Giacobini comet, 129
 Gillogly, Jim, 171, 196, 199, 202, 206, 269, 342, 346, 382
 Giordano, Robert, 371
 Girard, Dan, 356, 359
 “The Gold Bug” (Poe), 106
 Google Translate, 376–377
 Government Communications
 Headquarters (GCHQ), 59, 180–181, 355
Graham’s Magazine, 106
 Greek letters and symbols, 318–319
 Greeks, 310
 Gregg, John Robert, 308
 Gregg shorthand, 308
 Gross Island (aka Nauru), 251
 Gruber, Bernhard, 279
 GSM mobile phone standard, 306
 Guillaume, Günter, 348
 Guy, John, 138

H

Hagelin C-35, 323
 Hamburg, Germany, 173
 Hamidullin, Konstantin, 357
 Hamilton, Alexander, 288–289
Hamilton (musical), 288
 Hampton, James, 63–64
 handwritten note, 313
 Hannon, Ed, 382
 Hansky, Karsten, 2, 18, 78, 80, 126, 133
 Hanson, Chris, 376
 Harden, Bettye, 95–96

- Harden, Donald, 95
Harnisch, Larry, 171, 269–270
Have His Carcase (Sayers), 255, 257, 354
Hawaii, 104, 141
Hayes, Richard, 160
Heidel, Wolfgang Ernst, 320
Heidel’s cryptogram, 320
Heinz Nixdorf MuseumsForum, 30
Helm, Louie, 353
heptagraph, 398
Hermes, Jürgen, 315, 320
Herodotus, 310
Hester’s Way Park, 59
hexagrams, 54, 170, 346, 354, 356, 398
High Wycombe, UK, 366
Hill, Brian, 167
Hill, Donald, 188
hill climbing, 329–359, 373
 with dictionary attacks, 159
 with digraph substitution, 252, 270
 with double columnar transposition, 216
 with Enigma, 359
 with homophonic ciphers, 91
 with nomenclators, 129, 136–137
 with Pristocrats, 54
 with polyalphabetic ciphers, 153
 simulated annealing variation, 136, 336–337, 340, 356–357
 tools, 371
 with transpositions, 202
 with turning grilles, 223, 228, 233
Hindu conspiracy, 296
HistoCrypt, 120, 138, 377
Hitchhiker’s Guide to the Galaxy, The (Adams), 154, 157
Hitler, Adolf, 327
Hitt, Parker, 267, 372
Holmes, Jasper, 141
Holmes, Sherlock, 145, 290
Holy Blood, Holy Grail (Baigent and Leigh), 171
homophones, 88, 119, 121, 130, 398
homophonic cipher, 85–111, 340, 399
 detection, 89
 history, 120
 with nomenclator table, 137
 solving with hill climbing, 340–341
Hong Kong, 188
Hoover, Harry, 382
Hörenberg, Michael, 359
hostages, 311
Houck, Bill, 167
“The Hound of Heaven” (Thompson), 171
hourglass cipher, 311
House of Habsburg, 101
Howe, William, 311
“How the First Letter Was Written” (Kipling), 60
How to Wreck a Nice Beach (Tomkins), 306
Hungary, 237, 376
- I**
IBM, 141
IC. *See* index of coincidence
ice cream, 325
Imitation Game, The (movie), 326
incomplete columnar transposition ciphers, 197–217, 396
 breaking, 201
 detection, 201
 solving with hill climbing, 343
index of coincidence (IC), 37, 53, 69, 83, 152, 157, 163, 179, 248, 339, 393, 399
Index of Coincidence and Its Applications in Cryptology, The (Friedman), 394
India, 296
Indian Ocean, 73
initial letter frequencies, 93, 292
Inside Enigma (Perera and Perera), 326
IQLUSION. *See* Kryptos: spelling errors
IRA. *See* Irish Republican Army
Irish Confederate Wars, 130
Irish Republican Army (IRA), 198, 202, 216, 342, 344, 374
Irvine, Andrew, 142
Iserlohn, Germany, 75
Italian army, 228
Italian language, 132, 390–392, 394
- J**
JADE, 326
Jahr, Hans, 377
Japan, 115, 140–142, 188, 250, 326–328

jewelry, 310
 JN-25, 140–142
 Johnson, Cliff, 321
Johnson's Pocket Dictionary of the English Language, 295
 jokes, 234
 journals, encrypted. *See* diaries, encrypted
 Joux, Antoine, 373
Jungle Book, The (Kipling), 60
Just So Stories (Kipling), 60

