A
access control list (ACL), 285–286
accumulator
  events, 151
  pools, 151
  randomness, 147–155
ACL. See access control list
addition
  bitwise, 51
  modular, 246
  modulo, 168–169
  without carry, 51
AddRandomEvent, 154–155
add-with-carry, CPU, 243
Adelman, Leonard, 195
administrators, 127
Advanced Encryption Standard (AES),
  54–56, 78, 321–322
initialization, 132
  128-bit, 54
randomness generator, 143
rounds, 54–55
RSA, 205
S-box, 54
testing, 244
adversarial setting, 7–8
failure rate, 244
AES. See Advanced Encryption
  Standard
  algorithms, 24–25
  binary, 179
  distinguishers, 47–48
  efficiency, 37
  extended Euclidian algorithm,
    171–172
  Kerckhoff’s principle, 44
  primes, 164
  public keys, 28
  secure channel, 107–112
  wooping, 246
Anderson, Ross, 18
Applied Cryptography (Schneier), 18,
  323
The Art of Computer Programming
  (Knuth), 140
ASN.1, 220
assertions, 130–131
asymmetric key, encryption, 28
ATM, PIN code, 288
atomicity, file system updates, 158
attack tree, 5–6
attacks, 31–33. See also specific attack
types
  block ciphers, 44–45
  entropy, 142
  hash functions, 79
  MAC, 90
  plaintext, 69
attacks, (continued)
quantum physics, 139
RF, 252
RSA, 205
steps, 36
authentication, 25–27. See also
message authentication code
clock, 264
conventions, 230–231
encryption, 63, 71, 102–104
GMAC, 94
key negotiation, 227–228
MAC, 96, 102–104, 106
message order, 26
messages, 229
protocols, 97
public key, 189
secret keys, 26
secure channel, 102–104, 106
session keys, 229
symmetric keys, 239
authorization, PKI, 285–286

ciphertext c, 43, 49–50
ciphertext-only attack, 44
generic attacks, 47
GMAC, 94
hash functions, 45
ideal, 46–50
interface, 45
Kerckhoff's principle, 44
128-bit, 43
permutations, 44, 46
plaintext, 43, 49–50
rounds, 50–51
secret keys, 43
testing, 244
256-bit, 43
Boojum, 126
Bos, Jurjen, 245
bridges, 7, 14–15
buffer overflow, 131

B
backups, VMs, 157–158
banks
CA, 276
credit card organization, 277
Biham, Eli, 44
binary algorithm, 179
biometrics, 308–309
birthday attacks, 33–34
hash functions, 84
HMAC, 93
meet-in-the-middle attacks, 35
bitslice implementation, 56
bitwise addition, 51
blind signatures, 252
block cipher mode, 44, 63–76
ciphertext c, 64
padding, 64–65
block ciphers, 43–62
attacks, 44–45
chosen-plaintext attack, 44

