

# INDEX

## Numbers

- 0-RTT data, 267
- 3DES (triple DES), 67, 82–83.  
*See also* DES

## A

- A5/1, 21, 98–101
- Aaronson, Scott, 185, 193, 281, 293
- active attacker, 318
- adaptive corruption, 318
- Advanced Encryption Standard (AES),  
61, 67
  - AddRoundKey, 68–70
  - block size, 62
  - vs. DES, 67, 90
  - and GCM, 164–167, 171, 173
  - implementations, 71–74
  - internals, 67–70
  - KeyExpansion, 68–69
  - MixColumns, 68–69
  - with Poly1305, 148
  - and provable security, 50
  - security of, 73
  - ShiftRows, 68–69
  - SubBytes, 68–69
  - and TLS 1.3, 265–266
- Advanced Vector Extensions (AVX), 63
- AEAD (authenticated encryption with  
associated data), 18, 160,  
169–170
- AES. *See* Advanced Encryption  
Standard
- AES-CBC, 78
- AESENC instruction, 72
- AESENCLAST instruction, 73
- AES-GCM
  - efficiency, 166
  - internals, 164–165
  - security, 166
  - and small tags, 173
  - and weak hash keys, 171–173
- AES native instructions (AES-NI), 72
- AEZ, 174
- aggregate signature protocols, 311–314
- AKA (authenticated key  
agreement), 220–221
- algebraic attacks, 96
- Alvisi, Lorenzo, 136
- amplitude, 274–279
- Apple, 243, 246
- application-specific integrated circuit  
(ASIC), 89
- arithmetization, 328
- associated data, 160
- asymmetric encryption, 3, 18. *See also*  
RSA
- attack costs, 47–49
- attack models, 12
  - black-box, 13–14
  - gray-box, 14
  - for key agreement protocols, 221
- authenticated ciphers, 160
  - with associated data, 160–161
  - functional criteria, 163
  - nonces, 161–162
  - online, 163
  - performance, 162–163
  - permutation-based, 169–171
  - security, 162
  - streamability, 163
- authenticated decryption, 160
- authenticated Diffie–Hellman, 224–226
- authenticated encryption (AE), 18, 157
  - AES-GCM, 164–167, 171–173
  - authenticated ciphers, 160–163
  - OCB, 167–169
  - permutation-based AEAD, 169–171
  - SIV, 169
  - using MACs, 158–160

- authenticated encryption with
  - associated data (AEAD), 18, 160, 169–170
- authenticated key agreement (AKA), 220–221
- authentication tag, 18. *See also*
  - authenticated encryption; MACs
- AVX (Advanced Vector Extensions), 63

## B

- backtracking resistance, 30
- backward secrecy, 30
- BcryptGenRandom() function, 37–38
- Bellare, Mihir, 155
- Bellare, Giovan Battista, 5
- Bellcore attack, 211
- Bernstein, Daniel J., 57, 106, 110, 148, 151, 244, 248, 283
- big-number libraries, 206
- bilinearity, 312
- binary exponentiation, 207
- birthday attacks, 120
- birthday paradox, 120
- Bitcoin, 116, 297, 299–302, 306, 307
- bit security, 46–48
- BLAKE, 131
- BLAKE2, 115, 133–135, 143
  - BLAKE2b, 134
  - BLAKE2s, 134
  - compression function, 134–135
  - design rationale, 134
- blinding attacks, 203
- block ciphers, 61. *See also* Advanced Encryption Standard
  - block size, 62–63
  - CBC mode, 76–78
  - codebook attacks, 63
  - CTR mode, 80–82
  - decryption algorithm, 62
  - ECB mode, 74–76
  - encryption algorithm, 62
  - Feistel schemes, 66–67
  - key schedule, 64
  - meet-in-the-middle attacks, 82–83
  - modes of operation, 74
  - padding oracle attacks, 83–85
  - round keys, 64–65

- rounds, 64
- security goals, 62
- slide attacks, 64–65
- substitution–permutation networks, 65–66

- BLS curve, 312
- BLS signature, 312–313
- Bluetooth, 88
- Boneh, Dan, 214
- Bos, Joppe W., 251
- broadcast attack model, 105
- Brumley, David, 214
- brute-force attacks, 45, 100–101

