
Index

- Abnormal program terminations, 305–307
Abstract data types, 218–224,235–238
ACCAT Guard, 321–324
Access controls, 6–7,153–154,166,191–258
Access matrix model, 192–200,209–210,217,228,
240–248
Achugbue, J. O., 372
Activators, 224
Ada, 209,219,223
ADEPT-50 system, 287
Adleman, L., 13,101,103–108,110,157,170
Affine transformation, 64,66–67,127
AFFIRM, 239
Aggregation, 159,321
Aho, A., 31,34,182,242
Alberti, L. B., 74
Allen, F. E., 301
Ames, S. R., 325
Amount of information (*See* Entropy)
Amplification of rights, 220–221,224
Anagramming, 60
Anderson, J. P., 203,232,318
Andrews, G. R., 302–303,307–308,314
Ardin, B. W., 180
Arrays, 298–300,326–327
ASAP file maintenance system, 192,229
Asmuth, C., 183–184,186
Assignment statement, 295,298,309–310
Astill, K. N., 180
Asymmetric cryptosystem, 10–11
Atkinson, R., 219
Attenuation of privilege, 197
Attribute (database), 213,332
Audit trail, 356,380

Authentication
 login, 7,13,161–164,166,191
 sender (*See* Digital signatures)
 server, 174
 software, 15–16,318
 tree, 170–171
Authenticity, 4–15
Authority level, 266,275
Authorization, 191,267
Authorization lists, 207,209–216
Autokey cipher, 136–137,144–145,185

Backup, 7
Baran, P., 154,206
Barker, W. G., 85
Barksdale, G. L., 232
Basic Language Machine, 216,227
Bayer, R., 3,144,173
BCC Model I, 218
Beale ciphers, 70–71,73
Beaufort, F., 76
Beaufort cipher, 76,85,127,129
Beck, L. L., 380–382,389
Bell, D. E., 265,318
Bell-LaPadula model, 265,318
Bensoussan, A., 210
Berkhoff, G., 273
Berkovits, J., 53
Berlekamp, E. R., 53
Berson, T. A., 232
Biba, K. J., 321
Bisbey, R., 231
Bishop, M., 256
Blakley, B., 107