C
C++, 121–122
CA. See certificate authority
cache
CPU, 124, 152, 251
secrets, 124
Carmichael numbers, 177
CBC. See cipher block chaining
CCM, 71, 112–113
CEN. See European Committee for
Standardization
certificate(s), 30
credential systems, 286–288
multilevel, 277–278
PKI, 275, 277–278, 295–297
self-certifying, 296
SSL, 218
certificate authority (CA), 30
banks, 276
fast expiration, 290–291
liability, 30
PKI, 275–276, 283–285
RA, 279–280
root key, 293, 296–297
trust, 30
certificate chain, 277
certificate revocation list (CRL), 289–290
key servers, 292–293
Chaum, David, 245
checks. See testing
Chinese Remainder Theorem (CRT), 196–199
complexity, 198
exponentiations, 198
multiplication, 198
signatures, 239
chosen-ciphertext attack, 32
chosen-key attack, 45
chosen-plaintext attack, 32
block ciphers, 44
distinguishers, 48
cipher block chaining (CBC), 65–68
information leakage, 72, 74
MAC, 91–93
ciphertext c, 24
block cipher mode, 64
block ciphers, 43, 49–50
plaintext, 64
ciphertext-only attack, 31
block ciphers, 44
distinguishers, 48
clock, 259–268
authentication, 264
counters, 264
expiration time, 260
monotonicity, 260
PKI, 264
real-time clock chip, 261
real-time transactions, 260–261
security, 262–263
setting back, 262
setting forward, 263
stopping, 262–263
time, 266–267
time synchronization, 264
unique value, 260
CMAC, 93
code quality, 128
The Codebreakers (Kahn), 18
collision(s), 34
chances of, 73–74
hash functions, 84
collision attacks, 33–35
DH, 190
stream cipher, 69
collision resistance, 78
complexity, 17
CRT, 198
protocols, 238–241
security, 129
test-and-fix, 37–38
composites, 164
constant-time operations, 252
conventions, authentication, 230–231
correct programs, 116–119
test-and-fix, 118
counter IV, 66
counter mode (CTR), 70–71
counter mode (CTR), 70–71
encryption, 106
GMAC, 94
information leakage, 73, 74
counters
clock, 264
same-state problem, 266
CPU, 15–16
add-with-carry, 243
cache, 124, 152, 251
hash functions, 152
multiplication, 251
registers, 127
secrets, 122
credential systems
delegation, 287–288
PKI, 286–288
credit card(s)
digital signature, 11
PIN code, 11
SET, 10–11
viruses, 11
credit card organization, banks, 277
CRL. See certificate revocation list
CRT. See Chinese Remainder Theorem
Crypto-Gram, 18
CTR. See counter mode
current events, 19–20
CWC, 112–113

D
Data Encryption Standard (DES),
51–54
exhaustive search attack, 53
56-bits, 51
rounds, 51–52
64-bit, 52
data integrity, 127–128
data-dependent rotation, 251
Data Encryption Standard (DES), 55
Davies-Meyer hash function, 45
d debuggers, 127, 128
decryption, 24, 63
RSA, 207–208, 251
DECRYPTRANDOMKeyWithRSA,
207–208
defense in depth, 7
del egation, credential systems,
287–288
denial-of-service attack (DOS), 103
DES. See Data Encryption Standard
detection, security, 16
DH. See Diffie-Hellman key exchange
protocol
dictionary attack
offline, 241
passwords, 228
Diffie, Whitfield, 181
Diffie-Hellman key exchange protocol
(DH), 181–193
collision attacks, 190
groups, 182–183
information leakage, 248
man-in-the-middle attack, 184–185
pitfalls, 185–186
public keys, 239
safe primes, 186–187
Station-to-Station protocol, 228
subgroups, 187–188, 191
testing, 248
digest, 77
digital rights management (DRM), 14
digital signature
credit cards, 11
public key, 30
public keys, 29
RSA, 200
SET, 11
Dijkstra, Edsger, 118
direct authorization, 286
discrete logarithm (DL), 183
distinguishers
algorithms, 47–48
chosen-plaintext attack, 48
ciphertext-only attack, 48
known-plaintext attack, 48
distinguishing attack, 32–33
divisibility, primes, 163–166
DL. See discrete logarithm
Document Template Definition (DTD),
221
DOS. See denial-of-service attack
DRAM. See Dynamic RAM
DRM. See digital rights management
DTD. See Document Template
Definition
Dynamic RAM (DRAM), 125