## C

- CA (certificate authority), 258–262, 269–270
- cache-timing attacks, 72
- Caesar cipher, 4–5
- CAESAR competition, 174
- Canetti, Ran, 155
- carry-less multiplication (CLMUL), 165
- CBC. *See* cipher block chaining
- CBC-MAC, 146–147
- CCA (chosen-ciphertext attackers), 13–14
- CCM (counter with CBC-MAC), 174, 265
- CDH (computational Diffie–Hellman), 218–219
- certificate authority (CA), 258–262, 269–270
- certificate chain, 259, 269
- ChaCha20, 106, 131, 151, 265
- chaining values, 122
- Chinese remainder theorem (CRT), 210–211
- chosen-ciphertext attackers (CCA), 13–14
- chosen-message attacks, 140
- chosen-plaintext attackers (CPA), 13
- Chrome browser, 129, 271
- Chuang, Isaac, 293
- cipher-based MAC (CMAC), 146–147
- cipher block chaining (CBC), 76–78
  - ciphertext stealing, 79
  - padding, 78–79
  - padding oracle attacks, 83–85

- ciphers, 3
- ciphertext, 4
- ciphertext-only attackers (COAs), 13
- ciphertext stealing, 79
- circuit, 328
- C language, 91
- Clay Mathematics Institute, 50, 185
- client certificate, 268
- clique problem, 184
- CLMUL (carry-less multiplication), 165
- closest vector problem (CVP), 287
- CMAC (cipher-based MAC), 146–147
- CMAC-AES, 169
- code-based cryptography, 285–286
- codebook attacks, 63, 101
- Codonomicon, 270
- coding problems, 194
- Cohen, Henri, 251
- Cold War, 61
- collision resistance, 119–120, 123, 305–306
- completeness, 324
- complexity. *See* computational complexity
- complexity class, 182
- complex numbers, 275
- compression functions, 122
  - in BLAKE2, 134–135
  - Davies–Meyer construction, 124–125
  - in Merkle–Damgård construction, 122
  - in SHA-1, 127
- computational complexity, 178
  - bounds, 182
  - classes, 182
  - comparison, 180
  - constant factors, 179
  - constant time, 179
  - exponential, 179–181
  - exponential factorial, 181
  - linear, 179
  - linearithmic, 179
  - polynomial, 180–183
  - quadratic, 180
  - superpolynomial, 180
- computational complexity theory, 177
- computational Diffie–Hellman (CDH), 218–219
- computational hardness, 178
- computational security, 44–46
- confidentiality, 3, 21, 116, 162
- confusion, 65, 303
- constant-time implementations, 154
- Coppersmith, Don, 213
- counter mode (CTR), 80–82, 102, 164
- counter with CBC-MAC (CCM), 174, 265
- CPA (chosen-plaintext attackers), 13
- CRCs (cyclic redundancy checks), 116
- CRT (Chinese remainder theorem), 210–211
- CryptAcquireContext() function, 34
- CryptGenRandom() function, 37
- Crypto++, 214
- Cryptocat, 41
- cryptographic security, 43. *See also* security
- CTR (counter mode), 80–82, 102, 164
- cube attacks, 96
- Curve448, 265
- Curve25519, 248, 265
- Curve41417, 248
- CVP (closest vector problem), 287
- cyclic redundancy checks (CRCs), 116

## D

- Dahlin, Mike, 136
- Damgård, Ivan, 122, 237
- Data Encryption Standard. *See* DES
- Datagram Transport Layer Security (DTLS), 257
- Davies–Meyer construction, 124–125, 127, 134
- decisional Diffie–Hellman (DDH)
  - assumption, 219
  - problem, 218–219
- dedicated hardware, 90
- DeMillo, Richard A., 214
- DES (Data Encryption Standard), 61, 90
  - vs. AES, 67, 90
  - block size, 62
  - double DES, 83
  - Feistel schemes in, 66–67
  - 3DES, 67, 82–83
- deterministic random bit generator (DRBG), 16, 30, 88

- /dev/random*, 36–37
- /dev/urandom*, 34–37
- Diehard, 33
- differential cryptanalysis, 109
- Diffie, Whitfield, 195, 215
- Diffie–Hellman problem, 194
- Diffie–Hellman protocol, 241
  - anonymous, 223–224
  - authenticated, 224–227
  - CDH problem, 218
  - DDH problem, 218–219
  - function, 216–217
  - generating parameters, 217
  - and key agreement, 219–222, 241
  - MQV protocol, 227–228
  - and shared secrets, 216, 228–229
  - in TLS, 215, 229, 264–265
  - twin problem, 219
  - unsafe group parameters, 229–230
- diffusion, 65–66, 304
- digest, 116
- DigiNotar, 269
- digital signatures, 116–117, 196, 202–205
- discrete logarithm problem (DLP), 189–191
  - and CDH problem, 218
  - ECDLP, 240–241
  - and Shor’s algorithm, 281–282
- dishonest majority, 318
- distribution, 26–27
- domain separation, 305–306
- drand48, 32
- DRBG (deterministic random bit generator), 16, 30, 88
- DTLS (Datagram Transport Layer Security), 257
- Durumeric, Zakir, 40