- Blakley, G. R., 52,107,180,181,185
- Block chaining, 149,150
- Block ciphers, 135–136,138,145,147–154,161
- Bloom, J. R., 183–184,186
- Blum, M., 115,117
- Borosh, I., 107
- Boruch, R. F., 386
- Bourke, P. D., 386
- Boyer, R. S., 218,235–236,239,319
- Branstad, D. K., 98,138
- Brassard, 29,35
- Bright, H. S., 138,147
- Brillhart, J., 53,140
- Broadbridge, R., 232
- Browsing, 6,149
- Buckingham, B. R. S., 211,218
- Burke, E. L., 318
- Burroughs B5000, 217,227
- Caesar cipher, 2,23,63
- Cal system, 218
- Campasano, A. S., 165,173
- Campbell, C. M., 142
- Campbell, D. T., 390
- Capabilities, 173,207,216–228,233–236,238,248
- CAP system, 218,223
- Carlstedt, J., 231
- Cash, J., 230
- Category, 266,275
- Causey, B., 373
- Cell suppression, 342–343,359–364,369,387
- Certificates, public key, 170,179
- Chaitin, G. J., 138
- Channel capacity, 268
- Channels, types, 281
- Chansler, R. J., 218
- Characteristic formula, 334
- Chaum, D. L., 156–157
- Checksum, 147, 149–150,230
- Chehyl, M. H., 239
- Chicago Magic Number Computer, 218
- Chin, F. Y., 341,356,358,368–369,372
- Chinese Remainder Theorem, 46–48,116–117, 151,183
- Chosen-plaintext attack, 3,97,99,101,150
- Churchyard cipher, 64,126
- Cipher, 1
- Cipher block chaining (CBC), 98,101,150–151,177
- Cipher feedback mode (CFB), 136–137,145–147,150,177
- Ciphertext, 1,7
 - alphabet, 62,74
- Ciphertext-only attack, 2–3,19–20,66
- Ciphertext searching, 6,144,147–148,150,173
- Clark, D. D., 232,235
- Class, security, 232,265
- Classical cryptography, 3,11
- Clearance, security, 6,232,267,285–287
- Cleartext (plaintext), 1
- Clingen, C. T., 211
- Codd, E. F., 213,332
- Code, 2
- Codewords, 216,220,225
- Cohen, E., 218,268
- Coin flipping, 117,128,171
- Columnar transposition, 59–60
- Commands, access matrix, 194–199
 - take-grant graphs, 250
- Communications security, 3–7,138,154–157,166–169,173–179
- Compartment, 266
- Compiler certification, 291–307
- Complexity classes, 31–34
- Complexity theory, 30–34
- Compound statement, 294,298,310
- Compromise (personal disclosure), 337
- Computationally secure cipher, 3,16
- Concurrent programs, 302–305,313,327
- Confidence interval, 338–339
- Confinement, 203–204,266
- Confusion, 30
- Congruence, 36
- CoNP, 33–35
- Constraints, transition, 319–320
- Conte, S. D., 33–35
- Control flow graph, 300–301
- Conventional cryptosystem, 10,14–16,20,165
- Conway, R. W., 192,229
- Cook, S. A., 33
- Copy flag, 197
- Corwin, W. M., 218
- Counter method, 136–137,143,146
- count statistics, 334–335
- Cover, T. M., 21
- Covert channels, 281,296,305–307
- Cox, L. H., 336,361–362,364,373–374
- crt algorithm, 48
- Cryptanalysis, 2–3
- Cryptogram, 1
- Cryptographic sealing, 229–230
- Cryptographic system (cryptosystem), 7–8
- Cryptography, 1
- Cryptology, 3
- Dahl, O. J., 219
- Dalenius, T., 338,371,383,386
- Daley, R. C., 210
- Dantzig, G., 364,374
- Data Encryption Standard (DES), 2,11,14,27–31,92–101,107,127,129,135,142,146–147,150,164,177
- Data Mark Machine (DMM), 288–290,308
- Data perturbation, 159,380–383,388
- Data security, 3–7
- Data swapping, 159,383–387
- Database systems, 6–7,17
 - access controls, 149,192,194,202,205,213–216,229–231,235
 - encryption, 143–144,146–154,166,173
 - inference, 6,159,269,321,331–390
 - relational, 213–216,230,332

- Davida, G. I., 52,92,98,151,184,324,355
 Davies, D. W., 109,179
dcph (decipher), 167–169
 Deavours, C. A., 29,85
 deBoor, C., 180
 Decidability, 32,242–248,251,257,280
 Deciphering, 1,7–11
 key, 8–11
 Declaration of Independence (DOI), 71
 Decryption, 1
 De facto, de jure acquisition, 256
 DeMillo, R. A., 160,184,324,357–358
 Denning, D. E., 165,173,174,178,245,265,266,
 285,290,292,297,306,332,348,354,359,
 366,371,375
 Denning, P. J., 192–193,232,245,266,292,297,
 306,348,354
 Dennis, J. B., 217–218
 Dennis, T. D., 218,227
 Dertouzos, M. L., 157
 DES (*See* Data Encryption Standard)
 Descriptors, addressing, 217,224–225
 D'Hooge, H., 218
 Diffie, W., 11,34,83,85,97,101,137,141,143,
 176,178
 Diffusion, 30
 Digital signatures, 7,14–15,108–109,117,122–
 125,163–165,169–170,318
 Digram distributions, 20,60–61
 Dijkstra, E. W., 235
 Disclosure, 4,331,336–341
 Discretionary policy, 286
 Dobkin, D., 353–354,357–358
 Dolev, D., 187
 Domain, 192,203,206,217–219,233
 Downey, P., 318
 Downgrading, 321–324
 Downs, D., 235
 Drongowski, P. J., 232
 Durham, I., 218