E
EC. See error-correcting code memory
ECB. See electronic cookbook
EEPROM, 313
efficiency, 15
algorithms, 37
public keys, 28
safe primes, 187
Einstein-Podolsky-Rosen paradox, 139
Electrical and Electronics Engineers
(IEEE), 317
electronic banking, 276
electronic cookbook (ECB), 65
information leakage, 72
electronic payment systems, 260–261
encryption, 23–39
asymmetric key, 28
authentication, 63, 71, 102–104
CTR, 106
MAC, 102–104
public keys, 27–29, 189
RSA, 206–209, 248
secret keys, 24
secure channel, 102–104, 106–107
storage, 24
symmetric keys, 28
encryptRandomKeyWithRSA, 207
entropy, 137–138
attacks, 142
keystrokes, 147–148
mouse movements, 147–148
passwords, 302
pools, 149
sources of, 147–148
EPROM, 313
Eratosthenes, 164
error-correcting code memory (ECC), 128
events
accumulator, 151
pools, 150–151
randomness, 154–155
exhaustive search attack, 36
DES, 53
hash functions, 84
expiration time
certificates, 279
clock, 260
keys, 278–279, 299
public keys, 278–279
exponentiations, 179
CRT, 198
extended Euclidean algorithm, 171–172
extendedGCD, 171–172
RSA, 200

F
failure rate, adversarial setting, 244
fast expiration, CA, 290–291
FEAL, 55
Feistel construction, 52
Twofish, 57
Ferguson, Niels, 5, 11, 112, 132, 191, 222, 240, 260
Fermat test, 177
56-bits, DES, 51
file system updates, atomicity, 158
finally, 122
fingerprint, 77
fingerprint scanners, 308–309
finite fields, 169–170
firewall, LAN, 10
512-bit, 79
fixed IV, 66
floating point registers, 127
Fortuna, 142
forward secrets, 238
*Foundations of Cryptography* (Goldreich), 18
functional specification, 117
fundamental theorem of arithmetic, 165

G

garbage collection, 122
Garner’s formula, 196–197
GCD. See greatest common divisor
GCM, 71
GMAC, 113
GenerateBlocks, 146–147
GenerateLargePrime, 174, 203
generateRSAKey, 204–205
generateRSAPrime, 203–204
generator. See also pseudorandom
number generators; random
number generators
pools, 151
randomness, 143–147
reseeds, 152
speed, 147
generic attacks, 14
block ciphers, 47
hash functions, 79
GMAC, 94–95
authentication, 94
GCM, 113
interface, 94
Goldbach conjecture, 165
Goldreich, Oded, 18
greatest common divisor (GCD), 170–171
groups, 169–170
DH, 182–183
Gutmann, Peter, 312

H

*Handbook of Applied Cryptography*
(Menezes, van Oorschot, and Vanstone), 18, 243
hard drive, secrets, 301
hash functions, 77–88
attacks, 79
birthday attacks, 84
block ciphers, 45
collisions, 84
CPU, 152
exhaustive search attack, 84
generic attacks, 79
ideal, 79, 151
iterative, 80, 93
length extension bug, 83–84
NIST, 78
partial-message collision, 84
pools, 152
random mapping, 84, 207
security, 78–79
testing, 244
universal, 94, 112–113
weaknesses, 83–87
Hellman, Martin, 181
HMAC, 86, 93–94
birthday attacks, 93
iterative hash functions, 93
key recovery attacks, 93
SHA-1, 93
Horton Principle, 96–97
message identifiers, 220
Housley, Russ, 112
human memory
passwords, 302–303
secrets, 302–306

