INDEX

Numbers

0-RITT data, 245
2G mobile communications, 89
3DES (triple DES), 59, 72–74. *See also* DES (Data Encryption Standard)
3G mobile communications, 91, 128
4G mobile communications, 78, 91, 128, 129

A

A5/1, 18, 88–91
Aaronson, Scott, 171, 178, 259, 269
Advanced Encryption Standard (AES), 53, 59
- AddRoundKey, 60
- block size, 54
- vs. DES, 59, 80
- and GCM, 152–154, 159, 161
- implementations, 62–64
- internals, 59–62
- KeyExpansion, 60
- MixColumns, 60
- with Poly1305, 138
- and provable security, 48
- security of, 65
- ShiftRows, 60
- SubBytes, 60
- and TLS 1.3, 243–244

Advanced Vector Extensions (AVX), 55
AE. *See* authenticated encryption (AE)
AEAD (authenticated encryption with associated data), 16, 149, 157–158
AES. *See* Advanced Encryption Standard (AES)
AES-CBC, 69
`AESENC` instruction, 64
`AESENCLAST` instruction, 64
AES-GCM
- efficiency, 154
- internals, 152–153
- security, 154
- and small tags, 161
- and weak hash keys, 159–161

AES native instructions (AES-NI), 63–64
AEZ, 161–162
AKA (authenticated key agreement), 205–207
algebraic attacks, 85
Alvisi, Lorenzo, 125
amplitude, 252–253
Apple, 218, 231
application-specific integrated circuit (ASIC), 79
associated data, 149
asymmetric encryption, 1, 15. *See also* RSA (Rivest–Shamir–Adleman)
attack costs, 43–44
attack models, 10
- black-box, 11–12
- for key agreement protocols, 207
- gray-box, 12

authenticated ciphers, 148
- with associated data, 149
- functional criteria, 151–152
- nonces, 149–150
- online, 151
- performance, 150–151
- permutation-based, 157–158
- security, 150
- streamability, 151

authenticated decryption, 148
authenticated Diffie–Hellman, 210–213
authenticated encryption (AE), 16, 145
- AES-GCM, 152–154, 159–161
- autheticated ciphers, 148–152
- OCB, 155–156

authenticated encryption (AE), *continued*
  permutation-based AEAD, 157–158
  SIV, 156–157
  using MACs, 146–148
authenticated encryption with associated data (AEAD), 16, 149, 157–158
authenticated key agreement (AKA), 205–207
authentication tag, 16. *See also* authenticated encryption (AE); MACs (message authentication codes)
AVX (Advanced Vector Extensions), 55

B

backtracking resistance, 26
backward secrecy, 26
`BcryptGenRandom()` function, 33–34
Bellare, Mihir, 143
Bellaso, Giovan Battista, 3
Bellcore attack, 196–197
Bernstein, Daniel J., 52, 95, 100, 136, 139, 230, 231, 261
big-number libraries, 192
binary exponentiation, 192
birthday attacks, 109
birthday paradox, 109
Bitcoin, 106
bit security, 42–43
BLAKE, 120
BLAKE2, 215, 226
  BLAKE2b, 123
  BLAKE2s, 123
  compression function, 124
  design rationale, 123
blinding attacks, 189
block ciphers, 53. *See also* Advanced Encryption Standard (AES)
  block size, 54–55
  CBC mode, 67–70
  codebook attacks, 55
  CTR mode, 71–72
  decryption algorithm, 54
  ECB mode, 65–67
  encryption algorithm, 54
  Feistel schemes, 58–59
  key schedule, 56
  meet-in-the-middle attacks, 72–74
  modes of operation, 65
  padding oracle attacks, 74–75
  rounds, 56
  round keys, 56–57
  security goals, 54
  slide attacks, 56–57
  substitution–permutation networks, 57–58
Bluetooth, 78
Boneh, Dan, 199
Bos, Joppe W., 233
broadcast attack model, 95
Brumley, David, 199
brute-force attacks, 41, 90

