

Index

- 3DES, *see* triple DES
- 3GPP, 381, 389
- 3rd Generation Partnership Project,
 see 3GPP
- A3/A5/A8, 53–55, 80, 384–386
- access control, xvi, 4, 6–7, 229
 and operating system, 494
- access control list, *see* ACL
- access control matrix, 271–272
- ACK scan, 290, 306
- ACL, 272, 302
- Address Resolution Protocol, *see* ARP
- Address Space Layout
 Randomization, *see* ASLR
- Adleman, Leonard, 95, 422
- Adobe, 464
 eBooks, 471
- Advanced Encryption Standard, *see*
 AES
- AES, 67–69, 82, 117, 466
 - AddRoundKey, 69
 - block size, 67
 - ByteSub, 68
 - confusion and diffusion, 83
 - key length, 67
 - key schedule, 69
 - MixColumn, 69
 - number of rounds, 67
 - ShiftRow, 69
 - subkey, 69
- AFS Software, Inc., 146
- AH, 359, 371–372
 and Microsoft, 372
- Ali Baba's Cave, 335
- Alice, 1
- Alice's Restaurant, 2
- Almes, Guy, 511
- Amis, Kingsley, 531
- Anderson, Ross, 476, 497, 503–505
- anomaly detection, 427, 429
- anonymity, 342
- anti-debugging, 456
- anti-disassembly, 455
- Apple II, 95, 210
- application layer, 513–515
- Aristophanes, 242
- Aristotle, 51
- ARP, 522
 - cache poisoning, 522
- ASLR, 417
- asymmetric cryptography, 89
- ATM, 13
 - card, 231
 - machine, 315
- attack tree, 478
- authentication, 3, 229–231, 394
 - and TCP, 332–334
 - two-factor, 252
- Authentication Header, *see* AH
- authorization, 3, 6, 230
- availability, 3
- avalanche effect, 133
- Aycock, John, xviii, 421
- backdoor, 421
- Ballantyne, Sheila, 265
- Bell-LaPadula, *see* BLP
- Biba's model, 278–279, 303, 304
 - low water mark policy, 278

- write access rule, 278
- Biham, Eli, 186
- biometric, 242–251
 - attack, 250
 - authentication, 242
 - enrollment phase, 243
 - equal error rate, 244
 - error rate, 250
 - errors, 244
 - fingerprint, 244
 - fraud rate, 244
 - hand geometry, 246
 - ideal, 242
 - identification, 242
 - insult rate, 244
 - iris scan, 246–249
 - recognition phase, 243
- birthday paradox, *see* birthday problem
- birthday problem, 128–129
 - and hash functions, 129
- block cipher, 40, 57–76
 - bit errors, 75
 - cut-and-paste attack, 75, 84, 86
 - design, 202–203
 - modes of operation, 72–76
 - round function, 57
- Blowfish, 70
 - S-box, 70
- BLP, 276–279, 303, 304
 - simple security condition, 276
 - star property, 276
 - strong tranquility, 277
 - system Z, 277
 - weak tranquility, 277
- BMA, *see* British Medical Association
- Bob, 1
- Bob's Cave, 335–336, 348
- Bobcat hash, 155
- BOBE, 459
 - resistance, 467, 486
- Boeing 777, 405
- Bonaparte, Napoleon, 203
- botmaster, 433
- botnet, 433, 443
- Brain, 422
- break once break everywhere resistant,
 - see* BOBE
- British Medical Association, 280
- buffer overflow, 9, 407–414, 440
 - example, 411–415
 - prevention, 415–417
- Burleson, Donald Gene, 436
- C-list, *see* capabilities
- C#, 416
- CA, *see* certificate authority
- Caesar's cipher, 22, 43
- Caesar, Julius, 22
- canary, 416, 417
- capabilities, 272, 302
 - and digital signatures, 303
 - delegate, 302
- CAPTCHA, 13, 285–287, 305
 - Gimpy, 304
- Carroll, Lewis, 1, 19, 51, 125, 313, 317
- Catch-22, 363
- CBC mode, 73–76, 78, 85, 236
 - and random access, 84
 - cut-and-paste attack, 84
 - repeated IV, 84
 - residue, 77, 85
- cell phone
 - cloning, 381, 399
 - first generation, 381
 - second generation, 381
 - third generation, 381
- CERT, 424
- certificate
 - authority, 112
 - revocation, 113
- certificate revocation list, *see* CRL
- challenge-response, 316, 319, 320
- change detection, 427–428
- Chinese Remainder Theorem, 100, 217
- chosen plaintext attack, 212