I

iButton, 306
IDEA, 55
side-channel attacks, 250
ideals
  block ciphers, 46–50
hash functions, 79
MAC, 90
identifiers
  messages, 253–254
  protocols, 253–254
IEEE. See Electrical and Electronics Engineers
IETF. See Internet Engineering Task Force
IKE. See Internet Key Exchange
implementation, 115–134
design, 117
incentive, protocols, 215–217
indirect authorization, 285
information leakage, 33, 72–75
  DH, 248
initialization
  AES, 132
  secure channel, 107–108
  SSL, 37
initialization vector, 66
INITIALIZEGENERATOR, 145
INITIALIZEPRNG, 153
InitializeSecureChannel, 113
insiders, 10
instance identifiers, protocols, 253–254
interface
  block ciphers, 45
  GMAC, 94
International Organization for Standardization (ISO), 317
Internet Engineering Task Force (IETF), 317, 321
Internet Key Exchange (IKE), 191–192
Introduction to Modern Cryptography (Katz and Lindell), 18
IPsec, 101
message order, 111
iris scanners, 308–309
ISO. See International Organization for Standardization
  ISO 9001, 119
  isPrime, 175, 187
  iterative hash functions, 80, 151
  HMAC, 93
J
  Java, 122
K
  Kahn, David, 18
  Katz, Jonathan, 18
  Kelsey, John, 141
  Kerberos, 270–271, 273
  Kerckhoff’s principle, 24–25
  algorithms, 44
  block ciphers, 44
  key(s). See also specific key types
    compromise of, 238
    expiration time, 299
    key servers, 272
    phases of, 297–298
    secure channel, 100
    64-bit, 34–35
    key negotiation, 227–242, 272
    authentication, 227–228
    passwords, 228, 241
    secret keys, 228
    key recovery attacks, HMAC, 93
    key servers, 269–274
    CRL, 292–293
    keys, 272
    PKI, 292–293
    rekeying, 272–273
    secure channel, 272
  keystrokes
    entropy, 147–148
    randomness, 138
  known-plaintext attack, 31
  distinguishers, 48
  Knuth, Donald E., 140
  Kohno, Tadayoshi, 112
LAN, firewall, 10
large integer arithmetic, 243–249
errors, 244
side-channel attacks, 245
wooping, 246
law, trust, 214
LCM. See least common multiple
least common multiple (LCM), 171
Legendre symbol, 187
length extension bug, hash functions, 83–84
liability
CA, 30
VeriSign, 30
Lindell, Yehuda, 18
local time, 266
long-term card key, 240
MAC. See message authentication code
MAD. See Mutually Assured
Destruction
man-in-the-middle attack, DH, 184–185
MARS, 58
side-channel attacks, 250
mathematics, 75
RSA, 205
MD4, 81
MD5, 81
meet-in-the-middle attacks, 34–35
birthday attacks, 35
memory
human, 302–306
secrets, 125–127
XOR, 126
memset, 121
Menezes, A.J., 18, 243
message authentication code (MAC), 26–27, 89–98
attacks, 90
authentication, 96, 102–104, 106
CBC, 91–93
data integrity, 127
encryption, 102–104
ideal, 90
meet-in-the-middle attacks, 35
passwords, 241
random mapping, 93
security, 90
tags, 89, 103
XOR, 93
message digest functions. See hash functions
message identifiers
Horton Principle, 220
protocols, 219–220
message numbers, 26–27, 102
secure channel, 105
message order
authentication, 26
secure channel, 111–112
messages
authentication, 229
encoding, 220
identifiers, 253–254
 parsing, 220
protocols, 218–225, 253–255
secure channel, 100–101, 108–109
TCP, 219
MinPoolSize, 154
modular addition, 246
modular multiplication, 246
modularization, 129–130
protocols, 218, 240–241, 273
modulo
addition, 168–169
multiplication, 169, 249–250
primes, 167–173
subtraction, 168–169
wooping, 245
modulo 2, 172–173
modulo n, 199–200
monotonicity, clock, 260
Monte Carlo simulation, 144
Montgomery multiplication, 179, 249–250
Moore’s law, 305
mouse movements, entropy, 147–148
MsgCntSend, 109
MsgToRSA_Number, 209–210
multilevel certificates, 277–278
multiplication
  CPU, 251
  CRT, 198
  modular, 246
  modulo, 169, 249–250
  Montgomery, 179
multiplicative group modulo p, 170
Mutually Assured Destruction (MAD), 214

N
  names, PKI, 281–283
  National Institute of Standards and Technology (NIST), 54
  hash functions, 78
  primes, 193
  SHA, 82
  network security, 14
  NIST. See National Institute of Standards and Technology
  nonce-generated IV, 67–68
  GMAC, 94
  nonrepudiation, 293
  NSA, 80
  SHA, 82
  NTP, 264