C

CA (certificate authority), 238–240, 247–248
cache-timing attacks, 63
Caesar cipher, 2–3
CAESAR competition, 161
Canetti, Ran, 143
carry-less multiplication (`CLMUL`), 153
CBC. *See* cipher block chaining (CBC)
CBC-MAC, 134
CCA (chosen-ciphertext attackers), 11
CCM (counter with CBC-MAC), 162, 243
CDH (computational Diffie–Hellman), 204
certificate authority (CA), 238–240, 247–248
certificate chain, 239, 247
ChaCha20, 95, 120, 138, 243–244
chaining values, 112
Chinese remainder theorem (CRT), 195–196
chosen-ciphertext attackers (CCA), 11
chosen-message attacks, 129
chosen-plaintext attackers (CPA), 11
Chrome browser, 118, 231
Chuang, Isaac, 269
ciphers, 1
cipher-based MAC (CMAC), 134–135
cipher block chaining (CBC), 67–69.
  ciphertext stealing, 70
  padding, 69–70
  padding oracle attacks, 74
ciphertext, 2
ciphertext-only attackers (COA), 11
ciphertext stealing, 70
C language, 63

Clay Mathematics Institute, 46, 171
client certificate, 246
clique problem, 169
CLMUL (carry-less multiplication), 153
closest vector problem (CVP), 264–265
CMAC (cipher-based MAC), 134–135
CMAC-AES, 157
ciphertext-only attackers (COA), 11
code-based cryptography, 263–264
codebook attacks, 55, 90–91
Codenomicon, 248
coding problems, 179
Cohen, Henri, 233
Cold War, 53
collision resistance, 109, 113
complexity. *See* computational complexity
complexity class, 168
complex numbers, 253
compression functions, 111
- in BLAKE2, 124
- Davies–Meyer construction, 114
- in Merkle–Damgård construction, 112–113
- in SHA-1, 117

computational complexity, 164
- bounds, 167
- classes, 168
- comparison, 166
- constant factors, 165
- constant time, 166
- exponential, 165, 167
- exponential factorial, 167
- linear, 165
- linearithmic, 165
- polynomial, 166–168
- quadratic, 165
- superpolynomial, 166–168

computational complexity theory, 163
computational Diffie–Hellman (CDH), 204
computational hardness, 164
computational security, 40–41
confidentiality, 1, 106
confusion, 57
constant-time implementations, 142
Coppersmith, Don, 199
counter mode (CTR), 71–72, 91, 152
counter with CBC-MAC (CCM), 162, 243
CPA (chosen-plaintext attackers), 11
CRCs (cyclic redundancy checks), 106
CRT (Chinese remainder theorem), 195–196
CryptAcquireContext() function, 34
CryptGenRandom() function, 33–34
Crypto++, 199
Cryptocat, 37
cryptographic security, 39. *See also* security
CTR (counter mode), 71–72, 91, 152
cube attacks, 85
Curve448, 244
Curve25519, 230–231, 244
Curve41417, 231
CVP (closest vector problem), 264–265
cyclic redundancy checks (CRCs), 106

D

Dahlin, Mike, 125
Damgård, Ivan, 111, 126
Data Encryption Standard. *See* DES (Data Encryption Standard)
Datagram Transport Layer Security (DTLS), 237
Davies–Meyer construction, 114, 117, 124
decisional Diffie–Hellman (DDH)
- assumption, 205
- problem, 204–205

decryption, 2
dedicated hardware, 79
DeMillo, Richard A., 199
DES (Data Encryption Standard), 53, 80
- 3DES, 59, 72–74
- vs. AES, 59, 80
- block size, 54
- double DES, 73
- Feistel schemes in, 58–59

deterministic random bit generator (DRBG), 14, 25, 78
/dev/random, 32–33
/dev/urandom, 30–32
Diehard, 29
differential cryptanalysis, 98–99
Diffie, Whitfield, 201
Diffie–Hellman problem, 178
Diffie–Hellman (DH) protocol, 201
- anonymous, 209–210
- authenticated, 210–213
- CDH problem, 204
- DDH problem, 204–205
- function, 202