- Churchill, Winston, 38
CIA, 2
cipher, 20
cipher block chaining mode, *see* CBC mode
ciphertext, 20
Civil War, 35
Clinton, President, 505
Clipper chip, 39, 143
clock arithmetic, 524
clock skew, 330, 346
closed system, 462, 485
Cocks, Cliff, 95
Code Red, 422, 424
codebook cipher, 32–35, 46
 additive, 34
Cohen, Fred, 422
Common Criteria, 269–271
compartments, 6, 279–281, 303
Computer Emergency Response Team, *see* CERT
computer virus, *see* virus
confidentiality, 2, 10, 11, 109
 and integrity, 78
confused deputy, 273–274
confusion, *see* confusion and diffusion
confusion and diffusion, 39, 44, 51
 in AES, 82
 in DES, 81
cookie, 253, 258, 515
Coral Sea, 38
counter mode, *see* CTR mode
Coventry, 38
covert channel, 7, 281–283, 303, 304
 and TCP, 282, 283
 existence, 282
Covert_TCP, 283
CRC, 131–132, 155, 379
 collision, 155
crib, 177, 179
Cringely, Robert X., 403
CRL, 113
cryptanalysis, 20
 adaptively chosen plaintext, 42
 chosen plaintext, 41
 depth, 30–31, 36, 181
 differential, 187–190
 forward search, 42, 48, 122, 236
 known plaintext, 41
 linear, 190–191
 related key, 42
 taxonomy, 41
crypto, 20
 as a black box, 20
 terminology, 20
CRYPTO conferences, 39
cryptography, xvi, 3, 5, 20
 taxonomy, 40
cryptology, 20
cryptosystem, 20
CTR mode, 76, 83, 84
 and random access, 76
cyber disease, 432
cyclic redundancy check, *see* CRC

DAC, *see* discretionary access control
data confidentiality, *see*
 confidentiality
Data Encryption Standard, *see* DES
data integrity, *see* integrity
Daugman, John, 247
DDoS, 433
debit card protocol, 440
debugger, 448
decrypt, 20
defense in depth, 293, 308
demilitarized zone, *see* DMZ
denial of service, *see* DoS
Denver airport, 404
Department of Defense, *see* DoD
depth, 30–31, 36, 181
DES, 23, 39, 58–64, 67, 82, 85, 117,
 186–187
 confusion and diffusion, 81
 double, *see* double DES
 group, 225