K

Kahn, David, 61, 296, 315, 326, 373
 Kasiski's method, 156, 164
Katkryptolog blog, 377
 Kennedy, John F., 250, 312
 Kerckhoffs, Auguste, 223, 241
 key, 4, 399
 key search, exhaustive, 22
 keywords, 4, 399
 Kipling, Rudyard, 60–61
 Klivans, Gary, 23, 41–43, 46
 KL-7, 323
 Knauß, Gordian, 280
 KNOWLEDGE IS POWER, 313
 Knox, Dilly, 326
 Kohlhausen, Stuart, 366–370
 Kolker, Anatoly, 167
 Koltko-Rivera, Mark, 374
 Kopal, Nils, 338–340, 349, 356, 375
 Krah, Stefan, 358
 Krauß, Armin, 104, 210, 279, 352
 Kryha Standard, 323
 Kryptografie website, 377
Kryptos, 148, 163, 202, 207, 362, 378–379
 discussion group, 167, 376, 387
 K1, 207, 381–383
 K2, 207, 381–385
 K3, 206–207, 381–382, 385–387
 K4, 362–363, 381–382, 386–387
 maquette, 148–150, 152–153, 158
 meeting, 148, 378
 question marks, 207, 385
 spelling errors, 164–165, 383–385
 Kuhlemann, Oliver, 377
 Kullback, Solomon, 372
 Kumana, Eroni, 312

L

“La Buse” (Olivier Levasseur), 73
 La Crittografia da Atbash a RSA website, 376
 Laitner, Bill, 279
 Lampedusa, Italy, 193
 lamps representing ciphertext, 323
 Láng, Benedek, 376
Langenscheidt's Lilliput Dictionary English-German, 289
 Langie, André, 72–73, 229–232, 267, 290–293, 372
 Langley, Virginia, 148, 206, 362, 379, 381. *See also* *Kryptos*
 language detection, 65–83
 language statistics, 389–394
 Lann-Briere, Jew-Lee, 47, 149, 240
 La Réunion, 73
 Lasry, George, 138, 216, 346, 349, 356, 373
 Las Vegas, Nevada, 378
 Latin, 52, 62, 80, 102–103, 118, 166, 300, 309, 315–318, 320
 latitude and longitude, 3, 165, 368, 384
 Laurel, Maryland, xix
 Layton, Edwin T., 142
Learning and Experiencing Cryptography with CrypTool and SageMath (Esslinger and CrypTool team), 373
 Leckhampton Hill, UK, 356
 Lee, Robert E., 298
 Leeuw, Karl de, 120, 232–234
 Leiberich, Otto, 348–349
 Leigh, Richard, 171
 Leighton, Albert, 130
 lemons, lemon juice, 180, 310
 Leopold Wilhelm, 101–102
 letter frequencies, 20–21, 389. *See also* frequency analysis
 letter pair substitution, 153
 letter pattern search, 371
 letters, encrypted, 3, 41, 49, 101, 134, 296, 304
 Letter Stone, 59, 355–356
 Levasseur, Olivier, 73–74
 Lexington, Virginia, xxi