Diffie–Hellman (DH) protocol, *continued*
- generating parameters, 202–203
- and key agreement, 205–208, 225–229
- MQV protocol, 213–214
- and shared secrets, 202, 214–215
- in TLS, 215, 242–243
- twin problem, 205
- unsafe group parameters, 215–216

diffusion, 57
digest, 106
DigiNotar, 248
digital signatures, 106, 182, 188–189
discrete logarithm problem (DLP), 174–176
- and CDH problem, 204
- ECDLP, 224–225
- and Shor's algorithm, 259, 260

distribution. *See* probability distribution
`drand48`, 28
DRBG (deterministic random bit generator), 14, 25, 78
DTLS (Datagram Transport Layer Security), 237
Durumeric, Zakir, 36

E

ECB (electronic codebook), 65–67
ECC (elliptic-curve cryptography), 217
ECDH (elliptic-curve Diffie-Hellman), 226, 232–233
ECDSA. *See* elliptic curve digital signature algorithm (ECDSA)
ECDLP (elliptic curve discrete logarithm problem), 224–225
ECIES (elliptic curve integrated encryption scheme), 229
Ed448-Goldilocks, 231
Einstein–Podolsky–Rosen (EPR) paradox, 252
elliptic curves, 217–218, 244
- addition law, 221
- Curve448, 244
- Curve25519, 230–231
- Curve41417, 231
- Edwards curves, 219
- groups, 224
- with integers, 219–220
- NIST curves, 230
- order, 224
- point at infinity, 222, 224
- point doubling, 222–223
- point multiplying, 223
- prime curves, 230
- Weierstrass form, 218

elliptic-curve cryptography (ECC), 217
elliptic-curve Diffie-Hellman(ECDH), 226, 232–233
elliptic curve digital signature algorithm (ECDSA), 226
- and bad randomness, 232
- vs. RSA signatures, 227–228
- signature generation, 226
- signature verification, 226–227

elliptic curve discrete logarithm problem (ECDLP), 224–225
elliptic curve integrated encryption scheme (ECIES), 229
embarassingly parallel, 43, 90
Encapsulating Security Payload (ESP), 241
encrypt-and-MAC, 146–147
encryption, 1
- asymmetric, 15
- at-rest, 15
- in-transit, 15
- randomized, 13
- security, 9

encrypt-then-MAC, 147–148, 152
entanglement, 252, 255
entropy, 23–24, 35–36
entropy pool, 25
EPR (Einstein–Podolsky–Rosen) paradox, 252
error-correcting codes, 263
ESP (Encapsulating Security Payload), 241
eSTREAM competition, 86, 103
*e*th roots, 185
Euler's theorem, 198
Euler's totient function, 183
exponentiation, 192, 194
extended Euclidean algorithm, 184

F

factorials, 6
factoring methods, 172

factoring problem, 46, 171
  and **NP**-completeness, 173–174
  solving with Shor's algorithm, 259–260
factorization, 172–173, 176–177
fast correlation attacks, 85
fault injection, 196–197
FDH (Full Domain Hash), 190–191
feedback shift registers (FSRs), 80–82
  cycle, 82
  feedback function, 80
  linear, 83–85
  nonlinear, 86
  period, 82
Feistel schemes, 58–59
Ferguson, Niels, 26, 161
FHE (fully homomorphic encryption), 17
field-programmable gate array (FPGA), 79
filtered LFSR, 85
first-preimage resistance, 108
fixed points, 114
Flame, 126
forgery attacks, 128
format-preserving encryption (FPE), 16–17
Fortuna, 26–27
forward secrecy, 26, 208
  in authenticated DH, 211
  in TLS 1.3, 246–247
Fouque, Pierre-Alain, 143
FOX, 58
FPGA (field-programmable gate array), 79
frequency analysis, 4
Frey, Gerhard, 233
FSRs. *See* feedback shift registers (FSRs)
full diffusion, 99
Full Domain Hash (FDH), 190–191
fully homomorphic encryption (FHE), 17