- key schedule, 62–64
- S-box, 60, 62, 64, 188
- subkey, 57, 60, 62, 63, 82
- triple, *see* triple DES
- Descartes, Rene, 491
- differential cryptanalysis, 186–190
 - and TDES, 194–199
- Diffie, Whitfield, 91, 458
- Diffie-Hellman, 91, 100–102, 117
 - and MiM, 119
 - ECC, 105–106, 117
 - elliptic curve, 102
 - ephemeral, 328, 329, 361
 - MiM attack, 102
- diffusion, *see* confusion and diffusion
- digital certificate, 112–113, 115
- digital doggie, 261
- digital rights management, *see* DRM
- digital signature, 40, 90, 109, 115, 117, 123, 324, 325, 361, 379
 - protocol, 118
- digital watermark, 148–150
 - and Kerckhoffs' Principle, 152
 - fragile, 149
 - invisible, 149
 - robust, 149
 - visible, 149
- disassembler, 413, 448
- discrete log, 101, 102
- discretionary access control, 495–496
- distributed denial of service, *see* DDoS
- DMZ, 293
- DNS, 515
- DoD, 275, 277
 - and covert channel, 282
 - classifications and clearances, 275
- dog track problem, *see* voucher
- Domain Name Service, *see* DNS
- DoS, 3, 366
- double DES, 65–66, 82
 - attack, 65
- double transposition cipher, 26–27, 45
- DRM, 460–472, 485
 - analog hole, 463
 - and cryptography, 462
 - and human nature, 463
 - and Kerckhoffs' Principle, 463
 - and P2P, 469–470
 - and PDF, 465
 - and POS, 469
 - and SRE, 464
 - as hide and seek, 463
 - enterprise, 470–471
 - Exploit Systems, 469
 - failure, 471
 - MediaSnap system, 464–467
 - persistent protection, 461, 485
 - streaming media, 467–469
- ECB mode, 72–73, 75
- ECC, 91, 102
 - Diffie-Hellman, 102, 105–106, 117, 123
- EFF, *see* Electronic Frontier Foundation
- election of 1876
 - cipher, 35–37, 43, 44
- electoral college, 35
- electronic codebook mode, *see* ECB mode
- Electronic Frontier Foundation, 23
- Elgamal, 123
- elliptic curve, 103–106
 - addition, 103
 - example, 106
- elliptic curve cryptography, *see* ECC
- email, 422, 497, 510, 514
 - spoofed, 515
 - virus, 421
- Encapsulating Security Payload, *see* ESP
- encrypt, 20
- encrypt and sign, *see* public key cryptography
- encryption
 - weak, 284

- endian
 - little, 414
- Enigma, 12, 38, 168–174, 176–179, 218–221
 - attack, 176–179
 - cycles, 177
 - encryption, 170
 - key, 169
 - keyspace, 172–174
 - movable ring, 172
 - reflector, 171
 - rotor, 171
 - stecker, 169, 173, 178
 - ULTRA, 169
- ENORMOUS, 31
- entropy, 148
- ephemeral Diffie-Hellman, 328, 329
- ESP, 359, 371–372
 - null encryption, 371
- Ethernet, 521
- Euclidean Algorithm, 525
- Euler's Theorem, 96
- exact cover, 204
- exhaustive key search, 23, 24, 26, 43
- extended TEA, *see* XTEA
- Feistel cipher, 57–58, 67, 71, 81, 192
- Feistel, Horst, 57
- Feller, William, 527
- fence address, 492
- Fiat-Shamir, 335–339, 348, 349
 - challenge, 337
 - commitment, 337
 - response, 337
- fingerprint, 244, 260
 - minutia, 245
- Firewalk, 292, 307
- firewall, 7, 287–294, 306, 307, 426
 - and defense in depth, 293
 - and MLS, 276
 - application proxy, 288, 291–293, 307
 - packet filter, 288–290
 - personal, 293
 - stateful packet filter, 288, 290–291
- flash worm, 431–432
 - conjectured defense, 431
- FMEA, 478
- Ford, Henry, 266
- formal methods, 477
- Franklin, Benjamin, 89, 495
- fraud rate, 254
- freshness, 319
- FTA, 478
- gait recognition, 261
- Galton, Sir Francis, 244
- GCHQ, 90, 95, 100
- generator, 101
- Global System for Mobile Communications, *see* GSM
- Gram-Schmidt, 207, 209
- Greenglass, David, 31
- Groupe Spéciale Mobile, *see* GSM
- GSM, 8, 53, 381–389, 399
 - air interface, 381
 - anonymity, 383–384
 - authentication, 384
 - authentication center (AuC), 382
 - authentication protocol, 385
 - base station, 381
 - COMP128, 386
 - confidentiality, 384–385
 - crypto flaws, 386
 - design goals, 383
 - fake base station, 387–388
 - flashbulb, 387
 - home location registry (HLR), 382
 - IMSI, 382, 384
 - invalid assumptions, 386–387
 - key, 382
 - mobile, 381
 - optical fault induction, 387
 - partitioning attack, 387
 - PIN, 382