O
  OCB, 112–113
  OCSP. See Online Certificate Status Protocol
  odd permutations, 49
  OFB. See output feedback
  offline
    chosen-plaintext attack, 32
dictionary attack, 241
  128-bit, 60
  AES, 54

block ciphers, 43
GMAC, 94
MD5, 81
passwords, 302
security, 36
160-bit, 82
192-bit, 60
online
  certificate verification, 291
  chosen-plaintext attack, 32
  Online Certificate Status Protocol (OCSP), 291
  output feedback (OFB), 68–69
  information leakage, 73
  overwriting data, 312–313

P
  padding
    block cipher mode, 64–65
    RSA, 205–206
  paranoia, 8
    exercises, 18–21
    protocols, 218
  parity, permutations, 49–50
  parity attacks, 49
  parsing, messages, 220
  partial-message collision, hash functions, 84
  passphrases, 303
  Password Safe, 309
  passwords, 6
    dictionary attack, 228
    entropy, 302
    human memory, 302–303
    key negotiation, 228, 241
    MAC, 241
    128-bit, 302
    salting, 304–306
    64-bit, 303
    stretching, 304–306
    256-bit, 302
    patents, 322
    PayPal, phishing, 218
    PC Card, 306
PDA, secrets, 301
performance, security, 14–17, 37
permutations
  block ciphers, 44, 46
  even, 49, 50
  odd, 49
  parity, 49–50
phishing, PayPal, 218
PHT, 57
physical threat, trust, 214
PIN code
  ATM, 288
  credit cards, 11
  errors, 222
  secure token, 307–308
SET, 11
PKCS#1 v2.1, 206
PKI. See public key infrastructure
plaintext, 24
  attacks, 69
  block cipher mode, 64
  block ciphers, 43, 49–50
  ciphertext c, 64
pools
  accumulator, 151
  entropy, 149
  events, 150–151
  generator, 151
  hash functions, 152
  randomness, 148–150
  reseeds, 149
portable storage, 306
powers, 179
prevention, security, 16
primes, 163–180
  algorithms, 164
  divisibility, 163–166
  large, 173–179
  modulo, 167–173
  NIST, 193
  primitive elements, 173
  safe, 186–187
  small, 166–167
  testing, 176–178
  256-bit, 190
  wooping, 245
  primitive elements, 17, 36, 44, 64, 93,
    100, 182
  primes, 173
  privacy, storage, 283
  private keys, 202–203
  PRNGs. See pseudorandom number
generators
  probabilities, 75
  professional paranoia, 8
  exercises, 18–21
  protocols, 218
  proof by contradiction, 165
  proof of security, 299
  protocols, 213–225. See also specific
    protocols
    authentication, 97
    complexity, 238–241
    errors, 221–222
    execution states, 221
    identifiers, 253–254
    incentive, 215–217
    instance identifiers, 253–254
    message identifiers, 219–220
    messages, 218–225, 253–255
    modularization, 218, 240–241, 273
    paranoia, 218
    professional paranoia, 218
    roles, 213–214
    secure channel, 253
    smart cards, 240
    steps, 218–225
    timeouts, 255
    trust, 214–215, 217–218
    versions, 229–230
  pseudorandom data, 140
  pseudorandom function, 143–147
  pseudorandom number generators
    (PRNGs), 140–142
  PseudoRandomData, 146–147, 152
  public exponents, RSA, 201–202
  public key(s)
    algorithms, 28
<table>
<thead>
<tr>
<th>Authentication</th>
<th>Digital Signature</th>
<th>Efficiency</th>
<th>Encryption</th>
<th>Expiration Time</th>
<th>PKI</th>
<th>Primes</th>
<th>RSA</th>
<th>Secret Keys</th>
<th>SSL</th>
<th>Symmetric Keys</th>
<th>Timing Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Key Servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Names</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Practicalities</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Public Keys</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Reality of, 281–294</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Refinery Sensors</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Revocation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Rekeying, Key Servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RC4, 323–324</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RC6, 58</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Real-time Clock Chip</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Same-state problem</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Real-time Transactions, Clock</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ReceiveMessage, 110–111</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Reductio Ad Absurdum (Proof by Contradiction)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Refinery Sensors, PKI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Registers, CPU</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Registration Authority (RA)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Rekeying, Key Servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Related-key Attack</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Replay Attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Reputation, Trust</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ReSeedCnt, 154</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Reseeds, 145</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Generator, 152</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Pools, 149</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Resends</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Secure Channel</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Timing of, 255</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Response, Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Retry Attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TCP, 223</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>UDP Packets, 223</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Revocation, PKI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RF Attacks, 252</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Side-channel Attacks</td>
</tr>
</tbody>
</table>