 Eavesdropping, 4
ecph (encipher), 167, 169
 Edwards, D., 203
 Effects (of O-functions), 237
 Ehrsam, W. F., 166,175
 Electronic mail, 155–157,321–324
 Elementary set, 232
 Enciphering, 1,7–11
 key, 8–11
 Encryption, 1–190,205,213,229–230,240,269–
 270,321–324,376
 End-to-end encryption, 154–157
 England, D. M., 218
 Enigma, 85
 Enison, R. L., 138
 Entropy, 17–22,267,337
 Equivocation, 21–22,25,267,337
 Ernst, L. R., 373–374
 Error, transmission, 16,19,136–138,144,146–147
 Error codes, 13,53,137–138,144,149

 Euclid's algorithm, 43–44,102
 Euler's generalization of Fermat's Theorem,
 42,101
 Euler totient function, 41
 Evans, A., 161
 Even, S., 125
 Exclusive-or \oplus , 50
 Exhaustive search, 29,31,98–99,162
 Explicit flow, 270
 Exponential time, 31,34
 Exponentiation algorithm (*fastexp*), 38–39
 Exponentiation ciphers, 101–115,135

 Fabry, R. S., 218,225,228
 Factoring, 13,34,105–107,117
 Fagin, R., 216
 Farber, D. A., 207,239
fastexp algorithm, 39,101
 Feiertag, R. J., 218,235–236,318–319
 Feige, E. L., 371
 Feistel, H., 90,92,138,149,155,162,165
 Fellegi, I. P., 337,356,373
 Fenton, J. S., 266,282–283,285,288,308
 Fermat's Theorem, 42,101
 File systems, access controls, 191–193,196–200,
 203–205,210–213,226,248–249,251
 encryption, 143–144,146,150–151,166–
 168,172–173,213
 Finite field (*See* Galois field)
 Flow (*See* information flow)
 Floyd, R. W., 238
 Flynn, R., 165,173
 Formulary model, 194
 Frank, O., 340
 Frequency distributions, 20,29,60–61,65–70,
 73,77–84
 digram, 20,60–61,84
 single letter, 20,65–69,73,77–84
 trigram, 20,60,67,84
 Friedman, A. D., 364–365
 Friedman, W. F., 65,77,83–84
 Furtek, F., 268,319,327

 Gaines, H. F., 60,79
 Gaines, R. S., 266
 Gait, J., 142
 Galois field (GF), 48–53
 GF(p), 49–52,103,181–182
 GF(2^n), 49–53,104,178,181–182,186
 Gardner, M., 101
 Garey, M. R., 31,34
 Garland, S. J., 245
 Gasser, M., 239
 Gat, I., 285
gcd (greatest common divisor), 43–44
 Gehringer, E., 227
 Gifford, D. K., 229
 Gifkins, M. R., 218
 Gillogly, J. J., 71
 Global flows, 303–304,313
 Gold, B. D., 232

- Golumb, S. W., 140
 Gorn, S., 24–25
 GPLAN database system, 230
 Graham, G. S., 192–193, 232, 266
 Graham, R. L., 121
 Graham, R. M., 207
 Graham-Shamir knapsacks, 121–122
 Greatest lower bound \otimes , 273, 278
 Gries, D., 314
 Griffiths, P. P., 213, 215–216
 Guard, ACCAT, 321–324
 Gudes, E., 166, 229
 Guttag, J. V., 314