- security architecture, 383
 - SIM attacks, 387
 - SIM card, 382
 - system architecture, 381
 - visited network, 381
 - VLR, 382
- Hamming distance, 247
- hand geometry, 246–247
- hash function, 40, 41, 126–132
 - and CRC, 131
 - and digital signature, 127
 - and encryption, 157
 - and symmetric cipher, 129
 - as fingerprint, 127
 - avalanche effect, 133
 - birthday problem, 129
 - Bobcat, *see* Bobcat hash
 - coin flip, 158
 - collision, 126, 154, 155
 - collision resistance, 126
 - compression, 126
 - efficiency, 126
 - incremental, 158
 - k -way collision, 155
 - non-cryptographic, 130
 - one-way, 126
 - online auction, 156
 - online bid, 139–140
 - secure, 129
 - spam reduction, 140–141
 - Tiger, *see* Tiger hash
 - uses, 139
- hashed MAC, *see* HMAC
- hashed message authentication code,
see HMAC
- Hayes, Rutherford B., 35–37
- hazard analysis, 477
- HAZOP, 478
- Health Insurance Portability and
Accountability Act, *see*
HIPAA
- heap, 408
- heap overflow, 439
- Hellman, Martin, 91, 458
- Herodotus, 148
- hex editor, 449
- high water mark principle, 277, 303
- HIPAA, 470
- Hiss, Alger, 31
- HMAC, 78, 136–139, 379
 - RFC 2104, 138
- Honeywell, 498
- hosts, 511
- HTTP, 253, 353, 515
- hybrid cryptosystem, 108, 117
- Hypertext Transfer Protocol, *see*
HTTP
- ICMP, 292
- IDEA, 70
- identify friend or foe, *see* IFF
- IDS, 7, 294–296
 - anomaly-based, 295, 297–301, 310
 - host-based, 295
 - network-based, 295
 - signature-based, 295–297
- IFF, 315, 316, 346
- IKE, 359–366, 396
 - Phase 1, 360–366
 - Phase 2, 367–368
 - security association, 360
- IMAP, 515
- incomplete mediation, 418–419
- incremental transformation, 158
- inference control, 7, 283–284, 304
- information hiding, 148
- initialization vector, *see* IV
- insult rate, 254
- integer overflow, 439
- integrity, 2, 10, 76–78, 117
- International Data Encryption
Algorithm, *see* IDEA
- Internet, 511, 512, 515
- Internet Key Exchange, *see* IKE