- life-after-death experiments, 169–170,
174, 246–247, 267–269
- Lima, Ohio, 144
- Lima Times Democrat*, 144
- Linder, Leslie, 44
- linguistic computer programs, 307
- Linklater, Andro, 188, 192
- listening post, 286
- Listening Stones* sculpture, 59–60,
352–353, 355–356
- Litscape word finder tools, 371
- Lloyd, Greg, 367
- local maximum, 336
- London, England, 32, 115, 142, 325
newspapers, 5, 20–22, 138, 145,
216, 294
- Lord’s Prayer, 279
- Lorenz SZ40/42 machine, 327
- Lost Symbol, The* (Brown), iv, viii, xx
- Louis Round Wilson Special
Collections Library, 298
- Love in Code* (McCormick), 193
- love notes, 19, 23, 43, 71, 75–76, 188,
192–194, 225–227, 321–322
- Low, Richard M., 340, 373
- LTE mobile phone standard, 306
- M**
- M-138, 305
- M4 project, 358–359
- Macbeth* (Shakespeare), 268
- machine ciphers, 326–327, 330, 373
solving with hill climbing, 358–359
- Macrakis, Kristie, 311
- Madison, James, 120–121
- Mafia, Italian, 77
- magic communication, 315
- Mahon, Tom, 202, 342, 344, 346
- Mallory, George, 142
- Mammoth Book of Secret Codes and
Cryptograms* (Dunin), xx, 3,
23, 49
- Manchester, Lord, 145–146
- Manchester cryptogram, 145–146
- manual cipher, 3, 12, 382, 399
- Manual for the Solution of Military Ciphers*
(Hitt), 267, 372
- maquette (*Kryptos*), 148
- Markov models, hidden, 160
- Marsigli, Luigi, 119
- Mary, Queen of Scots, 134–138
- Marzi, Antonio, 209–215
- MASC, 31
- Masonic ciphers, 274–275, 279, 375
- Masonic Conservators, The* (Denslow), 274
- Masonic fable, 88
- mathematical tables, 188
- Mathias Sandorf* (Verne), 234
- matrix, 222
- Matyas, Stephen M., 295–296
- McClurg’s bookstore, Chicago, 297
- McConnell, Mike, 381–382
- McCormick, Donald, 193
- McCormick, Ricky, 364
- McDaniels, Denny, 382
- McElhiney, Larry, 376
- McIntosh, Glenn, 367
- McVey, John, 126, 134
- Mediterranean Sea, 193
- Meer, Hans van der, 232
- Megyesi, Beáta, 120
- metallurgy, 337
- metapuzzle, ii, 1, 117, 220, 309, 317, 319,
398, 410, 420, 436
cards, 178, 224, 227
cartoons, 29, 197, 243, 309, 361
license, 148, 410
NKRYPT, 368
music, 148, 219, 394, 396
1-1-2 1-2-3 1-4-7 1-4-6 1-4-3 1-2-
5 1-5-1 1-4-5 10-12-4 6-1-3
2-5-1 4-1-2 7-1-3 4-2-1 3-2-1 2-2-
10 1-4-1, 288
- “A Methodology for the Cryptanalysis
of Classical Ciphers with
Search Metaheuristics,”
(Lasry), 373
- Mexico, 114, 192, 286, 295
- MI-8, 286
- Midway, 141–142
- Military Cryptanalysis, Parts I–IV*
(Friedman), 182, 372
- Miller, Ken, 382
- Miranda, Lin-Manuel, 288
- Mistress Wilding* (Sabatini), 348
- Mitchell, Douglas W., 220

- mLH cipher, 370
- mnemonic book, 275–276
- Monge, Alf, 267, 271, 356
- monoalphabetic substitution ciphers, 31, 52, 150. *See also* simple substitution ciphers
- Monroe, Marilyn, 161
- Montgomery, Pennsylvania, 46
- Morning Post*, 177
- Morse code, 178, 197, 305, 307, 315, 380, 399, 403–404
- mottoes
 - Habsburg, 102
 - United States, 300
- Mount Everest telegram, 142
- Moustier, Belgium, altar inscriptions, 83
- movies
 - Enigma*, 326
 - Fair Game*, 370
 - Imitation Game*, 326
 - National Treasure: Book of Secrets*, 270
 - Prestige, The*, 26
 - Star Wars*, 46
 - Windtalkers*, 306
- Multi-Dec website, 371
- multiple anagramming, 182, 184, 187, 202, 208, 235, 237–238
- multiplication tables, 188
- murders, 282, 363
- Mysterious Stranger* (Blaine), 320–321
- MysteryTwister, 11, 210, 216, 241, 305, 341, 375