 Hagelin, B., 85
 Hagelin machines, 84–86, 136
 Halting problem, 32, 232, 242–244, 247
 Hammett, C., 71–73
 Hamming, R. W., 53
 Hansen, M. H., 343
 Haq, M. I., 337, 345, 373
 Harrison, M. A., 192, 195, 196, 240–242, 245, 257
 Hartson, H. R., 194
 Haseman, W. D., 230
 HDM (Hierarchical Design Methodology), 236–239, 319
 Heberd, B., 231
 Hellman, M. E., 11, 26, 34, 83, 85, 97–101, 103–104, 107, 118–120, 137, 141, 143, 176, 178
 Henry, P. S., 121
 Hierarchical systems design, 235–239
 High water mark, 287
 Hill, L. S., 88
 Hill cipher, 85–89, 127, 135
 Hoare, C. A. R., 219, 307
 Hoffman, L. J., 194, 344, 358, 364–365, 380
 Homomorphism, 36–37, 157–160
 Homophonic substitution, 62, 67–73, 127, 135
 Hopcroft, J., 31, 34, 182, 242
 Horning, J. J., 209, 314
 Hsiao, D. K., 194
 Hubka, D. E., 218
 Huff, G. A., 239
 Huffman, D., 18
 Huffman codes, 18, 30
 Hutchins, L. A., 218
 HYDRA system, 218, 220, 224

 IBM, 90, 92, 150, 213, 229
 if statement, 295, 298, 311–312
 Iliffe, J. K., 216, 220, 227
 Implicit flow, 270
 Implied queries, 364–368
 Index of Coincidence (IC), 77–79, 81–82
 Inference controls, 6–7, 159, 269, 321, 331–390
 Information flow
 controls, 6–7, 202–205, 256–257, 265–327
 logic, 307–317
 meaning of, 267–273
 Information theory, 16–30, 159, 265, 267–268, 337
 INGRES database system, 230

 Initialization block, 138, 141, 146, 150, 177
 Integrity, 4, 321
 Intel iAPX 432, 218, 223
 Intractable, 32
inv algorithm (compute inverses), 44
 Inverses, computing, 39–44
 IPS (Information Protection System), 150–151, 164–165
 Irreducible polynomial, 49, 140, 181
 ISI (Information Sciences Institute), 231, 239

 Jacobi symbol, 106, 114–115
 Jefferson, D., 218
 Jodeit, J. G., 216
 Johnson, D. S., 31, 34
 Jones, A. K., 218, 223, 248, 251–252, 256–257, 280, 353–354

 Kahn, D., 66, 70, 74, 76–77, 79, 83, 85–87, 101, 144
 Kahn, K. C., 218
 Kam, J. B., 92, 151, 355
 Kampe, M., 218, 232
 Kanodia, R. K., 304
 Kantrowitz, W., 161
 Karger, P. A., 275
 Karp, R. M., 118, 122
 Karpinski, R. H., 389
 Kasiski, F. W., 79
 Kasiski method, 79–83
 Keeton-Williams, J. G., 324
 Kemmerer, R. A., 239
 Kent, S. T., 138, 149, 161, 179
 Kernel (*See* Security kernel)
 Key, encryption/decryption, 1, 7–11
 database, file, 151–154, 166–168, 172–173
 distribution of, 173–179
 generating, 171–173
 group, 173
 hardware, 162, 165, 173
 management, 164–185
 master, 166–169, 171, 175–176, 179
 private, 1, 11, 164–169, 173–176
 public, 11, 169–171, 177–179
 read/write, 11, 151–154, 166, 213
 secondary, 167, 172, 176
 signature, 11, 165
 stream, 24–25, 83, 85–87, 135–147
 subkeys, 151–154, 185
 terminal, 166–169, 176
 threshold schemes, 179–186, 206, 229
 Key-specified query, 353
 Keys record, 166, 213, 229
 King, R. C., 21
 Kline, C. S., 15, 138, 165, 179, 206, 218, 232
 Knapsack problem, ciphers, 13, 33–34, 117–126, 135
 simple knapsacks, 118
 trapdoor knapsacks, 119
 Known-plaintext attack, 3, 29, 98, 103, 141, 185, 186
 Knuth, D., 43, 104, 138, 182

- Kohnfelder, L. M., 109,170
 Konheim, A. G., 29,85,150
 Kowalchuk, J., 53,177
 Kreissig, G., 200
 Kruh, L., 64
 KSOS (Kernelized Secure Operating System), 232–236,240,319,323
 Kurzban, S., 380
 KVM/370 (Kernelized VM/370), 232