- Internet Message Access Protocol, *see* IMAP
- Internet Protocol, *see* IP
- intrusion detection system, *see* IDS
- intrusion prevention, 294
- intrusion response, 295
- IP, 519–521
- address, 332, 515, 519
 - best effort, 519
 - fragmentation, 520
 - header, 520
 - version 4, 521
 - version 6, 358, 521
- IPSec, 7, 332, 359
- and IP header, 368
 - cookie, 362, 366, 396
 - security association, 367
 - transport mode, 369–370
 - tunnel mode, 369–370, 397
 - versus SSL, 358
- IPv6, *see* IP
- iris scan, 246–249
- iris code, 247
- IsDebuggerPresent, 483
- iTunes, 426
- IV, 35, 74, 83, 236, 355
- repeated, 84
- Java, 416, 448
- bytecode, 450
 - JVM, 450
 - SRE, 450, 481
- John the Ripper, 241
- Kahn, David, 37
- Karatsuba multiplication, 217
- Kerberos, 8, 330, 372–374, 509
- KDC, 373, 375, 376
 - key, 393
 - login, 374–375
 - replay prevention, 377
 - security, 376–377
 - stateless, 373
 - TGT, 373–376
 - ticket, 373, 375
 - TTP, 373
- Kerckhoffs' Principle, 21, 41, 151, 152, 386, 463, 466, 472, 474, 495
- key, 20, 53
- key diversification, 158, 399
- key escrow, 143–144
- keystream, 52
- King, Stephen, 461
- knapsack, 224
- cryptosystem, 91–95, 118, 119
 - problem, 92
 - superincreasing, 92, 207
- Kocher, Paul, 210
- Konheim, Alan, 186
- L0phtCrack, 241
- Lai-Massey multiplication, 70
- LAN, 521
- lattice, 203, 204
- lattice reduction, 95, 203–207
- attack, 203–210
- Lennon, John, xv
- LFSR, *see* shift register
- Liberty Alliance, 253
- Lincoln, Abraham, 37
- linear algebra, 527–529
- linear cryptanalysis, 186, 190–191
- and TDES, 199–202
- linear feedback shift register, *see* shift register
- linear independence, 529
- linearization attack, 434–436, 445
- TENEX, 436
- link layer, 513, 521–522
- Linux, 405
- LLL algorithm, 207, 208, 224
- local area network, *see* LAN
- logging, 497
- Longhorn, 500
- low water mark principle, 303
- Lucifer cipher, 58–60

- Luftwaffe, 38
- lunchtime attack, 42
- MAC, 379
 - and integrity, 77–78, 85, 86, 117, 136
 - and repudiation, 109
- MAC address, 521–522
- Mac OS X, 334, 475
- MAGIC, *see* Purple
- magnetic remanence, 496
- majority vote function, 53, 80
- malware, 4, 8, 14, 421
 - detection, 427–429
 - encrypted, 429
 - future, 429
 - metamorphic, 430
 - polymorphic, 430
- mandatory access control, 495–496
- Mars lander, 404
- Massey, James L., 70, 73
- matrix, 527
 - addition, 528
 - block, 528–529
 - identity, 528
 - multiplication, 528
 - square, 528
- Matsui, Mitsuru, 186
- McCartney, Paul, xv
- McLean, John, 277
- MD5, 70, 132
 - collision, 132, 159
- mean time between failure, *see* MTBF
- MediaSnap, Inc., 462, 464
- memory protection, 492–494
- Merkle, Ralph, 91, 92
- Merkle-Hellman knapsack, *see* knapsack cryptosystem
- message authentication code, *see* MAC
- message indicator, *see* MI
- MI, 34
- Microsoft
 - canary, 417
 - Death Star, 488
 - fallacy, 474
 - knowledge base article 276304, 231
 - MS-DRM, 472
 - Passport, 253
- Midway, 38
- MiG-in-the-middle attack, 316, 317
- MiM attack, 102, 117, 328
- mkdir, 419, 420
- MLS, 6–7, 274–276, 280, 303
- modular arithmetic, 95, 524–526
 - addition, 524
 - exponentiation, 96, 98
 - inverse, 94, 525
 - multiplication, 93, 524
 - repeated squaring, 211
- Montgomery multiplication, 217
- Monty Python, 229
- more eyeballs, 21, 473
- Morris Worm, 422–424
 - and NSA, 423
- mp3, 426
- MTBF, 475–476, 480, 487
- multilateral security, *see* compartments
- multilevel security, *see* MLS
- Musashi, Miyamoto, 210
- mutual authentication, 321–323, 325, 329, 341
- MV-22 Osprey, 404
- National Bureau of Standards, *see* NBS
- National Institute of Standards and Technology, *see* NIST
- National Security Agency, *see* NSA
- native code, 448
- NBS, 39, 59, 67
- need to know, 279, 303
- Netscape, 357, 405
- network
 - circuit switched, 512
 - client, 514