- N**
- Nashville, Tennessee, 378
- Nathan Bailey's Dictionary*, 288
- National Cryptologic Museum, 30, 104
- National Library of France, 138
- National Puzzlers' League, 144, 376
- National Security Agency (NSA), 11, 30, 53, 377, 381
 - Monday Challenges, 1, 3, 53, 61, 78
 - Symposium on Cryptologic History, xix, 47, 240, 377
- National Treasure: Book of Secrets* (movie), 270
- National Union of Racing Pigeons (NURP), 366
- Nauru (aka Gross Island), 251
- Navajo code talking, 116, 306
- Nazi spy cryptogram, 370
- Newberry Library, 296
- New Headquarters Building, CIA, 380
- Newman, Walter C., 276
- newspaper ads, encrypted, 5, 145
 - Collinson ads, 138–140
- New York, 23, 43, 52, 110, 133, 378
- New York Times*, 320, 362
- New Zealand, 228, 376
- n*-factorial, 177
- n*-graph, 55, 350
- Nicht zu knacken* (Schmeh), 370
- Nimitz, Chester W., 142
- NKRYPT*, 366–368
- Noah Webster, William Greenleaf Webster Dictionary*, 299
- nomenclators, 90, 118, 120, 309, 399
 - breaking, 126
 - Charles I of England, used with letter from, 121
 - detection, 124
 - Lord Manchester, used with letter from, 145–146
 - Mary, Queen of Scots, used with letters from, 134–138
 - one-part, 120
 - two-part, 120
- nonoverlapping digraphs, 249–250
- nonstandard alphabet, 34, 195, 245, 314, 317, 353, 400
- Normandy, 328, 366
- NORTHEAST (*Kryptos* hint), 362
- North Pole, 229
- notebooks, encrypted, 10, 228. *See also* diaries, encrypted
- notes
 - abbreviation cipher, 277
 - encrypted, 180, 192, 229, 282, 288, 298, 363–364
 - handwritten, 313
 - love, 194
 - private, 188
 - steganographic, 250
- NSA. *See* National Security Agency
- nullifiers, 121

nulls, 120–121, 130–131, 134, 211, 215,
223, 228, 247, 399
Number Stone, 59–60, 355
NURP, 366

O

Oahu, Hawaii, 141
octagraphs, 343, 353–354, 399
Oddfellows, 280
odometer, 323
Olson, Dan, 25
Olson, Edwin, 371
Olsson, John, 58
one-time pad, 151–152, 305, 366,
398, 400
 breaking, 160–161
OP-20-G, 141
Operation Barbarossa, 359
Operation Overlord, 328
Oranchak, Dave, 90, 144, 371, 376
Ostwald, Olaf, 359
Oval Office, 312
overlapping digraphs, 249

P

Pacific Theater, 306
palimpsest, 382
Palmer, Jean. *See* Gaffney, Tony
papal cipher, 130
paper-and-pencil cipher, 2–3, 399
paper tape, 327
paperweight, 312
paranormal methods, 169, 174
parapsychology, 246, 267
Patristocrat ciphers, 51–57, 60, 104, 400
 breaking, 54–56
 detection, 53
Pearl Harbor, 141
Pelling, Nick, 74, 83, 144, 280, 371, 375
pen name, 5
Pennsylvania, 280
Penny, Dora, 62
pentagraph, 54, 400
Perera, Dan, 326
Perera, Tom, 326
Persian language, 282
Perwich, William, 118–119
Peterson International Code, 134

PGP, 14
Phelippes, Thomas, 134–135
Philadelphia, Pennsylvania, 363
Philadelphia International Airport, 363
PhreakNIC v3.0 Code, 375, 378
Piccolomini, Octavio, 102–104
pigeon message, 364–366
pigpen ciphers (aka Freemason
 ciphers), 30, 47, 72, 74, 161,
 367, 400
Pilcrow, Phil, 371
pilot, military, 188
Pitman, Isaac, 308
Pitman shorthand, 307–308
plaintext, 4, 400
Playfair, Lyon, 246
Playfair Analyzer (CrypTool 2), 354
Playfair cipher, 243–244, 246, 354–355,
 372, 400
 1936 record, 30 letters, 271
 breaking, 253
 challenge, 356
 24-letter challenge, 271
 50-letter challenge, 356
 cryptogram properties, 251
 detection, 250
 matrix, 246
 rules, 247, 254
 world records, 356
Plum Pudding Island, 250
pocketknife, 312
Poe, Edgar Allan, 32, 106, 195
poems
 in abbreviation ciphers, 277
 by Debosnys, Henry, 110–111
 “The Hound of Heaven”
 (Thompson), 171
 Poems of Solitary Delights (Akemi), 60
 Selected Poems of Francis
 Thompson, 170
 “Un giovinetto pallido e bello”
 (Alerdi), 210
poison, 282, 363
Poland, 141, 398
 Enigma team, 324–328
 Polish language, 393
 Poznań, 325
 Warsaw, 257

police. *See also* FBI
 Australian, 382
 Italian, 77
 UK, 58
 US, 95, 105, 144, 338, 364

polio, 176

Polk, James K., 287

Pollaky, Ignatius, 145

polyalphabetic ciphers, 115, 147–174,
 304, 372, 400–401
 books, 371
 breaking, 153
 detection, 152
 Heidel’s cryptogram, 318
 Thouless’s ciphers, 169–170, 174,
 246–247, 267–269
 tools, 304