 Lagrange polynomials, 180–182,186
 Lampson, B. W., 192,203,209,218,281,285,314
 LaPadula, L. J., 265,318
 Lattice model, 265–278
 definition of lattice, 273
 input/output lattice, 275
 subset lattice, 274–275
 Leakage of information, 6,265
 of rights, 240–248
 Least privilege, 203,206–207,219,286
 Least upper bound \oplus , 273,277–278
 Legendre symbol, 114
 Lempel, A., 35,121,125
 LeVeque, W. J., 36,106,112
 Levin, G., 314
 Levin, R., 218
 Levitt, K. N., 218,235–236,238–239,318–319
 Linde, R. R., 203,231,232
 Linden, T. A., 219
 Linear Feedback Shift Registers, 136–137,139–142,185
 Link encryption, 154–157
 Linton, D. J., 355
 Lipner, S. B., 281
 Lipton, R. J., 111,115,160,184,248,251–252, 256,280,324,353–354
 Lipton, S. M., 165,357
 Liskov, B. H., 219,223
 Liu, L., 354
 Locks and keys, 228–230
 Logarithm, computing, 103–106,173,176
 Login protocols, 161–164
 London, R. L., 209,219,314
 LUCIFER, 90,92

 Mack, M. H., 150
 Macrostatistics, 341–343,360
 MacWilliams, F. J., 53
 Masquerading, 7
 Matyas, S. M., 98,165,166,171,175
 Mauborgne, J., 86
 Maximum order control, 359–360
 Maxwell, W. L., 192,229
 McCauley, E. J., 232
 McEliece, R., 13,53
 McNeil, L., 160
 McNeill, R. K., 150
 Meaningful/meaningless messages, 26
 Mechanism, protection, 191,200–207,279–281, 340–341
 median statistics, 336,356–357

 Meijer, H., 173
 Mekota, J., 232
 Mellen, G. E., 60
 Memoryless programs, 203–204
 Mental poker, 110–115,128
 Merkle, R. C., 14–15,97–98,118–120,165,170, 176,178
 Merkle-Hellman knapsacks, 118–122,128
 Metzger, J., 3,144,173
 Meyer, C. H., 98,141,166,171,175
 Microaggregation, 371
 Microstatistics, 341–343,384
 Millen, J. K., 232,239,268,318–319,327
 Miller, W. F., 344,380
 Minsky, M., 31,242,288
 Minsky, N., 224
 Minsky machine, 288
 Mitchell, J. G., 209,314
 MITRE, 177–178,232,318–320
 Modular arithmetic, 35–53
 Module (*See* Abstract data types)
 Moments, finite, 335,371
 Morgan, H. L., 192,229
 Monitors, protection, 193,232,234
 Montague, J. T., 218
 Moore, J. S., 239,319
 Morris, J. B., 219
 Morris, J. H., 223
 Morris, R., 97,162
 MULTICS, 207,210–211,227,232
 Multilevel security, 232,235,266,275–276,286–287,318–324
 Multiple encryption with DES, 98
 Mutual suspicion, 204–205
 Myers, G., 218,225,227

 Nargundkar, M. S., 373
 Needham, R. M., 15,161,170,174–175,218
 Need-to-know, 286
 Networks, 4,15,154–157,173–176,179,205, 239,240
 Neumann, P. G., 210,218,232,235–236,239
 Niven, I., 36,106,112
 Noise (*See* Perturbation)
 Nondiscretionary policy, 286
 Norris, J., 106
 Notz, W. A., 92,138,155,162,165
 NP, NP-complete, NP-hard, 33–35
 n -respondent, k %-dominance rule, 336,360

 Object-oriented languages, 219
 Objects (of access matrix), 192
 Oblivious transfer, 115–117
 O -function, 237
 Olsson, L., 369
 One-key cryptosystem, 10
 One-time pad, 25,86–87,136,141,185
 One-way cipher, 161–162
 One-way function, 341,161,166