- core, 511
- edge, 511
- P2P, 469, 470, 514
- packet switched, 512
- server, 514
- network economics, 473, 480
- network interface card, *see* NIC
- network layer, 513, 519–521
- Next Generation Secure Computing Base, *see* NGSCB
- NGSCB, 339, 462, 500–506
 - and closed systems, 500
 - and DRM, 500, 508
 - and TTP, 503
 - and ZKP, 503
 - applications, 503–504
 - attestation, 503, 509
 - criticisms, 504–506
 - design goals, 501
 - feature groups, 502
 - malware, 509
 - NCA, 501, 504
 - Nexus, 501, 504
 - overview, 501
 - process isolation, 502
 - sealed storage, 502
 - secure path, 502
- NIC, 521
- NIDES, 300
- NIST, 39, 59, 67
- non-repudiation, 109–111, 117
- nonce, 319, 330, 355
- NP-complete, 92, 101
- NSA, xix, 59, 64, 67, 90, 186, 315
 - and DES, 59
 - and SIGINT, 59
- NULL cipher, 371
- number used once, *see* nonce
- NX bit, 416, 438
- object, 271
- Office Space, 14
- one way function, 90
- one-time pad, 27–31, 46, 79
 - VENONA, 31
- opaque predicate, 458
- open system, 454, 486
- operating system, 4, 8
 - trusted, 8, 495–499
- orange book, 266–269
- OS, *see* operating system
- OSI reference model, 513
- P2P, 433, 514
- paging, 493–494
- Palladium, 500
- Pascal, 147
- password, 6, 231–241, 319
 - and passphrase, 233
 - attack, 235, 255, 256
 - dictionary, 232, 236
 - generator, 251, 252, 258, 263, 264
 - hash, 235
 - keystroke logging, 241
 - LANMAN, 257
 - math of cracking, 237–240
 - salt, 236
 - selection, 232–234
 - social engineering, 241
 - verification, 235–237
 - versus key, 232
- Pearl Harbor, 37
- Peer-to-Peer, *see* P2P
- penetrate and patch, 472, 480
 - fallacy, 472
- perfect forward secrecy, *see* PFS
- permutation, 526
 - and DES, 60–63
 - and RC4, 55
 - and TDES, 192
- PFS, 327–329, 340, 347
- PGP, 114
- photo ID, 256
- physical layer, 513
- PIN, 231, 241, 252, 255, 315
- PKI, 108, 112–114

- anarchy model, 114
- monopoly model, 113
- oligarchy model, 114
- trust model, 113–114
- plaintext, 20
- Plankton, 421
- plausible deniability, 342, 365
- Poe, Edgar Allan, 19, 43
- Pokémon, 233
- poker
 - Texas hold 'em, 146–147
- Polish cryptanalysts, 38
- poly-alphabetic substitution cipher, 171
- POP3, 515
- port number, 520
- port scan, 289
- POS, 470
- Post Office Protocol, *see* POP3
- prime number, 525
- privacy, 11
- probability, 526–527
- protocol, xvi, 3, 7–8
 - header, 513
 - stack, 512–514
 - stateful, 512
 - stateless, 512
- PSTN, 382
- public key certificate, *see* digital certificate
- public key cryptography, 20, 323
 - encrypt and sign, 110, 111, 326, 330–332, 340
 - forward search, 122
 - key pair, 90
 - notation, 107
 - private key, 20, 90
 - public key, 20, 90
 - sign and encrypt, 110, 326, 330
 - uses, 107
- public key infrastructure, *see* PKI
- public switched telephone
 - network, *see* PSTN
- Purple, 37–38
- Różycki, Jerzy, 176
- rabbit, 421
- race condition, 419–420, 440
- random numbers, 145–148
 - cryptographic, 146
- randomness, *see* random numbers
- Ranum, Marcus J., 351
- RC4, 55–56, 70, 80, 148, 168, 179–185, 378
 - attack, 56, 181–185
 - initialization, 56, 180, 181
 - key, 180
 - keystream, 56, 180, 181
- RC6, 70
- reference monitor, 498
- Rejewski, Marian, 176
- related key attack, 180
- relatively prime, 525
- repeated squaring, 98–99, 211, 212, 214
- replay attack, 319, 346
- return-to-libc, 415
- reversing, *see* SRE
- RFC, 512
- RFC 2104, 138
- RFC 2407, 359
- RFC 2408, 359
- RFC 2409, 359
- RFC 2410, 371
- RFID tags, 11
- RGB colors, 163
- Rijndael, 67
- Ritchie, Dennis, 491
- Rivest, Ron, 70, 95, 167, 500
- Rosenberg, Ethyl, 31
- Rosenberg, Julius, 31
- rotors, 174–176, 221
- router, 511, 516
- routing protocols, 519
- RSA, 70, 91, 95–97, 117, 120
 - common encryption exponent, 100
 - cube root attack, 100, 116
 - decryption exponent, 96