G

GCD (greatest common divisor), 36, 184, 195, 260
GCHQ (Government Communications Headquarters), 202
GCM (Galois Counter Mode), 146, 152, 161. *See also* AES-GCM
`gcm_ghash_clmul` function, 153
general number field sieve (GNFS), 173, 204
`getrandom()` system call, 33
GHASH, 152–154, 159–160
Gilbert, E.N., 136
Git, 105
GitHub, 51
Gmail, 248
GMR-1, 103
GMR-2, 103
GNFS (general number field sieve), 173, 204
GNU Multiple Precision (GMP), 192
GnuPG, 52
Go, 140, 191, 193
Goldberg, Ian, 35
Goldwasser, Shafi, 19
Google, 118, 248
  Chrome, 231
  Internet Authority, 239
GOST, 53, 59
Govaerts, René, 126
Government Communications Headquarters (GCHQ), 202
Grain-128a, 86–88
graphics processing unit (GPU), 91
greatest common divisor (GCD), 36, 184, 195, 260
Grøstl, 120
groups, 174
  axioms, 175
  commutativity, 175
  cyclic, 175
  finite, 175
  generator, 175
  in RSA, 182–183
Grover's algorithm, 260
GSM mobile communication, 78
guess-and-determine attacks, 89–90

H

Hadamard gate, 256–257
Halderman, Alex, 36, 233
hardness assumption, 174
hard problems, 163. *See also* computational complexity
  closest vector problem, 264
  discrete logarithm problem, 174–176
  factoring problem, 171–174
  learning with errors, 264

hard problems, *continued*
- multivariate quadratic equations, 265
- **NP**-complete problem, 169–170
- and provable security, 46–47
- **P** vs. **NP** problem, 170–171
- short integer solution, 264

hardware, 63, 102
hash-based cryptography, 266–267
hash-based MACs, 132–133
hash functions, 105. *See also* Merkle–Damgård (M–D) construction
- 3-collisions, 113
- collisions in, 109–111
- compression functions, 112
- Davies–Meyers construction, 114
- in digital signatures, 106
- iterative, 111
- keyed, 127
- multicollisions, 113
- noncryptographic, 106
- preimage resistance, 107–109
- in proof-of-storage protocols, 125–126
- and **P** vs. **NP** problem, 171
- security notions, 106
- sponge functions, 115–116
- universal, 136–137
- unpredictability, 107

hash values, 106
Heartbleed, 248–249
Hellman, Martin, 201
Heninger, Nadia, 36, 233
heuristic security, 48–49
HMAC-based KDF (HKDF), 215, 244
HMACs (hash-based MACs), 132–133
host-based intrusion detection system (HIDS), 105
HTTPS, 237
- insecure, 154, 178
- keys for, 49, 52
- over TLS, 94, 215, 236

I

iCloud, 248
identity gate, 256
IES (integrated encryption scheme), 229
IETF (Internet Engineering Task Force), 152
IKE (Internet Key Exchange), 134
imaginary number, 253
IND-CPA, 13–14
indifferentiability, 126
indistinguishability (IND), 12–13, 129
informational security, 40
initial value (IV), 67–69, 112, 135
integrated encryption scheme (IES), 229
integrity, of data, 16, 106, 128
Intel, 30
Internet Engineering Task Force (IETF), 152
Internet Key Exchange (IKE), 134
internet of things (IoT), 235
intractable problems. *See* hard problems
invalid curve attack, 232
invasive attacks, 12
ion traps, 262
ipad, 132
IPSec (Internet Protocol Security), 128, 132, 134, 148, 152
iterative hashing, 111
IV (initial value), 67–69, 112, 135