**E**

- ECB (electronic codebook), 74
- ECC (elliptic curve cryptography), 231
- ECDH (elliptic curve Diffie–Hellman), 241, 249, 292
- ECDLP (elliptic curve discrete logarithm problem), 240–241
- ECDSA. *See* elliptic curve digital signature algorithm
- ECIES (elliptic curve integrated encryption scheme), 246
- Ed25519, 244, 250
- Ed448-Goldilocks, 248
- EdDSA, 244
- Einstein–Podolsky–Rosen (EPR) paradox, 274
- elliptic curve cryptography (ECC), 231
- elliptic curve Diffie–Hellman (ECDH), 241, 249, 292
- elliptic curve digital signature algorithm (ECDSA), 241, 321
  - and bad randomness, 249
  - vs. RSA signatures, 243–244
  - signature generation, 242
  - signature verification, 242–243
- elliptic curve discrete logarithm problem (ECDLP), 240–241
- elliptic curve integrated encryption scheme (ECIES), 246
- elliptic curves, 231
  - addition law, 235
  - Curve25519, 248, 265
  - Curve41417, 248
  - Curve448, 265
  - Edwards curves, 233, 244
  - groups, 239–240
  - with integers, 233–234
  - NIST curves, 247–248
  - order, 240
  - pairing, 312
  - point at infinity, 236, 239–240, 314
  - point doubling, 237–238
  - point multiplying, 238–239
  - prime curves, 247
  - Weierstrass form, 232
- embarrassingly parallel, 48, 100
- Encapsulating Security Payload (ESP), 263
- encrypt-and-MAC, 158–159
- encryption, 3
  - asymmetric, 18
  - at-rest, 17
  - in-transit, 17
  - randomized, 15–16
  - security, 12
- encrypt-then-MAC, 158, 159–160, 164
- entanglement, 274, 277

entropy, 27–31, 36–37  
entropy pool, 29–31  
EPR (Einstein–Podolsky–Rosen)  
    paradox, 274  
error-correcting codes, 285  
ESP (Encapsulating Security  
    Payload), 263  
eSTREAM competition, 97, 106, 113  
Ethereum, 306  
eth roots, 199  
Euler’s theorem, 212  
Euler’s totient function, 196  
exponentiation, 206–208, 210  
extended Euclidean algorithm, 198

## F

factorials, 9  
factoring methods, 187  
factoring problem, 50–51, 186  
    and **NP**-completeness, 188–189  
    solving with Shor’s algorithm,  
        281–282  
factorization, 187–188, 191–192  
fast correlation attacks, 96  
fault injection, 211  
FDH (Full Domain Hash), 205  
feedback shift registers (FSRs), 90–92  
    cycle, 92  
    feedback function, 90  
    linear, 93–95  
    nonlinear, 96  
    period, 92  
Feistel schemes, 66–67  
Ferguson, Niels, 30, 173  
FHE (fully homomorphic  
    encryption), 20  
Fiat–Shamir transform, 327, 330  
field-programmable gate array  
    (FPGA), 89  
filtered LFSR, 95–96  
first-preimage resistance, 118  
fixed points, 125  
Flame, 137  
Flexible Round-Optimized Schnorr  
    Threshold (FROST), 321  
forgery attacks, 140  
format-preserving encryption (FPE),  
    19–20

Fortuna, 30–31  
forward secrecy, 221–222, 225, 228  
    in authenticated DH, 225  
    in TLS 1.3, 268–269  
Fouque, Pierre-Alain, 155  
FOX, 66  
FPGA (field-programmable gate  
    array), 89  
frequency analysis, 6  
Frey, Gerhard, 251  
FROST (Flexible Round-Optimized  
    Schnorr Threshold), 321  
FSRs. *See* feedback shift registers  
full diffusion, 110  
Full Domain Hash (FDH), 205  
fully homomorphic encryption  
    (FHE), 20