Pommerening, Klaus, 234–238

“Pomp and Circumstance” (Elgar), 62

Porta, Giambattista della, 244

Portal of Historical Ciphers website,
 371, 376

Portugal, Portuguese language, 66, 394

postcards, encrypted, 2, 10, 34, 46,
 49–50, 66, 68, 75, 78, 104, 109,
 177, 283, 304, 307, 309

Potomac River, 381

Potter, Beatrix, 44–46

Prestige, The (movie), 26

prisoner ciphers, 23, 41, 46, 110, 188,
 311, 338

prisoner exchange, 348

prisoner of war, 188

Prisoners, Lovers, and Spies (Macrakis), 311

Prohibition era in US, 313

Project Gutenberg, 170, 357

Psalms 51, 318

pseudonyms, 21

psychic phenomena, 79, 169

PT-109 torpedo boat, 250, 312

punch card tabulating machine, 141

punched paper tape, 327

PURPLE (machine), 141, 326

PVL cryptograms, 369–370

Q

Questacon Science and Technology
 Centre, 366

question mark (*Kryptos*), 207, 385
 Quipqup, 371

R

Rabson, John, 138

radio message, encrypted, 173–174,
 209–215, 286, 322, 326,
 358–359

rail fence cipher, 220

Randi, James, 79

Random House, 171

Rasterschlüssel 44 cipher, 220

Rayburn cryptogram, 370

rebellion in India, 296

recommended reading, 371–375

Red Book code, 327

Reeds, Jim, 316–318, 320

reflector, 325. *See also* Enigma

Regan, Brian, 25–26

Rejewski, Marian, 325

Rejtjtelek, kódok, titkosírások
 website, 376

Renza, Louis, 106

repeating patterns, 155–157

Reuvers, Paul, 376

reward, monetary, 269

Reynard, Robert, 373

Riga, Latvia, 357

Rilke cryptogram, 370

Rio de Janeiro, Brazil, 173

“Rising for the Moon” (song), 151

Ritchie, John, 126–129

Riverbank Laboratories, 313, 322

Rivers-Cofield, Sara, 143

Robert (blog reader), 60

Rochefort, Joseph, 141

Rockville, Maryland, xix

Rohonc Codex, 370

Roman numerals, 211

Romanovs, 266

Roosevelt, Franklin D., 176

ROT-13, 19, 23, 115, 400

rotor cipher, 323, 367

Rous, Anne-Simone, 120

route transposition cipher, 220

Rowlett, Frank, 141, 326

Royal Air Force Bomber
 Command, 366

- Różycki, Jerzy, 325
 RSA, 14, 373
Rubaiyat of Omar Khayyam, The
 (FitzGerald translation), 282
 Rubik's Cube encryption, 220
 Rubin, Paul, 363–364
 rumrunner, 313
Russel's Mathematical Tables, 188
 Russia, Russian language, 68, 165, 393
- S**
- Sabatini, Raphael, 348
 Sacco, Luigi, 133, 227–228, 350–351
 Salinas, California, 95
 Sanborn, Jim
Cyrillic Projector, 165–168
Kryptos, 163–165, 362–363,
 379–387
 maquette, 148–149
 San Francisco, California, xxi, 49, 109
 SantaColoma, Richard, 66, 81
 Sarasota, Florida, 338
 Sayers, Dorothy L., 255, 257, 354
 Scheidt, Ed, 148
 Schmeh, Klaus, xiv–xxii, 12,
 153–154, 320
 books, iv, 12, 310, 370, 375
Cipherbrain blog, xxi, 216, 375
 challenges, 248, 270–271, 300,
 357–358
 Emil Snyder's booklet,
 279–280
 solved cryptograms, 58, 60,
 72, 76, 170, 294–295,
 298–299, 338, 346–347,
 352–353, 355–356
 unsolved cryptograms, 50, 82
 cryptologic travel guide, 31
 DCT challenge, 348–349
 “Encrypted Books List” (EBL), 80
 “Top 50 Unsolved Cryptograms”
 list, 61, 370
 Schneier, Bruce, 12, 376
Schneier on Security blog, 376
 Schooling, John Holt, 173
 Schrödel, Tobias, 67, 76, 159, 228