- efficiency, 99
- encryption exponent, 96
- example, 97–98
- key pair, 96
- modulus, 96
- private key, 96
- public key, 96
- signature verification, 115, 116
- timing attack, 211–218, 224
- Rubin, Theodore I., 10
- Rueppel, Rainer, 52
- S-box
 - analysis, 190
- salami attack, 434, 446
- salt, 255
- SAML, 253
- Sarbanes-Oxley Act, *see* SOA
- Scherbius, Arthur, 169
- Schneier, Bruce, 58, 70, 447, 478
- SCOMP, 498
- Screamer, Beale, 472
- script kiddie, 295
- SDMI, 153, 471
- secrecy, 11
- secret key, 20
- secret sharing, 142–143
- secure cipher, 25
- Secure Digital Music Initiative, *see* SDMI
- Secure Sockets Layer, *see* SSL
- Security Assertion Markup Language,
 - see* SAML
- security by obscurity, 463
- security kernel, 498
- security modeling, 6, 274
- segmentation, 493–494
- Seneca, 265
- separation, 492
- session key, 325, 329, 331
- SHA–1, 133
- Shamir, Adi, 67, 95, 143, 180, 181,
 - 186, 335, 378
- Shannon, Claude, 39, 51, 148
- shift register, 53
 - initial fill, 53
- side channel attack, 210–211, 217
- SIGINT, 59
- sign and encrypt, *see* public key cryptography
- signature detection, 427–428
- Silicon Valley, xix
- Simple Mail Transfer Protocol, *see* SMTP
- simple substitution cipher, 22–25, 44
 - cryptanalysis, 24–25
- simplified TEA, *see* STEA
- single sign-on, 252–253
- slow worm, 443
- smartcard, 251
 - reader, 251
- smash the stack, *see* buffer overflow
- SMTP, 515
- SOA, 470
- socket, 520
- socket layer, 353
- software, xvi, 4, 8
 - active fault detection, 479
 - and trust, 436
 - bug injection, 479, 488
 - bugs, 404
 - cloned, 459
 - closed source, 473, 476, 488
 - configuration management, 479
 - design, 477
 - development, 472–480
 - error, 405
 - failure, 406
 - fault, 406
 - fault injection, 479
 - flaws, 8, 404, 476
 - genetic diversity, 460
 - guards, 457, 484
 - metamorphic, 430, 459
 - obfuscation, 458
 - open source, 473, 488