## G

GCD (greatest common divisor), 40,  
    198, 211, 282  
GCHQ (Government Communications  
    Headquarters), 216  
GCM (Galois Counter Mode), 158, 164,  
    173. *See also* AES-GCM  
gcm\_ghash\_c1mul function, 165  
general number field sieve (GNFS),  
    187, 218  
getrandom() system call, 36  
GHASH, 165–166, 171–172  
Gilbert, Edgar, 148  
Git, 115  
GitHub, 55  
Gmail, 268, 270  
GMR-1, 113  
GMR-2, 113  
GNFS (general number field sieve),  
    187, 218  
GNU Multiple Precision (GMP), 206  
Go, 152, 206, 208  
Goldberg, Ian, 39, 321  
Goldwasser, Shafi, 22  
Google, 129, 258–261, 269, 270  
    Chrome browser, 129, 271  
GOST, 61, 67  
Govaerts, René, 137  
Government Communications  
    Headquarters (GCHQ), 216

Grain-128a, 97–98  
graphics processing unit (GPU),  
101, 178  
greatest common divisor (GCD), 40,  
198, 211, 282  
Grøstl, 131  
groups  
axioms, 190  
commutativity, 190  
cyclic, 190  
finite, 190  
generator, 190  
in RSA, 196–197  
Grover’s algorithm, 282–283  
GSM mobile communication, 88, 140  
guess-and-determine attacks, 100–101

## H

Hadamard gate, 278–279  
Halderman, Alex, 40, 251  
hardness assumption, 189  
hard problems, 177. *See also*  
computational complexity  
closest vector problem, 287  
discrete logarithm problem,  
189–191  
factoring problem, 50–51, 186  
learning with errors, 194, 286  
multivariate quadratic  
equations, 287  
**NP**-complete problem, 183–186  
**P** vs. **NP** problem, 185–186  
and provable security, 50–51  
short integer solution, 194, 286  
hardware, 72, 113  
hash-based cryptography, 288–289  
hash-based MACs, 144–145  
hash functions, 115. *See also* Merkle–  
Damgård construction  
collisions in, 119–121  
compression functions, 122  
Davies–Meyers construction,  
124–125  
in digital signatures, 116  
iterative, 122  
keyed, 139  
multicollisions, 123–124  
noncryptographic, 116

**P** vs. **NP** problem, 185–186  
preimage resistance, 117–119  
in proof-of-storage protocols,  
136–137  
security notions, 116  
sponge functions, 122, 125–126  
3-collisions, 123  
universal, 148–149  
unpredictability, 117  
hash values, 116, 117–121  
Heartbleed, 256, 270  
Hellman, Martin, 195, 215  
Heninger, Nadia, 40, 251  
heuristic security, 50, 52–53  
HMAC-based KDF (HKDF), 229, 265  
HMACs (hash-based MACs), 144–146  
honest majority, 318  
HTTPS, 258  
insecure, 166, 193  
keys for, 53, 56  
over TLS, 104, 215, 256

## I

iCloud, 270  
identity gate, 278  
IES (integrated encryption  
scheme), 246  
IETF (Internet Engineering Task  
Force), 134, 164, 250, 314  
IKE (Internet Key Exchange), 146  
imaginary number, 275  
IND-CPA, 15–17  
indifferentiability, 137  
indistinguishability (IND), 15  
initial value (IV), 76, 81, 89, 122, 147  
integrated encryption scheme  
(IES), 246  
integrity, of data, 19, 116, 140  
Intel, 38, 73, 165  
Internet Engineering Task Force  
(IETF), 134, 164, 250, 314  
Internet Key Exchange (IKE), 146  
internet of things (IoT), 255  
intractable problems. *See* hard  
problems  
invalid curve attack, 249–250  
invalid key, 314–315  
invasive attacks, 14

ion traps, 284  
ipad, 144  
IPSec (Internet Protocol Security), 140,  
144, 146, 160, 164, 263  
iterative hashing, 122  
IV (initial value), 76, 81, 89, 122, 147

## J

Jager, Tibor, 250  
Java, 22, 32, 152  
JH, 131

## K

KDF. *See* key derivation function  
Keccak, 126, 131–133, 171. *See also*  
SHA-3  
Kelsey, John, 30, 41, 50  
Kerckhoffs, Auguste, 6, 13  
Kerckhoffs's principle, 13  
key agreement protocols, 53, 216, 219  
AKA, 220–221  
attack models, 221  
breaches, 221, 225, 228  
data leaks, 221, 226, 268  
eavesdroppers, 216, 218  
forward secrecy, 221–222, 225, 228  
performance, 222  
security goals, 221  
key cancellation attack, 309–310,  
315–316  
key confirmation, 226, 228  
key control, 221, 225  
key derivation function (KDF), 53  
in DH functions, 216, 229  
in ECIES, 246  
in TLS 1.3, 265–266  
key generation, 39, 40, 198, 323  
key-generation algorithm, 53, 54  
key management, 323  
key scheduling algorithms (KSAs),  
102–104  
key wrapping, 55  
knapsack problem, 184  
knowledge extractor, 326  
known-message attack, 140  
known-plaintext attackers (KPA),  
13, 100  
Knudsen, Lars, 51