 Schrödel's method, 159–160
 Schuyler, Philip, 288
Science Observer Code, The, 127–128
 Scorpion cryptograms, 109–110
 Scotland Yard, 296
Scrabble, 39
 scytale, 304, 367
Secret Code Breaker: A Cryptanalyst's
Handbook (Reynard), 373
Secret History (Bauer), 159, 328, 373
Secrets of the Lost Symbol (Brown), iv, xx
Seizing the Enigma (Kahn), 326
Selected Poems of Francis Thompson, 170
 Sewell, Anna, 269
 Shakespeare, William, 169, 246,
 268, 321
Shakespearean Ciphers Examined, The
 (Friedman and Friedman), 321
 Shakespeare-Bacon debate, 321
 Shanghai, China, 62
Sheahan's Telegraphic Cipher Code, 117, 197
 Shermer, Michael, 79
 ShmooCon, 378
 shorthand, 178, 224, 227, 309, 400
 Siemens & Halske T52, 323
 Signal Intelligence Service (SIS), US
 Army, 141, 326
 SIGSALY (machine), 305
 silk dress cryptogram (and possible
 solution), 143
 Simons, Marc, 376
 simple substitution ciphers, 29–50, 106,
 304, 353, 372
 breaking, 38–41
 detection, 34–37
 “The Gold Bug” (Poe), 106
 in non-English languages, 65–83
 Patristocrats, 51–64, 195
 solving with hill climbing, 331–340
 Simpson, Ralph, 376
 simulated annealing, 336–337, 340,
 352, 356–357
 Sinagra, Filippo, 210
 Singh, Simon, 373
 Sinkov, Abraham, 123, 372
 Slovakia, Slovak language, 371, 376–377
 Smith, Joseph P., 338
 Smith, Peter, 171
 Smithsonian American Art Museum, 63
 Smithy Code, 171–172, 375

Snyder, Emil, 279–281
 Solomon Islanders, 250, 312
Solution of a Playfair Cipher (Monge), 267
 Somerton Beach, 282
 Somerton Man, xxii, 282–283, 375
 songs, 151
 South America, Nazi ciphers in, 326
 Spain, 296
 Spanish language, 73, 287, 389–390, 394
 Speirs, Dale, 307
Spektrum der Wissenschaft, 348
 spelling alphabet, 307
Spelling Book, The, 274
 spies, 152, 192–193, 200, 220, 310, 348
 squirrel cryptogram, 368–370
 Stamp, Mark, 340, 373
Star Wars, 46
Statistical Methods in Cryptanalysis
 (Kullback), 372
 steganalysis, 312
Steganographia (Trithemius), 102,
 315–320, 361
 steganography, 5, 188, 309, 401
 Stehle, Ferdinando, 386
 Stein, David, 163, 207, 382
 stencils, 221, 311
 stenography, 308, 401
 St. Louis, Missouri, 364
 St Martin’s church, Belgium, 83
 stockbroker codes, 116
Stones, Listening, 59–60, 352–353,
 355–356
 Stott, William, 366
 Strasser, Gerhard, 309
 strip ciphers, 304
 Stuart, Mary, 134–138
 Studeman, William O. “Bill,” 381–382
 substitution ciphers, 401. *See also* simple
 substitution ciphers
 substitution table, 43

Beale cryptograms, 57
 Cheltenham Number Stone, 59–60
 definition, 4, 401
 digraph, 244
 Ferdinand III’s letters, 101–103
 hill climbing, 331–343
 NSA, 56–57
 Potter, Beatrix, 45

prison inmate, 24, 43
Steganographia, 320
 Zodiac Killer, 99
 Sullivan, Geoff, 359
 Sunnyvale, California, xxi
 super-encryption, 123, 141, 401
 SURPRISE (keyword), 246
 Surrey, UK, 364
 Survival Research Foundation, 269
 Sutherland, Denise, 374
 Sweden, Swedish language, 68, 357,
 376, 394
 Sweigart, Al, 373
 Switzerland, 72, 353
 sympathetic inks, 310–311
 Symposium on Cryptologic History,
 xix, 47, 240, 377
Systeme des Chiffrierens (Figl), 372
 SZ40/42, 327