J

Jager, Tibor, 233
Java, 19
JH, 120
Jovanovic, Philipp, 158

K

KDF. *See* key derivation function (KDF)
Keccak 121–123. *See also* SHA-3
Kelsey, John, 26, 38, 45
Kerckhoffs, Auguste, 4, 10
Kerckhoffs's principle, 10–11
key agreement protocols, 49, 202, 205
- AKA, 205–207
- attack models, 207
- breaches, 207, 211, 214
- data leaks, 207, 212
- eavesdroppers, 207, 211
- forward secrecy, 208
- performance, 208
- security goals, 207–208

key confirmation, 212, 214
key control, 208

key derivation function (KDF), 49
  in DH functions, 202, 215
  in ECIES, 229
  in TLS 1.3, 243–244
key generation, 49–50
key-generation algorithm, 50
key scheduling algorithms (KSAs), 11, 92
key wrapping, 50
knapsack problem, 169
known-message attack, 128
known-plaintext attackers (KPA), 11
known-plaintext attacks (KPAs), 89
Knudsen, Lars, 47
Kohno, Tadayoshi, 26
Kotla, Ramakrishna, 125
Kozierok, Charles, 237
Krawczyk, Hugo, 143, 216
Krovetz, Ted, 156
KSAs (key scheduling algorithms), 11, 92
Kupyna, 116

L

lattice-based cryptography, 264–265
lattice problems, 179
learning with errors (LWE), 264, 267
least significant bit (LSB), 165, 193
length-extension attacks, 125, 131
Let's Encrypt, 249
Leurent, Gaëtan, 143
linear code, 263
linear combination, 28
linear feedback shift registers (LFSRs), 83
  in A5/1, 88–89
  filtered, 85
  in Grain-128a, 87–88
  polynomials, 83
  security, 84
linear transformation, 265
Linux, 32, 66, 239
Lipton, Richard J., 199
logarithm, 23, 42
long-term key, 211
lower bound, 41
low-exponent attacks, 195
LSB (least significant bit), 165, 193
Lucifer, 58
LWE (learning with errors), 264, 267

M

MACs (message authentication codes), 127
  authentication tag, 128
  CBC-MAC, 134–135
  chosen-message attacks, 129
  CMAC, 134
  dedicated designs, 136
  encrypt-and-MAC, 146–147
  encrypt-then-MAC, 147–148, 152
  forgery attacks, 128
  HMAC, 132–133
  MAC-then-encrypt, 147
  vs. PRFs, 130
  replay attacks, 129
  timing attacks, 140–142
  Wegman–Carter, 137–138
MacBook, 194
MAC-then-encrypt, 147
MacWilliams, F.J., 136
malleability, 186
man-in-the-middle attacks, 206, 209–210, 236
mask generating function, 188
matrix multiplication, 256
McEliece cryptosystem, 263
MD5, 116, 126
M–D construction. *See* Merkle–Damgård (M–D) construction
measurement (quantum physics), 252, 255
MediaWiki, 36
meet-in-the-middle (MitM) attacks, 72–74
memory, 44
memory footprint, 55
Menezes–Qu–Vanstone (MQV), 213–214, 226
Merkle, Ralph, 111, 126, 202
Merkle–Damgård (M–D) construction, 111
  length-extension attacks, 125, 131
  multicollisions, 113
  padding, 112–113
  security, 113
Merkle's puzzles, 202
Mersenne Twister (MT) algorithm, 28, 36
message authentication codes. *See* MACs (message authentication codes)

Micali, Silvio, 19
Microsoft, 65
Microsoft Windows CryptoAPI, 194
misuse resistance, 150
MitM (meet-in-the-middle) attacks, 72–74
mode of operation, 4, 5, 65
Moore, Jonathan, 233
most significant bit (MSB), 28, 135, 138, 215
MQ (multivariate quadratics), 265
MQV (Menezes–Qu–Vanstone), 213–214, 226
MT (Mersenne Twister) algorithm, 28, 36
`mt_rand`, 28
multicollisions, 113
multivariate cryptography, 265–266
multivariate problems, 179
multivariate quadratics (MQ), 265