Kohno, Tadayoshi, 31  
Kotla, Ramakrishna, 136  
Kozierok, Charles, 257  
Krawczyk, Hugo, 155, 230  
Krovetz, Ted, 168  
KSAs (key scheduling algorithms),  
102–104  
Kupyna, 127

## L

Lagrange interpolation, 319  
lattice-based cryptography, 286–287  
lattice problems, 194, 287, 291  
learning with errors (LWE), 286, 291  
least significant bit (LSB), 179, 207  
length-extension attacks, 135–136,  
142–143  
Let's Encrypt, 271  
Leurent, Gaëtan, 155  
linear code, 285–286  
linear combination, 33  
linear feedback shift registers  
(LFSRs), 93  
in A5/1, 98–100  
filtered, 95–96  
in Grain-128a, 97–98  
polynomials, 93  
security, 95  
linear transformation, 33, 93, 287  
Linux, 34, 36, 74, 152  
Lipton, Richard J., 214  
logarithm, 27, 46  
long-term key, 225  
lower bound, 45  
low-exponent attacks, 209  
LSB (least significant bit), 179, 207  
Lucifer, 66  
LWE (learning with errors), 286, 291

## M

MacBook, 154, 191, 209  
MACs (message authentication  
codes), 139  
authentication tag, 140  
CBC-MAC, 146–147  
chosen-message attacks, 140  
CMAC, 146–147  
dedicated designs, 148

- MACs (*continued*)
    - encrypt-and-MAC, 158–159
    - encrypt-then-MAC, 158, 159–160, 164
    - forgery attacks, 140
    - HMAC, 144–146
    - MAC-then-encrypt, 158–160
    - vs. PRFs, 141–142
    - replay attacks, 141
    - timing attacks, 140–142
    - Wegman–Carter, 149–150
  - MAC-then-encrypt, 158–160
  - MacWilliams, F.J., 148
  - malleability, 199–200
  - man-in-the-middle attacks, 220, 223–224, 256
  - mask generating function, 202
  - matrix multiplication, 278
  - McEliece cryptosystem, 285–286
  - MD5, 122, 127, 133
  - M–D construction. *See* Merkle–Damgård construction
  - measurement (quantum physics), 274, 278
  - MediaWiki, 40
  - meet-in-the-middle (MitM) attacks, 82–83
  - memory, 48
  - memory footprint, 63
  - Menezes–Qu–Vanstone (MQV), 227–228, 241
  - Merkle, Ralph, 122, 137, 216, 297
  - Merkle–Damgård (M–D) construction, 122
    - length-extension attacks, 135–136, 142–145
    - multicollisions, 123–124
    - padding, 123
    - security, 123
  - Merkle’s puzzles, 216
  - Mersenne Twister (MT) algorithm, 32, 40, 305
  - message authentication codes. *See* MACs
  - Micali, Silvio, 22
  - Microsoft, 111, 131
  - Microsoft Windows CryptoAPI, 208
  - misuse resistance, 162
  - MitM (meet-in-the-middle) attacks, 82–83
  - mode of operation, 7–8, 61, 74
  - Moore, Jonathan, 251
  - most significant bit (MSB), 32, 147, 150, 229
  - MQ (multivariate quadratics), 287
  - MQV (Menezes–Qu–Vanstone), 227–228, 241
  - MT (Mersenne Twister) algorithm, 32, 40, 305
  - mt\_rand, 32, 40
  - multicollisions, 123–124
  - multiparty computation (MPC), 316
  - multisignature protocols, 306
  - multivariate cryptography, 287–288
  - multivariate problems, 194
  - multivariate quadratics (MQ), 287
  - MuSig, 310–311
- ## N
- Naehrig, Michael, 251, 312
  - Netscape, 39, 257
  - network-based intrusion detection systems (NIDS), 115
  - Neves, Samuel, 133, 135
  - NFSR (nonlinear feedback shift register), 96–98
  - Nguyen, Phong Q., 155
  - Nielsen, Michael, 293
  - NIST (National Institute of Standards and Technology), 33, 61, 67, 129–131, 247–248, 289–291
  - NM (nonmalleability), 15
  - nonces, 80–82, 88–89
    - predictability, 161–162
    - reuse, 111, 169
    - in TLS records, 263
    - WEP insecurity, 103–104
  - nondeterministic polynomial time class. *See* NP class
  - noninteractive zero-knowledge (NIKZ), 326–327
  - nonlinear equation, 33, 96
  - nonlinear feedback shift register (NFSR), 96–98
  - nonmalleability (NM), 15
  - nonrepudiation, 202