- Operating systems, access controls, 192–193, 196–208, 216–229, 249–250, 285–288
 - authentication, 15, 318
 - flow controls, 285–288, 318–324
 - verification, 231–240, 288, 318–324
- Order of statistic, 336
- Organick, E. I., 207, 210
- Output-block feedback mode (OFB), 136–137, 142–143
- Overlap control, 354–357, 387
- OV*-function, 237
- Ownership, 191, 196–198, 200, 202–205, 210–213
- Ozsoyoglu, G., 341, 356, 358, 368–369
- P** (polynomial time), 32–34
- Palme, J., 346, 373
- Parnas, D. L., 236
- Partitioning, 368–371, 387
- Passwords, 7, 161–164
- Peeler, R. J., 232
- Peleg, S., 67
- Penetration analysis, 231–232
- Percentile complexity, 35
- Perfect secrecy, 16, 22–25, 339
- Periodic ciphers, 60–62, 74–82, 84–85, 136–137
- Permutation cipher (*See* Transposition cipher)
- Perturbation, 341, 343, 360, 371–388
- Peterson, W. W., 53, 140
- Phillips, J. L., 373
- Pierson, C., 218
- Plaintext, 1, 7
 - alphabet, 62, 74
- Playfair, L., 87
- Playfair cipher, 87–88, 127, 135
- Pohlig, S., 97, 101, 103–104, 107, 120
- Pohlig-Hellman scheme, 101–104, 112, 127–128, 178
- Policy, protection, 191, 199–201, 233–234, 265–267, 279, 336, 340
- Pollack, F. J., 218
- Polyalphabetic substitution, 62, 73–87
- Polygram substitution, 62, 87–89
- Polynomial interpolation, 180–182, 184, 186
- Popek, G. J., 15, 138, 165, 179, 206, 207, 209, 218, 231, 232, 235, 239, 314, 318
- Powers, S. A., 177
- Pratt, F., 70
- Precise, 200–201, 279–280, 340–341
- Price, W. L., 109, 179
- Price, W. R., 236
- Prime numbers, 34, 42, 48
 - generating, testing, 106–107
- Privacy, 4
- Privacy homomorphism, 157–160, 185
- Privacy transformation, 159, 343
- Privileged modes, 15, 207–208, 233–235
- Procedure call, 218–224, 296, 298, 313–316
- Product ciphers, 90–98
- Program counter class, 288, 308
- Programming languages, 21, 193, 208–209, 219–224
- Program proving, 238, 291–317
- Proof rules, 307–316
- Proprietary software, 6, 159–161, 203–205
- Protected entry point, 218–219
- PSOS (Provably Secure Operating System), 218, 235–240, 319
- PSPACE**, 34
- Public-key cryptosystems, 8, 11–15, 19–20, 29–30, 34, 101–109, 117–125, 156–157, 163–165, 187, 230
- Public-key distribution system, 176–179
- Purdy, G. P., 161
- Quadratic residue, 111–117
- Query, 335–336, 353
 - modification, 230–231
 - processing systems, 230–231, 343
 - set, 334
 - set-overlap control, 354–357, 387
 - set-size control, 345–352, 364, 376, 387–388
- Rabin, M. O., 15, 107, 115, 117, 128
- Rail-fence cipher, 1
- Random cipher model, 25–29
- Randomized response, 386–387, 389
- Random sample queries, 374–380, 388
- Rate of language, 20–21, 26–27
- Redell, D. R., 228
- Redundancy, 20–21, 27–30, 83, 138
- Reed, D. P., 304
- Reed, I. S., 159
- Reference monitor, 232, 234
- Reiss, S. B., 358, 383, 385
- Reitman, R. P., 302–303, 307–308, 314
- Relatively prime, 40
- Reliability, 7, 201, 204–205, 219
- Replay, 4–6, 144, 148–150, 173
- Residue, 36
 - reduced set, 41
- Revocation, 197–198, 213–216, 227–228, 233, 258
- rfmk* (reencipher from master key), 167–169, 171, 175–176
- Rice University Computer, 216, 227
- Rights (of access matrix), 192
- Rings (protection), 207–208
- Ritchie, D. M., 212
- Rivest, R. L., 13, 85, 100–101, 104–108, 110, 157, 170
- Robinson, L., 218, 235–236, 238–239, 318–319
- Rogers, H., 247
- Rosenfeld, A., 67
- Rotenberg, L. J., 287
- Rotor machines, 84–85, 90, 136
- Rounding, 159, 343, 372–374, 389
- RSA scheme, 13, 34, 101–109, 115, 120, 122, 127–129, 186
- rtmk* (reencipher to master key), 168–169, 172, 176
- Running key cipher, 83–84, 87, 136
- Rushby, J. M., 206, 239, 320
- Ruzzo, W. L., 192, 195, 196, 240–242, 245, 257