N

Naehrig, Michael, 233
National Institute of Standards and Technology (NIST), 29, 53, 59, 120–121
National Security Agency (NSA), 59, 116, 213, 251
Netscape, 35, 237
network-based intrusion detection systems (NIDS), 105
Neves, Samuel, 123, 158
NFSR (nonlinear feedback shift register), 86
Nguyen, Phong Q., 143
Nielsen, Michael, 269
NIST (National Institute of Standards and Technology), 29, 53, 59, 120–121
NM (non-malleability), 13
nonces, 71–72, 78–79
  predictability, 149–150
  reuse, 101
  in TLS records, 241
  WEP insecurity and, 93–94
nondeterministic polynomial time class. *See* **NP** (nondeterministic polynomial time) class
nonlinear equation, 29
nonlinear feedback shift register (NFSR), 86
non-malleability (NM), 13
nonrepudiation, 188
non-uniform distribution, 23
NP (nondeterministic polynomial time) class, 168–169
  NP-complete problem, 169–170
  NP-hard problem, 170
NSA (National Security Agency), 59, 116, 213, 251
NSS library, 199
number field sieve, 204

O

OAEP. *See* Optimal Asymmetric Encryption Padding (OAEP)
OCB (offset codebook)
  efficiency, 156
  internals, 155–156
  security, 156
one-time pad, 7
  encrypting with, 7–8
  security, 8–9, 13, 40
one-way function, 107
opad, 132
OpenSSH, 136, 217, 231
OpenSSL toolkit
  generating DH parameters, 203
  generating keys, 30, 49, 177–178
  GHASH bug, 153
  Heartbleed, 248–249
  unsafe DH group parameters, 215–216
Optimal Asymmetric Encryption Padding (OAEP), 52, 186
  encoded message, 187
  mask generating function, 188

P

P (polynomial time) class, 166–168, 168–169
padding, 19, 69–70, 112–113
  OAEP, 52, 186–188
  zero padding, 241
padding oracle attacks, 19, 74–75
parallelism, 43
parallelizability, 151, 154, 156
parent process ID (PPID), 35
password, 49, 129
Paterson, Kenny, 103

Peikert, Chris, 268
perfect secrecy, 7
period, 259
permutation, 4–5, 111
  permutation-based AEAD, 157–158
  pseudorandom, 54
  security, 5, 7
  in sponge functions, 115–116
  trapdoor, 181–182, 183
PID (process ID), 35
pigeonhole principle, 109
PKCS (Public-Key Cryptography Standards), 186
plaintext, 2
PLD (programmable logic device), 79
Poly1305, 136–138, 139
Poly1305-AES, 138
polynomials, 83
  multiplication, 153
  primitive, 83–84
polynomial time (**P**) class, 166–168, 168–169
post-quantum cryptography, 252, 263
  code-based, 263–264
  hash-based, 266–267
  lattice-based, 264–265
  multivariate, 265–266
Post-Quantum Crypto Project, 269
post-quantum security, 261
power-analysis attacks, 193
PPID (parent process ID), 35
PQCrypto, 269
precomputation, 44, 208
prediction resistance, 26
preimage resistance, 107–109
Preneel, Bart, 126
pre-shared key (PSK), 243, 245
PRFs. *See* pseudorandom functions (PRFs)
prime numbers, 172
prime number theorem, 172
private keys, 15, 181
PRNGs. *See* pseudorandom number generators (PRNGs)
Probabilistic Signature Scheme (PSS), 189–190, 191
probability, 9, 22
probability distribution, 22–23
process ID (PID), 35
programmable logic device (PLD), 79
proof-of-storage protocols, 125–126
proof-of-work, 106
provable security, 46–48
pseudorandom functions (PRFs), 127
  vs. MACs, 130
  security, 129
pseudorandom number generators (PRNGs), 24–26
  cryptographic, 27–28
  entropy and, 35–36
  Fortuna, 26–27
  generating on Unix, 30–32
  generating on Windows, 33–34
  hardware-based, 34–35
  non-cryptographic, 27–28, 36–37
  security, 26
pseudorandom permutation (PRP), 54, 58, 138
PSPACE, 168
PSK (pre-shared key), 243, 245
PSS (Probabilistic Signature Scheme), 189–190, 191
public-key cryptography, 15
Public-Key Cryptography Standards (PKCS), 186
public-key distribution scheme, 201
public keys, 181
P vs. **NP**, 170–171
PyCrypto, 62
Pythagorean theorem, 253
Python language, 62, 66, 71, 92, 198