nonuniform distribution, 27  
**NP** (nondeterministic polynomial time) class, 182–183  
    **NP**-complete problem, 183–185  
    **NP**-hard problem, 185–186  
NSA (National Security Agency), 10, 85, 105, 127, 129, 227, 244, 247, 273  
NSS library, 214  
number field sieve, 218

## O

OAEP. *See* Optimal Asymmetric Encryption Padding  
OCB (offset codebook)  
    efficiency, 168–169  
    internals, 167–168  
    security, 168  
one-time pad, 9  
    encrypting with, 9–10  
    security, 10–11, 12, 44  
one-way function, 117  
opad, 144  
OpenSSH, 148, 159, 231, 246, 248  
OpenSSL toolkit  
    generating DH parameters, 217  
    generating keys, 53–54, 192–193  
    GHASH bug, 165  
    Heartbleed, 256, 270  
    unsafe DH group parameters, 229–230  
Optimal Asymmetric Encryption Padding (OAEP), 56, 200  
    encoded message, 201  
    mask generating function, 202

## P

**P** (polynomial time) class, 180–185  
**P** vs. **NP**, 185–186  
padding, 22, 78–79, 83–84, 123  
    OAEP, 56, 200  
    zero padding, 263  
padding oracle attacks, 22, 83–84  
pairing, 312  
parallelism, 47–48  
parallelizability, 162, 166, 168  
parent process ID (PPID), 39  
passive attacker, 318

password, 53, 55, 141  
Peikert, Chris, 291  
perfect secrecy, 9  
period, 92–94, 97–98, 281–282  
permutation, 6  
    permutation-based AEAD, 169–171  
    pseudorandom, 62, 150  
    security, 7, 8–9  
    in sponge functions, 125–126  
    trapdoor, 196, 197–199  
PID (process ID), 39  
pigeonhole principle, 119  
PKCS (Public-Key Cryptography Standards), 200–201  
plaintext, 4  
PLD (programmable logic device), 89  
Poly1305, 148–151  
Poly1305-AES, 150–151  
polynomials, 93  
    multiplication, 165–166  
    primitive, 93–94  
polynomial time (**P**) class, 180–185  
post-quantum cryptography, 274, 285  
    code-based, 285–286  
    hash-based, 288–289  
    lattice-based, 286–287  
    multivariate, 287–288  
Post-Quantum Cryptography Standardization project, 289  
post-quantum security, 283, 304  
power-analysis attacks, 208  
PPID (parent process ID), 39  
PQCrypto, 293  
precomputation, 48, 222  
prediction resistance, 30  
preimage resistance, 117–119  
Preneel, Bart, 137  
preshared key (PSK), 265, 267  
PRFs. *See* pseudorandom functions  
prime numbers, 187  
prime number theorem, 187  
private keys, 18, 195  
PRNGs. *See* pseudorandom number generators  
Probabilistic Signature Scheme (PSS), 203–205  
probability, 11, 26

- probability distribution, 26–27
- process ID (PID), 39
- programmable logic device (PLD), 89
- proof-of-storage protocols, 136–137
- proof-of-work, 300
- provable security, 50–53
- pseudorandom functions (PRFs), 139
  - vs. MACs, 141–142
  - security, 141
- pseudorandom number generators
  - (PRNGs), 28–30
  - cryptographic, 32–33
  - and entropy, 39–40
  - Fortuna, 30–31
  - generating on Unix, 34–36
  - generating on Windows, 37–38
  - hardware-based, 38
  - noncryptographic, 32, 40
  - security, 30
- pseudorandom permutation (PRP), 62, 67, 150
- PSK (preshared key), 265, 267
- PSPACE, 182
- PSS (Probabilistic Signature Scheme), 203–205
- public-key cryptography, 18, 231
- Public-Key Cryptography Standards (PKCS), 201
- public-key cryptosystem, 215
- public keys, 195
- PyCrypto, 70
- Pythagorean theorem, 275
- Python language, 70, 75, 80–81, 102, 212