- Saal, H. J., 285
 Sacco, G. M., 174,178
 Safe prime, 103,107
 Safety, 240–257
 Salt, with passwords, 162
 Saltzer, J. H., 165,206,207,232,235
 Sam, E., 64
 Sampling, 343,374–380
 Sande, G., 364
 Sanitization, 321
 Savage, J. E., 144
 Saveland, W., 373
 S-box, 93–98
 Schaefer, M., 232
 Schaffert, C., 219
 Schanning, B., 53,177
 Scheid, J. F., 232
 Schell, R., 232,318
 Scherbius, A., 85
 Schiller, W. L., 232
 Schlörer, J., 332,346,348,350–351,359–360,373, 379,383–384
 Schneider, F. B., 173
 Schroeder, M., 15,170,174–175,206,207,232,235
 Schroepel, R., 97,105
 Schwans, K., 218
 Schwartz, M. D., 348,354,374
 Schwartz, R. D., 386
 Schweitzer, P., 97
 SCOMP, 232,319
 SDC (Systems Development Corporation), 231, 232,239,287,319
 Sealing, 223,229–230
 Secrecy, 4,6,8–13,16–17
 Secure, 200–201,279–281,293,316,340–341
 Security
 data, 3–7
 class (level), 232,265
 variable class, 267,278,284–285,287,307
 clearance, 6,232,267,285–287
 kernel, 232–236,239,287,292,318–320,324
 Sederberg, T., 18
 Selective confinement, 204,266
 Self-synchronous stream ciphers, 136–138, 144–147
 Sensitive statistic, 336
 Session keys, distribution, 173–179
 Sestri, I. G., 76
 Sevcik, K. C., 218
 Shadows, 180
 Shamir, A., 13,15,35,101,104–108,110,117,120–122,128,170,180,182,184,186
 Shannon, C. E., 16–30,90,268
 Sharing, 201–205
 Shaw, M., 219
 Shifted substitution, 2,23,28–29,63,66,74,83,145
 Signature (*See* Digital signatures)
 Signature-only knapsacks, 122–125,128–129
 Silverberg, B., 239
 Simmons, G., 10,13,17,106
 Simple security condition, 318
 Simple substitution, 62–66,73,135
 Single Accumulator Machine, 290–291
 Sinkov, A., 60,63,66,77
 Size control, 345–352,364,376,387,388
 Sloane, N. J. A., 53,97
 Smid, M., 15
 Smith, D. C. P., 369
 Smith, J. L., 92,138,155,162,165
 Smith, J. M., 369
smk (set master key), 167,171
 Smullyan, R., 83
snap algorithm, 118
 Snyder, A., 219
 Snyder, L., 248,251–252,256–257
 Software protection, 6,15–16,159–161,203–205
 Solovay, R., 106
 SPECIAL language, 236–239,319
 Specifications, 236–239,292–293,318–320
 Sphere of protection (domain), 217–218
 SRI, 235–239,318–319
 Stahl, F. A., 70
 StarOS for CM*, 218
 Star property, 318
 Statistical database, 159,269,321,331–390
 Steinberg, J., 386
 Stonebraker, M., 230
 Stoughton, A., 218,232
 Strassen, V., 106
 Stream ciphers, 135–148
 Strong cipher, 3
 Sturgis, H. E., 218
 Subadditive/superadditive, 362
 Subjects (of access matrix), 192
 Subkeys, 151–154,185
 Substitution ciphers, 2,62–89
 Substitution-permutation ciphers, 90–92
 SUE system, 218
 Sugarman, R., 98
sum statistics, 334–335
 Supervisor states, 207–208,233–234
 Suspicion, 201–205
 Swanson, L., 185
 SWARD, 211–212,218,219,225,227,228
 Symmetric cryptosystems, 10
 Synchronization channels, 302–305,313
 Synchronous stream ciphers, 136–144,185
 System R, 213–216,257–258
 Szeleg, C. R., 355
 Table lookup, 99
 Tagged memory, 223,226–227,288–291
 Take-grant model, 241,248–258
 Tampering, 4–7
 TENEX system, 207
 Theories of protection, formal, 240–257
 THE system, 235
 Thompson, K., 162,212
 Threat monitoring, 380
 Threshold schemes, 179–186,206,229
 Tickets, 207,224
 Time-memory tradeoff, 97–101,120