T

Tamám Shud (aka Somerton Man)
 cryptogram, xxii, 282–283
 Tel Aviv, 133
 telegrams, encrypted, 3, 18, 124, 133,
 193, 240, 287, 289
 astronomers’, 126–129
 Mount Everest, 142
 silk dress, 143–144
 train station robbery, 144
 Zimmermann, 114–116
 telegraphy, 115–116, 123
 telephones, 305–306
 telephony, 305
 temperature, 336
 Tench, Dan, 172
 Tenzer, Christoph, 149
 tetragraphs, 54, 184, 187, 254,
 369–370, 401
 The cake is a lie, 178
 Thirty Years’ War, 101
 Thompson, Francis, 170–171
 Thouless, Robert, 169–170, 174,
 246–247, 267–269
*Throne of the Third Heaven of the Nations’
 Millennium General Assembly*
 (Hampton), 63
 Thuringia, 82

- Tiltman, John, 141, 327
Times, The (London), 5, 138, 145, 294
 Toebes, John, 371
 Toebes, Mary Ellen, 371
 tombstones, 31, 313, 315, 321
 Tomokiyo, Satoshi, 126, 135–136, 138, 298
 Tompkins, Dave, 306
 tracing paper, 229–231
 train station robbery cryptogram, 144
 transcript, 33
 transposition ciphers, 176, 188, 194, 220, 372, 401. *See also* columnar transposition ciphers; turning grille transposition ciphers
 treasure
 Beale, xix–xx, 86–88, 107–109
 Dors, Diana, 161–163
 La Buse, 73–75
 Mysterious Stranger, 320–321
 Triantafyllopoulos, Christos, 376
 trigraphs, 54, 269, 352, 392, 401
 Trist, Nicholas, 287–288, 295–296
 Trithemius, Johannes, 102, 315
True Principles of the Spanish Language (Borras), 287–288, 296
 Tunny (Lorenz SZ40/42), 327
 Turing, Alan, 182, 325–326
 Turing, Dermot, 326
 Turing Test, 182
 Turkish language, 394
 turning grille transposition ciphers, 221, 349, 401
 detection, 223
 Tutankhamun, 209, 386
 Tutte, William T., 327
 Twickenham, 366
 Twitter, 53, 313
 Twomey, Moss, 342, 346–347
 Tyler, W.B., 32, 106, 195
 typewriter, 323
- U**
- Udine, Italy, 210–211
 umlauts, 69, 228, 232
 UMTS mobile phone standard, 306
 UNDERGRUUND. *See Kryptos*: spelling errors
 “Un giovinetto pallido e bello” (Aleardi), 210
 United Kingdom
 colonies, 296
 Government Communication Headquarters (GCHQ), 59, 180–181, 355
 military, 188
 Royal Air Force, 366
 United States
 Army, 141, 193, 306, 313
 Signal Intelligence Service (SIS), 141, 326
 Civil War, 298
 Coast Guard, 173, 313
 Declaration of Independence, 86, 288, 290
 Department of Justice, 297
 Founding Fathers, 89, 120, 288
 motto, 300
 Navy, 141, 250, 313
 Oval Office, 312
 Papers of the Continental Congress, 89
 Pearl Harbor, 141
 president, 120, 176, 250, 287, 312
 Prohibition, 313
 Revolutionary War, 288–289, 311
 vice president, 289
United States Diplomatic Codes and Ciphers (Weber), 295
 United States Geological Survey, 384
Universal Code of Signals, 138–139
 University of Illinois at Chicago, 195
 University of North Carolina, Chapel Hill, 298
 University of North Carolina at Charlotte, 165–166
 University of Poznań, 325
 University of Surrey, 188
 University of Uppsala, 371, 376
Unsolved! (Bauer), 61–62, 268, 364, 370, 373
 unsolved cryptograms, 33, 48–50, 63, 66, 80–83, 110–111, 143–145, 163–164, 174, 216, 270, 282–283, 301

Beale, 86–88, 107–109
Dorabella, 61–62
Kryptos, 147–149, 362–363, 379–387
lists of, 11, 362–363, 370–371, 373,
375–377
NKRYPT, 367–370
reporting solutions of, 4, 12–13
Voynich manuscript, 80–81
Zodiac Killer, 96–100, 109
Usenet, 353