## Q

- Qualys, 271
- quantum bit (qubit), 274, 276–279, 284
- quantum byte, 277
- quantum circuits, 278
- quantum computers, 188–189, 274
- quantum gates, 277–279
- quantum mechanics, 274
- quantum random number generators
  - (QRNGs), 29
- quantum speedup, 279
  - exponential, 280
  - quadratic, 280

- quarter-round function, 106–107
- qubit (quantum bit), 274, 276–279, 284

## R

- randomness, 25
- random number generators (RNGs), 28–29
- random oracle, 117
- Ray, Marsh, 74
- RC4, 89, 102
  - broken implementation, 111–113
  - in TLS, 104–105
  - in WEP, 103–104
- RDRAND instruction, 38
- RDSEED instruction, 38
- reduction, 50
- replay attacks, 142, 220, 330
- Rho method, 120–121
- Rijndael, 67
- ring-LWE, 291
- Rivest, Ron, 102
- Rivest–Shamir–Adleman. *See* RSA
- RNGs (random number generators), 28–29
- Rogaway, Phillip, 168, 169
- rogue key attack, 310
- root of unity, 212
- rounds, 53
- round trips, 222
- round-trip times (RTTs), 267
- RSA (Rivest–Shamir–Adleman), 195
  - Bellcore attack, 211–212
  - CRT, 210–211
  - vs. ECDSA, 243–244
  - encryption, 199
  - and factoring problem, 50–51, 186
  - FDH, 205
  - groups, 196–197
  - implementations, 205–206
  - key generation, 208–209
  - modulus, 212
  - OAEP, 200–202
  - private exponents, 212–213
  - private keys, 54, 197, 198
  - problem, 218
  - PSS, 203–204, 205
  - public exponents, 197
  - public keys, 197

- secret exponents, 197
- security, 198
- shared moduli, 212–213
- signatures, 202–205
- small exponents, 208–209
- speed, 208–210
- square-and-multiply, 207–208
- textbook encryption, 199–200
- textbook signature, 203
- trapdoor permutation, 196, 197, 199
- RSAES-OAEP, 200
- RSA Security, 102
- RTT (round-trip times), 267

**S**

- Saarinen, Markku-Juhani O., 132, 173
- safe prime, 217
- SageMath, 191, 198, 239
- Salsa20, 106
  - attacking, 110–111
  - column-round function, 108
  - double-round function, 107
  - internal state, 107
  - and nonlinear relations, 110
  - quarter-round function, 106–107
  - row-round function, 107
  - Salsa20/8, 110–111
- salt, 204
- sandwich MAC, 144
- satellite phone (satphone), 113
- S-boxes (substitution boxes), 65
- scheduling problems, 184
- Schneier, Bruce, 30, 31, 41, 131
- Schnorr, Claus-Peter, 244, 307
- Schnorr signature protocol, 307–309
- Schnorr’s proof-of-knowledge protocol, 325–326
- Schwenk, Jörg, 250
- searchable encryption, 20
- search algorithm, 178
- second-preimage resistance, 118
- secret-prefix MAC, 143, 145
- secret sharing, 319
  - additive, 319
  - threshold, 319
- secret-suffix MAC, 143
- secure channel, 216, 256

- secure cookie, 268
- Secure Hash Algorithm with Keccak (SHAKE), 132
- Secure Shell (SSH), 55, 140, 144, 159, 160, 241, 262
- Secure Socket Layer (SSL), 39, 255, 257
- security
  - bit, 46–47
  - computational, 44–45
  - cryptographic, 43
  - goals, 12, 15
  - heuristic, 50, 52–53
  - levels, choosing, 49–50
  - margin, 53
  - notions, 12, 15–17
  - post-quantum, 283
  - proof, 46
  - provable, 50–52
  - semantic, 15, 16
- session key, 53, 219
- SHA-0, 127–128
- SHA-1, 127–129, 266
- SHA-2, 129–133
- SHA-224, 129–130
- SHA-256, 117, 123, 129–130, 242, 297, 300
  - compression function, 130, 146
  - security, 130–131, 297
- SHA-3, 126, 132–133, 229
  - competition, 131–132
  - security, 133–134
  - Zoo, 137
- SHA-384, 130
- SHA-512, 130
- SHAKE (Secure Hash Algorithm with Keccak), 132
- Shamir’s secret sharing, 319
- Shannon, Claude, 10
- SHAs (Secure Hash Algorithms), 126
- Shor, Peter, 281
- Shor’s algorithm, 281–282
- short integer solution (SIS), 286
- Shrimpton, Tom, 169
- side-channel attacks, 14, 65, 153, 292
- Signal, 292
- signatures, 116, 196, 202–205
- SIM card, 220
- Simon’s problem, 280–281