**Q**
- Quantum Physics, Attacks, 139

**R**
- RA. See Registration Authority
- Rabin-Miller Test, 175–178
- Random Delay, 251
- Random IV, 66–67
- Random Mapping
- Hash Functions, 84, 207
- MAC, 90, 93
- Random Number Generators, 139
- Same-state Problem, 265
- RandomData, 152, 153
- Randomness, 137–161
- Accumulator, 147–155
- Events, 154–155
- Generator, 143–147
- Keystrokes, 138
- Pools, 148–150
- Secret Keys, 12
- RC4, 323–324
- RC6, 58
- Real-time Clock Chip, 261
- Same-state Problem, 265
- Real-time Transactions, Clock, 260–261
- ReceiveMessage, 110–111
- Reductio Ad Absurdum (Proof by Contradiction), 165
- Refinery Sensors, PKI, 277
- Registers, CPU, 127
- Registration Authority (RA), CA, 279–280
- Rekeying, Key Servers, 272–273
- Related-key Attack, 45
- Replay Attacks, 223–225
- Reputation, Trust, 214
- Requirements, 117
- ReSeedCnt, 154
- Reseeds, 145
- Generator, 152
- Pools, 149
- Resends
- Secure Channel, 102
- Timing of, 255
- Response, Security, 16
- Retry Attacks, 223–225
- TCP, 223
- UDP Packets, 223
- Revocation, PKI, 289–292
- RF
- Attacks, 252
- Side-channel Attacks, 132
Rijndael, 54
  randomness generator, 143
risk, trust, 215
Rivest, Ron, 81, 195
roles
  protocols, 213–214
  secure channel, 99–100
root key, CA, 293, 296–297
rounds
  AES, 54–55
  block ciphers, 50–51
  DES, 51–52
RSA, 195–211
  AES, 205
  attacks, 205
  decryption, 207–208, 251
  digital signature, 200
  encryption, 206–209, 248
  EXTENDEDGCD, 200
  mathematics, 205
  padding, 205–206
  pitfalls, 205–206
  public exponents, 201–202
  public keys, 239
  signatures, 239, 248
  SSL, 251
  symmetric keys, 302
  testing, 248–249
RSA-OAEP, 206
RSA-PSS, 206