- peer review, 478
- postmortem analysis, 480
- tamper resistance, 457
- testing, 478–479
- software reverse engineering, *see* SRE
- space shuttle, 405
- SQL Slammer, 422, 425–426
 - and Internet traffic, 425
 - and UDP, 426
- square and multiply, *see* repeated squaring
- SRE, 8, 448–454, 474, 481, 484
 - example, 451
 - Java, 450, 481
- SSH, 7, 352–353
- SSL, 7, 51, 56, 353–356, 392
 - and HTTP, 357
 - connection, 357
 - MiM attack, 356, 393
 - pre-master secret, 355
 - session, 357
 - versus IPsec, 358
- stack, 408, 409
 - pointer, 408
- STE, 71, 225
- steganography, 148–149
 - and HTML, 151–152
 - and RGB colors, 150–152
 - collusion attack, 153
- Stimson, Henry L., 37
- stream cipher, 40, 52, 56, 79
- strong collision resistance, 126
- subject, 271
- substitution cipher
 - Vigenère, 47
- superincreasing knapsack, 92
- Swiss cheese, 179
- symmetric cipher, 20
- symmetric key
 - key diversification, 158
 - storage, 157
- symmetric key cryptography, 320
 - notation, 65
- Syrus, Publilius, 89
- system Z, 277
- tagging, 493
- TCB, 498–499, 507
- TCG, 500–501
- TCP, 353, 517–518
 - ACK, 518
 - ACK scan, 290
 - authentication, 332–334, 340
 - congestion control, 517
 - connection oriented, 517
 - DoS attack, 518
 - FIN, 518
 - flow control, 517
 - half-open connection, 518
 - header, 517
 - RST, 518
 - SEQ number, 333, 334
 - SYN, 518
 - SYN-ACK, 518
 - three-way handshake, 332, 518
- TCPA, 500
- TCSEC, 266–269
- TDES, 192–194, 223
 - differential cryptanalysis, 222
 - linear cryptanalysis, 223, 224
- TEA, 70–71, 81, 83
 - decryption, 72
 - encryption, 71
- TENEX, 436
- Texas hold 'em poker, 146–147
- Thomborson, Clark, 505
- Tiger hash, 133–136
 - inner round, 134, 136
 - key schedule, 135, 137
 - outer round, 134, 135, 155
 - S-boxes, 135
- Tilden, Samuel J., 35–37
- time bomb attack, 436
- time to live, *see* TTL
- timestamp, 330–332, 340, 341
- timing attack

- Kocher's, 214–217
- Tiny DES, *see* TDES
- Tiny Encryption Algorithm, *see* TEA
- Torvalds, Linus, 504
- totient function, 525
- transport layer, 513, 516–519
- trap door one way function, 90
- trapdoor, *see* backdoor
- trinity of trouble, 438
- triple DES, 65–66, 86
- trojan, 421, 426–427, 441
- Trudy, 1
- trust versus security, 495
- trusted computing base, *see* TCB
- Trusted Computing Group, *see* TCG
- Trusted Computing Platform Alliance, *see* TCPA
- Trusted Computing System
 - Evaluation Criteria, *see* TCSEC
- trusted OS, *see* operating system
- trusted path, 497
- trusted third party, *see* TTP
- TTL, 292, 307, 368, 371, 520
- TTP, 112
- Turing test, 285
- Turing, Alan, 38, 177, 285
- Twain, Mark, 244, 351
- two-factor authentication, 252

- U.S. Postal Service, 516
- UDP, 303, 519
- ULTRA, *see* Enigma

- VENONA, 31
 - decrypt, 32
- VeriSign, 113
- Vernam cipher, 27, *see* one-time pad
- virus, 421, 422
 - boot sector, 421
 - memory resident, 422
- Vista, 500
- visual cryptography, 144–145

- voucher, 394

- Walker spy ring, 40
- Warhol worm, 430–431
- watermark, *see* digital watermark
- weak collision resistance, 126
- Web cookies, *see* cookies
- Welchman, Gordon, 177
- WEP, 8, 51, 56, 132, 168, 179–180, 377–381, 398
 - initialization vector, 180, 181, 379
- Whitehead, Alfred North, 313
- Williamson, Malcolm J., 100
- Windows, 405, 498, 500
 - PE file format, 449
- Wonka, Willy, 447
- worm, 421, 422, 424, 425, 430
- wu-ftp, 474

- XTEA, 71

- zero knowledge prof, *see* Stamp, Mark
- zero knowledge proof, *see* ZKP
- Zimmermann telegram, 32–34
- Zimmermann, Arthur, 32
- ZKP, 335–339
- zombie, 433
- Zygalski, Henryk, 176