Q

Qualys, 249
quantum bit (qubit), 252
quantum byte, 255
quantum circuits, 255
quantum computers, 174, 251
quantum gates, 255, 256
quantum mechanics, 252
quantum random number generators (QRNGs), 25
quantum speed-up, 257
  exponential, 258
  quadratic, 258
quarter-round function, 96
qubit (quantum bit), 252

R

`rand`, 28
randomness, 21
random number generators (RNGs), 24–25

random oracle, 107
Ray, Marsh, 65
RC4, 79, 92–93
  broken implementation, 101–102
  in TLS, 94–95
  in WEP, 93–94
RDRAND instruction, 34–35
RDSEED instruction, 34
reduction, 46
replay attacks, 129, 206
Rho method, 110–111
Rijndael, 59
ring-LWE, 267
Rivest, Ron, 92, 103
Rivest–Shamir–Adleman. *See* RSA (Rivest–Shamir–Adleman)
Rogaway, Phillip, 155, 156, 157
RNGs (random number generators), 24–25
root of unity, 198
rounds, 48
round trips, 208
round-trip times (RTT), 245
RSA (Rivest–Shamir–Adleman), 181–182
  Bellcore attack, 196–197
  CRT, 195–196
  vs. ECDSA, 227–228
  encryption, 185
  and factoring problem, 46–47, 177
  FDH, 190–191
  groups, 182–183
  implementations, 191–192
  key generation, 184–185
  modulus, 182
  OEAP, 186–188
  private exponents, 197–199
  private keys, 50, 183, 184
  problem, 204
  PSS, 189–190, 191
  public exponents, 183
  public keys, 183
  secret exponents, 183
  security, 185
  shared moduli, 197
  signatures, 188–189
  small exponents, 194–195
  speed, 194–196
  square-and-multiply, 192–193
  textbook encryption, 185–186
  textbook signature, 188
  trapdoor permutation, 183
RSAES-OAEP, 186
RSA Security, 92
RTT (round-trip times), 245

S

Saarinen, Markku-Juhani O., 121, 166
safe prime, 203
SageMath, 176, 184
Salsa20, 95
  attacking, 99–100
  column-round function, 97
  double-round function, 97
  internal state, 96
  and nonlinear relations, 98–99
  quarter-round function, 96
  row-round function, 97
  Salsa20/8, 99
salt, 190
sandwich MAC, 133
satellite phone (satphone), 102
S-boxes (substitution boxes), 57
scheduling problems, 170
Schneier, Bruce, 26, 38, 121
Schwenk, Jörg, 233
searchable encryption, 17
search algorithm, 164
second-preimage resistance, 108
secret-prefix MAC, 130, 133
secret-suffix MAC, 131
secure channel, 201, 236
secure cookie, 246
Secure Hash Algorithms (SHAs), 116
Secure Hash Algorithm with Keccak (SHAKE), 121
Secure Shell (SSH), 51–52, 128, 132, 147, 148, 152, 226, 240
Secure Socket Layer (SSL), 35, 235, 237
security
  bit, 42–43
  computational, 40–41
  cryptographic, 39
  goals, 10, 12–13
  heuristic, 46, 48–49
  informational, 40
  levels, choosing, 44–45
  margin, 48–49
  notions, 10, 13–15