S
safe primes
  DH, 186–187
  efficiency, 187
salting, passwords, 304–306
same-state problem, 265–266
S-box. See substitution box
Schilder, Marius, 240
Schneier, Bruce, 18, 323, 326
  secret keys
    authentication, 26
    block ciphers, 43
    encryption, 24
key negotiation, 228
management, 14
PKI, 275–276
public keys, 28, 275–276
randomness, 12
secure tokens, 307
storage, 12, 14
256-bit, 306
secrets, 120–128
cache, 124
CPU, 122
forward, 238
hard drive, 301
human memory, 302–306
memory, 125–127
PDA, 301
secure channel, 101–102, 120
sharing, 310–311
smart phones, 301
storage, 301–314
swap files, 122–124
virtual memory, 122–124
wiping state, 311–313
Secrets and Lies (Schneier), 18, 326
secure channel, 99–114
  algorithms, 107–112
  authentication, 102–104, 106
  encryption, 102–104, 106–107
  initialization, 107–108
  key servers, 272
  keys, 100
  message numbers, 105
  message order, 111–112
  messages, 100–101, 108–109
  properties, 101–102
  protocols, 253
  resends, 102
  roles, 99–100
  secrets, 101–102, 120
Secure Hash Algorithm (SHA), 79, 82
secure tokens, 306–308
PIN code, 307–308
secret keys, 307
secure UI, 307–308
<table>
<thead>
<tr>
<th>Security Features</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clock</td>
<td>IDEA, 250</td>
</tr>
<tr>
<td>Complexity</td>
<td>Large integer arithmetic, 245</td>
</tr>
<tr>
<td>Detection</td>
<td>MARS, 250</td>
</tr>
<tr>
<td>Evolving Systems</td>
<td>RF, 132</td>
</tr>
<tr>
<td>Features</td>
<td>Signatures. See also digital signature</td>
</tr>
<tr>
<td>Hash Functions</td>
<td>blind, 252</td>
</tr>
<tr>
<td>Level</td>
<td>CRT, 239</td>
</tr>
<tr>
<td>MAC</td>
<td>RSA, 209–211, 239, 248</td>
</tr>
<tr>
<td>Mindset</td>
<td>SignWithRSA, 210</td>
</tr>
<tr>
<td>128-bit</td>
<td>Simplicity, 129</td>
</tr>
<tr>
<td>Performance</td>
<td>Single sign-on, 309</td>
</tr>
<tr>
<td>Prevention</td>
<td>64-bit</td>
</tr>
<tr>
<td>Response</td>
<td>DES, 52</td>
</tr>
<tr>
<td>Reviews</td>
<td>Encryption, 106</td>
</tr>
<tr>
<td>Standards</td>
<td>Keys, 34–35</td>
</tr>
<tr>
<td>Weakest Link</td>
<td>Message numbers, 105</td>
</tr>
<tr>
<td>Security Engineering (Anderson)</td>
<td>Passwords, 303</td>
</tr>
<tr>
<td>Seed Files</td>
<td>SmallPrimeList, 166</td>
</tr>
<tr>
<td>Self-Certifying Certificate</td>
<td>Smart cards, 222, 306</td>
</tr>
<tr>
<td>SendMESSAGE</td>
<td>Protocols, 240</td>
</tr>
<tr>
<td>Sequences</td>
<td>Smart phones, secrets, 301</td>
</tr>
<tr>
<td>Serpent</td>
<td>SNTTP, 264</td>
</tr>
<tr>
<td>Randomness Generator</td>
<td>Social Security number (SSN), 283</td>
</tr>
<tr>
<td>Session Keys</td>
<td>SoFi number, 283</td>
</tr>
<tr>
<td>Authentication</td>
<td>Software bugs, 14</td>
</tr>
<tr>
<td>SET</td>
<td>Specifications, 117–118</td>
</tr>
<tr>
<td>Credit Cards</td>
<td>Splitting operations, 110</td>
</tr>
<tr>
<td>Digital Signature</td>
<td>SRAM. See Static RAM</td>
</tr>
<tr>
<td>PIN Code</td>
<td>SRP, 241</td>
</tr>
<tr>
<td>Viruses</td>
<td>SSH, 101</td>
</tr>
<tr>
<td>SHA</td>
<td>SSL certificates, 218</td>
</tr>
<tr>
<td>SHA-0, 82</td>
<td>Initialization, 37</td>
</tr>
<tr>
<td>SHA-1, 79, 82</td>
<td>PKI, 321</td>
</tr>
<tr>
<td>HMAC, 93</td>
<td>Public keys, 37</td>
</tr>
<tr>
<td>SHA-2, Fixes for</td>
<td>RSA, 251</td>
</tr>
<tr>
<td>SHA-224, 82–83</td>
<td>SSL/TLS, 101</td>
</tr>
<tr>
<td>SHA-256, 79, 82–83</td>
<td>SSN. See Social Security number</td>
</tr>
<tr>
<td>SHA-512, 79, 82–83</td>
<td>Security, 320</td>
</tr>
<tr>
<td>Shamir, Adi, 195</td>
<td>SSL, 320–321</td>
</tr>
<tr>
<td>Side-Channel Attacks, 33, 132–133, 250–252</td>
<td>Start-of-protocol attack, 255</td>
</tr>
</tbody>
</table>
Static RAM (SRAM), 125
Station-to-Station protocol, DH, 228
steps
attacks, 36
protocols, 218–225
storage
encryption, 24
portable, 306
privacy, 283
secret keys, 12, 14
secrets, 301–314
XOR, 126
stream cipher, 68
collision attacks, 69
XOR, 69
stretching, passwords, 304–306
STU-III, 290
subgroups, DH, 187–188, 191
subsequences, 27
substitution box (S-box), 52
AES, 54
Twofish, 57
subtraction, modulo, 168–169
Sun Tzu, 196
superusers, 127, 128
swap files, secrets, 122–124
symmetric keys
authentication, 239
encryption, 28
public keys, 29, 188–189
RSA, 302
SYN flood attack, 255
System.gc(), 122
System.runFinalization(), 122
complexity, 37–38
correct programs, 118
testing, 13, 131–132
AES, 244
block ciphers, 244
DH, 248
Fermat, 177
hash functions, 244
primes, 176–178
Rabin-Miller, 175–178
RSA, 248–249
32-bit
encryption, 106–107
MD4, 81
message numbers, 105
SHA-1, 82
threat model, 10–12
time, clock, 266–267
time server, 264
time stamps, 260
time synchronization, clock, 264
timeouts, protocols, 255
timing attacks
errors, 221–222
public keys, 250–251
TLS, 321
TLV. See Tag-Length-Value
traffic analysis, 101
transient secrets, 120
transport layer, 219
trust
CA, 30
ethics, 214
law, 214
MAD, 214
physical threat, 214
PKI, 284–285
protocols, 214–215, 217–218
reputation, 214
risk, 215
try-finally, 122
256-bit, 60
block ciphers, 43
passwords, 302