V

Vaasa, Finland, 68
Vatican, 120, 122, 130–131
VeraCrypt, 14
Vernam, Gilbert S., 152
Vernam cipher, 152, 398
Verne, Jules, 234
Versteckte Botschaften (Schmeh), 310
Vienna, Austria, 101
Vigenère, Blaise de, 149
Vigenère cipher, 149–153, 162–169,
381, 401
 breaking, 155–160
 detection, 152–153
 solving with hill climbing, 341–343
vinyl records, 305
violinist, 358
Viterbi analysis, 160
vocoders, 306
voice digitalization, 306
voice encryption, 305–306
voice radio, 305–306
vowel frequencies, 182–187
vowel-to-consonant ratio, 182
Voynich, Wilfrid, 80
Voynich manuscript, xxii, 66, 80–81,
375, 387

W

Waberski, Pablo, 192–193
Wacker, Arno, 216, 349
Wales, 162
Walsh, John, 109
Walsingham, Francis, 134–135, 137
Wang, General, 62
war journal, encrypted, 210

Warsaw, Poland, 257–258
Warzin, Gary, 376
Washington, DC, xix, 313, 377–378
water purification, 141
wax tablet, 310
Weber, Ralph E., 295–296
Weierud, Frode, 124, 359
Welchman, Gordon, 325
Wells, Elizabeth, 110
Wenmeckers, Bart, 228, 337, 350, 376
Western Ohio Railway, 144
Whalen, Terence, 106, 195–196
Wheatstone, Charles, 246
Wheel of Fortune, 338
Whitaker's Almanac, 290
Wikipedia, 352–353, 390
Wilhelm, Leopold, 101–102
William V, Prince of Orange, 232
Wilson, David Allen, 298
Windtalkers (movie), 306
Wink, Inkeri, 68
Winslet, Kate, 326
Witzke, Lothar, 192
Woman Who Smashed Codes, The
 (Fagone), 313, 374
Wood, T.E., 169, 174
word guessing, 57, 70, 154, 292
word lengths, 392
word pattern guessing, 70–71
words, most frequent, 392
World Bank, 167
WorldCon, 378
world records, xxii, 270, 356
World War I, 322, 372
 book cipher, 296–298
 code talking, 306
 dictionary code, 286
 transposition ciphers, 192, 195,
 227–229
 Zimmermann Telegram, 114
World War II
 carrier pigeon message, xxii,
 364–366
 codes, 123, 140–142
 code talking, 306–307
 dictionary codes, 289
 encryption machines, 326–328

- World War II (*continued*)
 Enigma, 324–326, 358–359, 372, 398
 female codebreakers, 374–375
 Hill, Donald, diary of, 188–192
 Playfair, 247, 250–251
 radio messages, 173–174, 209–215
 steganography, 312
 transposition ciphers, 200, 220
 voice encryption, 305
 Wostrowitz, Edouard Fleissner von, 221
 Wouw, Richard van de, 134
 writing, invisible, 310
- X**
 X02, 366
 XOR operation (exclusive-or operation), 152, 398
 XRZAH, 238
- Y**
 Yale University, 66, 80
 Yardley, Herbert, 26–27, 192–193, 195, 286, 374
 Young, Gordon, 59–60, 355
- Z**
 Z (NSA organization), 382
 Zandbergen, René, 81
Zentralstelle für das Chiffrierwesen (ZfCh), 348
 Zimmermann, Arthur, 114
 Zimmermann, Philip, 14
 Zimmermann Telegram, 114–116
 Zodiac Killer
 AZDecrypt software, 98, 340, 371
 copycat, 52
 Celebrity Cypher, 49
 Scorpion cryptogram, 109–110
 “How to Know That You Haven’t Solved the Zodiac-340 Cipher” (Garlick), 13
 messages, 387, 418
 police challenge, 89–90, 105
 solutions, 12–13, 95, 97–98, 340–341
 tools, 340, 371
 web pages, 376, 405, 425
 Z13 cryptogram, 109
 Z32 cryptogram, 109
 Z340 cryptogram, 13, 96–97, 341
 homophonic substitution table, 99
 Z408 cryptogram, 95, 340
 Zygalski, Henryk, 325
 ZZ Top, 300