post-quantum, 261
proof, 46
provable, 46–48
semantic, 13, 18
session key, 205
SHA-0, 116–117
SHA-1, 116, 244
attacks, 118–119
collision, 118
internals, 117–118
SHA-2, 119, 120, 125
SHA-3, 115, 121–123, 215
competition, 120–121
security, 123
Zoo, 126
SHA-224, 119–120
SHA-256, 119–120, 226
compression function, 119
security, 120
SHA-384, 120
SHA-512, 120
SHAs (Secure Hash Algorithms), 116
SHAKE (Secure Hash Algorithm with Keccak), 121
Shannon, Claude, 8
Shor, Peter, 259
Shor's algorithm, 259–260
short integer solution (SIS), 264
Shrimpton, Tom, 157
side-channel attacks, 12, 140, 264, 269
Signal, 268
signatures, 106, 182, 188–189
SIM card, 206
Simon's problem, 258
Simple Mail Transfer Protocol (SMTP), 237
SipHash, 139–140, 142
SipRound function, 139–140
SIS (short integer solution), 264
SIV (synthetic IV), 156–157
Skein, 121
slide attacks, 56–57
sliding window method, 193
Sloane, N.J., 136
SM3, 116
SMTP (Simple Mail Transfer Protocol), 237
SNOW3G, 91
Somorovsky, Juraj, 233
space complexity, 168
SPHINCS, 267
SPNs (substitution–permutation networks), 57–58, 60
sponge functions, 111, 115, 142
absorbing phase, 115
capacity, 116
squeezing phase, 116
square-and-multiply, 192–193
SSH (Secure Shell), 51–52, 128, 132, 147, 148, 152, 226, 240
SSL (Secure Socket Layer), 35, 235, 237
SSL Labs, 249
statistical test, 29
Stevens, Marc, 118
streamability, 151, 154, 156
stream ciphers, 77
counter-based, 79
encryption and decryption, 78
hardware-oriented, 79–80
keystream, 78
nonce resuse, 101
software-oriented, 91
stateful, 79
Streebog, 116
substitutions, 4–5
substitution boxes (S-boxes), 57
substitution–permutation networks (SPNs), 57–58, 60
superconducting circuits, 262
superposition, 252
symmetric encryption, 1, 15, 16
synthetic IV (SIV), 156–157

T

tags, 16. *See also* authenticated encryption (AE); MACs (message authentication codes)
TE (tweakable encryption), 17
TEA, 126
TestU01, 29
time complexity, 168
time-memory trade-off (TMTO) attacks, 18, 44, 90–91
timing attacks, 141, 193, 199, 269
TLS (Transport Layer Security), 78, 35, 128, 130, 147, 235
ClientHello, 242, 244, 245
and Diffie–Hellman, 215
downgrade protection, 244
handshake, 237, 238–240, 241–243

TLS (Transport Layer Security), *continued*
  history of, 237
  RC4 in, 92, 94–95
  record, 240
  record payload, 240
  record protocol, 237, 240–241
  security, 236, 246–247, 247–249
  ServerHello, 242, 245
  session resumption, 245
  single round-trip handshake, 245
  version 1.3 algorithms, 243–244
  version 1.3 improvements, 244–245
  zero padding, 241
TLS Working Group (TLSWG), 249
TMTO (time-memory trade-off) attacks, 18, 44, 90–91
TOFU (trust-on-first-use), 240
traffic analysis, 241
Transport Layer Security. *See* TLS (Transport Layer Security)
trapdoors, 182
trapdoor permutations, 181–182, 183
traveling salesman problem, 169
triple DES (3DES), 59, 72–74
trusted third party, 238
trust-on-first-use (TOFU), 240
Turing Award, 202
tweakable encryption (TE), 17

U

UDP (User Datagram Protocol), 237
unforgeability, 128
uniform distribution, 23
unitary matrix, 257
universal hash functions, 136–137
Unix, 30
unpredictability, 107
upper bound, 42

V

Vandewalle, Joos, 126
van Oorschot, Paul C., 126
Vigenère, Blaise de, 3
Vigenère cipher, 3–4
virtual private network (VPN), 94

W

Wagner, David, 35, 38, 56, 101
Wegman–Carter MAC, 137–138, 152
Weierstrauss form, 218
WEP (Wireless Encryption Protocol), 92, 93–94
Wiener, Michael, 52, 126, 199
Wi-Fi, 77
Wilcox-O’Hearn, Zooko, 123
Windows, 30
Winnerlein, Christian, 123
Winternitz one-time signature (WOTS), 266–267
Wireless Encryption Protocol (WEP), 92, 93–94
WPA2, 162
Wustrow, Eric, 36, 233

X

Xbox, 126
XOR swap, 101–102

Y

Yao, Andrew C., 216
Yarrow, 26

Z

Zhao, Yunlei, 216
ZUC, 91