- Timestamps, 163–165, 170, 175, 178–179
- Timing channel, 281, 296
- Trackers, 346–353, 356, 364, 377, 380, 388
- Tractable, 32
- Traffic flow analysis, 4, 155
- Tranquility principle, 318
- Transposition ciphers, 1–2, 59–62, 135
- Trapdoor one-way function, 34
- Trigram distributions, 20, 60, 67, 84
- Trojan Horse, 203, 206, 207, 288, 318
- Trusted processes, 234–235, 239, 281, 321, 324
- Tsichritzis, D. C., 218
- Tuchman, W. L., 98, 141, 166, 175
- Tuckerman, B., 150
- Turing, A., 32
- Turing machine, 31–32, 242–245, 247, 258
- Turn, R., 21, 159
- Two-key cryptosystem, 10–11
(*See also* Public-key cryptosystems)
- UCLA Secure UNIX, 218, 232–234, 239, 240
- Ullman, J. D., 31, 34, 182, 192, 195, 196, 240–242, 245, 257, 355
- Uncertainty (entropy), 16–22, 25, 157, 267–268, 338
- Unconditionally secure cipher, 3, 16, 25
- Undecidability, 32, 242–248, 257, 280
- Unicity distance, 25–29, 31, 61–62, 64–65, 76–77
- Urban, M., 218, 232
- UNIX, 18, 162, 207, 212, 218, 232–235, 239, 319, 323
- VanHorn, E. C., 217–218
- Vegdahl, S. R., 218
- Verification, 15, 231–240, 291–320, 324
- Vernam, G., 86
- Vernam cipher, 86–87, 136, 138, 269
- V-function, 237
- Vigenère, B. de, 74, 144–145, 185
- Vigenère cipher, 74–76, 83, 101, 126, 129, 136
- Vigenère Tableau, 75–76
- Vinogradov, I. M., 36, 106, 112
- Virtual machines, 206, 240
- Wade, B. W., 213, 215–216
- Waldbaum, G., 150
- Walker, B. J., 239
- Walker, R. D. H., 218
- Walter, K. J., 232
- Walton, E., 218, 232
- Ward, J. B., 70
- Ward, P. D., 232
- Warner, S. L., 386
- Washington, L., 97
- Watts, H. W., 371
- Wehrle, E., 332, 359
- Weiss, E., 161
- Weissman, C., 266, 287
- Weldon, E. J., 53, 140
- Wells, D. L., 151, 355
- Wheatstone, C., 87
- while** statement, 295, 298, 312–313
- Whinston, A. B., 230
- Wilkes, M. V., 161
- Williams, H. C., 107
- Wiretapping, 4–5, 137, 149, 187
- Wong, E., 230
- Woodward, J. P. L., 321
- Wulf, W. A., 218, 219
- Wyner, A., 97
- Yacobi, Y., 125
- Yao, A. C., 187
- Yu, C. T., 368
- Zierler, N., 53, 140
- Zippel, R. E., 120–122
- Zuckerman, H. S., 36, 106, 112