- Simple Mail Transfer Protocol (SMTP), 229, 257
- simulator, 326
- SipHash, 151–152, 155
- SipRound function, 151–152
- SIS (short integer solution), 286
- SIV (synthetic IV), 169
- Skein, 131
- slide attacks, 64–65
- sliding window method, 208
- Sloane, N.J., 149
- SM3, 127
- SMTP (Simple Mail Transfer Protocol), 229, 257
- SNOW3G, 102
- Somorovsky, Juraj, 250
- soundness, 324
- space complexity, 182
- SPHINCS+, 289–290
- SPNs (substitution–permutation networks), 65–66, 68
- sponge functions, 122, 125–126, 155
  - absorbing phase, 126
  - capacity, 126
  - squeezing phase, 126
- square-and-multiply, 207–208
- SSH (Secure Shell), 55, 140, 144, 159, 160, 241, 262
- SSL (Secure Socket Layer), 39, 255, 257
- SSL Labs, 271
- static corruption, 318
- statistical test, 33–34
- streamability, 163, 167–169
- stream ciphers, 87
  - counter-based, 89
  - encryption and decryption, 88
  - hardware-oriented, 89–90
  - keystream, 88
  - nonce reuse, 111
  - software-oriented, 101
  - stateful, 89
- Streebog, 127
- substitution boxes (S-boxes), 65
- substitution–permutation networks (SPNs), 65–68
- substitutions, 7
- superconducting circuits, 284
- superposition, 274

- symmetric encryption, 3, 18
- synthetic IV (SIV), 169

## T

- tags, 18. *See also* authenticated encryption; MACs
- TEA, 137
- threshold signature protocol, 316
- time complexity, 180–182
- time-memory trade-off (TMTO)
  - attacks, 21, 48, 101
- timing attacks, 153–154, 208, 292
- TLS (Transport Layer Security), 39, 88, 140, 142, 159, 255
  - ClientHello, 257, 264–267
  - and Diffie–Hellman, 229
  - downgrade protection, 266–267
  - handshake, 257, 258–268
  - history of, 257
  - RC4 in, 102, 104–106
  - record, 262
  - record payload, 262
  - record protocol, 257, 262
  - security, 256, 268–271
  - ServerHello, 257, 264–267
  - session resumption, 267–268
  - single round-trip handshake, 267
  - version 1.3, 265–267
  - zero padding, 263
- TLS Working Group (TLSWG), 271
- TMTO (time-memory trade-off)
  - attacks, 21, 48, 101
- TOFU (trust-on-first-use), 262
- traffic analysis, 263
- Transport Layer Security. *See* TLS
- trapdoor permutations, 196, 197, 199
- trapdoors, 196, 197–199
- traveling salesman problem, 184
- triple DES (3DES), 67, 82–83
- trusted third party, 258
- trust-on-first-use (TOFU), 262
- Turing Award, 216
- tweakable encryption (TE), 20–21

## U

- UDP (User Datagram Protocol), 257
- unforgeability, 140
- uniform distribution, 27

unitary matrix, 279  
universal hash functions, 148–149  
Unix, 34  
unpredictability, 117  
upper bound, 46

## V

Vandewalle, Joos, 137  
van Oorschot, Paul C., 137  
Vigenère, Blaise de, 5  
Vigenère cipher, 5–6  
virtual private network (VPN), 104

## W

Wagner, David, 39, 41, 64, 112  
Wegman–Carter MAC, 149–150, 155  
Weierstrass form, 232  
WEP (Wireless Encryption Protocol),  
102, 103–104  
Wiener, Michael, 57, 137, 213  
Wi-Fi, 87, 103–104  
Wilcox-O’Hearn, Zooko, 133, 135  
Windows, 37–38  
Winnerlein, Christian, 133

Winternitz one-time signature  
(WOTS), 288–289  
Wireless Encryption Protocol (WEP),  
102, 103–104  
WPA2, 174  
Wustrow, Eric, 40, 251

## X

Xbox, 137  
XOR swap, 112–113

## Y

Yao, Andrew C., 230  
Yarrow, 30  
Yung, Moti, 305

## Z

zero-knowledge proof (ZKP),  
323–324  
noninteractive, 326  
0-RTT data, 267  
Zhao, Yunlei, 230  
zkSNARK, 327–329  
ZUC, 102