T
Tag-Length-Value (TLV), 220
tags, MAC, 89, 103
TCP
messages, 219
retry attacks, 223
TCP/IP, 101
message order, 112
test-and-fix

sun Tzu, 196
temporary secrets, 120
transport layer, 219
trust
CA, 30
ethics, 214
law, 214
MAD, 214
physical threat, 214
PKI, 284–285
protocols, 214–215, 217–218
reputation, 214
risk, 215
try-finally, 122
256-bit, 60
block ciphers, 43
passwords, 302

T
Tag-Length-Value (TLV), 220
tags, MAC, 89, 103
TCP
messages, 219
retry attacks, 223
TCP/IP, 101
message order, 112
test-and-fix
primes, 190
secret keys, 306
Twofish, 45, 57–58
randomness generator, 143

**U**
UDP packets, 219
  retry attacks, 223
uncertainty, 137
unique value, clock, 260
universal hash function, 94
  CWC, 112–113
universal PKI, 276, 284
UNIX, 127
UpdateSeedFile, 156
USB dongle, 306
USB stick, 12
  storage, 306
UTC, 267

**V**
van Oorschot, Paul C., 18, 243
Vanstone, S.A., 18, 243
VerifyRSASignature, 210
VeriSign, liability, 30
version-rollback attack, 230
versions, protocols, 229–230
Viega, John, 112
virtual machines (VMs), 141–142
  backups, 157–158
virtual memory, secrets, 122–124
virtual private network (VPN), PKI,
  276
viruses
  credit cards, 11
  SET, 11
  VMs. See virtual machines
  VPN. See virtual private network

**W**
weakest link, security, 5–7
WEP. See wired equivalent privacy
whitening, 57
Whiting, Doug, 112
wiping state, 121–122
  secrets, 311–313
wired equivalent privacy (WEP),
  323–324
wooping, 245–248
  algorithms, 246
  errors, 247
  large integer arithmetic, 246
  modulo, 245
  primes, 245
WriteSeedFile, 156

**X**
XML, 221, 295
XOR. See exclusive-or operation
X.509v3, 279, 295

**Y**
Yarrow, 141

**Z**
Zener diode, 139