Subject Index

A
Abelian groups, 458–460, 465
Absorption, set theoretic identities, 495
Active attacks; See also specific attacks
  basic concepts, 12
  on OFB mode, 285
Addition
  AES
    algorithm operations, 433
    computer program for, 449
    encryption, 423
    Galois fields, 413, 423
    nibble, 419, 445–446
    algorithm complexity analysis, assessing work required to execute, 246, 247
    elliptic curve, 454–458
    algebraic algorithm, 455–458
    computer implementations and exercises, 483–484, 485
    curves over \( \mathbb{Z}_p \), 463–466
    geometric algorithm, 455, 456
  finite fields, 383, 384
  Galois fields, 398, 413, 423
  rings, 378–379, 381, 410
  matrix, 146–147, 149, 150, 175
  modular integer systems, 59
  polynomial; See Polynomials, addition
  vector, 457
Addition algorithm with base \( b \)
  expansions, 229–231
Additive groups, 459
Additive identity, 378, 383, 410
elliptic curve addition, 458
modular arithmetic, 59
Additive inverses, 379
Add Round Key operation, AES
  computer program for, 447
  decryption, 431
  encryption, 422, 424, 429, 437
  exercises, 444–445
  full (128 bit) AES, 438
ADFGVX cipher, 32–35, 102
Adjacent digits, 78, 80
Adjacent letters, 182, 183, 215
Adjacent pairs, 34, 571
Adleman, Leonard, 22, 331, 338, 339
Advanced encryption standard (AES)
  protocol, 21, 417–449
  byte representation and arithmetic, 432–434
  computer implementations and exercises, 445–449
  decryption algorithm, 439–440
  development of, 254, 417–419
  encryption algorithm, 437–438
  exercises, 441–445
  exercise solutions, 560–563, 609–611
  full (128 bit key) AES, 432
  437–438
  Galois fields, 399, 400
  nibbles, 419–421
  scaled-down version, 421–429
    computer programs for, 446–449
    decryption, 429–432
    encryption, 421–429
    encryption algorithm, 435–437
    438
security of, 440
Affine ciphers
  computer programs for, 136, 137–140
  with homophones, 138–139
  with homophones and nulls, 139–140
  with nulls, 137–138
  evolution of codemaking, 96–100
  passive attacks on, 98–100
Affine function/mapping, 96
  AES, 444
  composition, 109–110
  digraph block cryptosystems, 132–133
  homophones, 105–106
  nulls, 103–104
Agrawal, Manindra, 309
AKS test, 309
Algorithm complexity analysis, assessing work required to execute, 246–247
Algorithms, defined, 3–4
Alice (literature convention), 2, 22, 23, 339, 340
Alphabets
basic concepts, 3
cryptosystem components, 94
English, 13–14, 95
monoalphabetic and polyalphabetic
ciphers, 12–15
number of characters, 95
plaintext conversion to numerical
equivalents, 225–228
American Standard Code for
Information Interchange
(ASCII), 227, 254, 340
Ancient codes, 91–94
Arab culture, cryptography in, 102
Arithmetic
algorithm complexity analysis,
assessing work required to
execute, 246–247
elliptic curve, 451
integers in different bases
addition algorithm with base \( b \)
expansions, 229–231
computer implementations and
exercises, 248–250
exercises, 241–247
exercise solutions, 536–540
large integers, 237–239
multiplication algorithm
with base \( b \) expansions,
234–237
subtraction algorithm with base
\( b \) expansions, 231–234
matrix, 175
addition, subtraction, and scalar
multiplication, 146–147
multiplication, 147–151;
See also Matrix
multiplication
properties of, 149–150
modular integer systems, 59; See
also Divisibility and modular
arithmetic
nibble
addition and multiplication,
419–420
computer implementations and
exercises, 445–446
ASCII, 227, 254, 340
Assissi, Benicio de, 102
Associativity
abelian group, 459
addition, 378, 383, 459
elliptic curve, 458, 483
matrix arithmetic, 149, 150
multiplication, 379, 383
rings, 379
set theoretic identities, 495
Asymmetric key cryptography,
21–22; See also Public key
cryptography
Attacks on cryptosystems, 2; See also
specific attacks
affine ciphers, 98–100
evolution of codebreaking; See
Evolution of codebreaking
till computer era
overview, 12–15
Authentication
basic concepts, 1
features of public key
cryptosystems, 25
public key cryptography, 343–345
digital signatures, 343–345
ElGamal cryptosystem,
347–349, 373
RSA digital signatures, 371
Avalanche condition, strong, 419
Avalanche effect, 272, 290–291

B
Babbage, Charles, 187, 207
Babbage/Kasiski attack, 108
computer programs to aid in,
216–218
Vigenère cipher demise, 188–192
Bases; See also Integers in different
bases
elliptic curve discrete logarithm
problem, 466
Bayes’ formula, 510–511
Belaso, Giovanni Battista, 15
Ben-Or’s irreducibility determination
algorithm, 410–411, 414–415
Biased, probabilities, 502
Big-O notation, 247
Bijections
finite fields, 382
overview, 5–7
Binary alphabet, basic concepts, 3
Binary expansions
AES algorithm operations, 434
integers in different bases, 221,
224–227
addition algorithm with base \( b \)
expansions, 231–234
multiplication algorithm in base
\( b \) expansions, 234–237
Binary operations
abelian group, 458–460
algorithm complexity analysis,
assessing work required to
execute, 246–247
elliptic curve, 483
finite fields, 377–378
rings, 378–379, 381, 406–407
Binary strings
basic concepts, 3
plaintext conversion to numerical
equivalents, 225–228
Binary vectors
  knapsack problem reformulation, 350
  nibble addition and multiplication, 419
  rings, 406–407
Binomial random variables, 511–513
Birthday problem, 505–507
Bit operations, work required to execute
  algorithm complexity analysis, 246–247
Bits, word size, 238
Bit strings, 238
  conversion programs, 286
  nibble addition, 420
  plaintext conversion to numerical equivalents, 225–228
Bitwise representation, AES algorithm, 432, 433
Bletchley Park, 22, 202, 206–208, 252
Block ciphers, 20, 26
  evolution of codebreaking, 190
  Hill cryptosystem, 162–166; See also Hill cryptosystem
  Playfair cipher as, 18
Block cryptosystems, 132–133, 251–292
  computer implementations and exercises, 286–292
  DES, 265–272
    adoption of, 252–254
    fall of, 272–273
    scaled-down version, 258–265
    triple, 273–274
    evolution of computers into cryptosystems, 251–252
    exercises, 279–286
    public key cryptography, 367–368
    solutions, 540–545, 599–601
  Feistel cryptosystems, 255–258
    modes of operation for, 274–279
    block mode, 274–276
    cipherblock chaining (CBC) mode, 275–276
    cipher feedback (CFB) mode, 276–278
    electronic codebook (ECB) mode, 274–275
    output feedback (OFB) mode, 278–279
  XOR operation, 254–255
  Block matrix multiplication, 172–174
  Block mode operations, block cryptosystem, 274–276
  Block size
    AES
      versus Rijndael, 419
      scaled-down versus 128-bit key, 421
    DES, scaled-down, 258
    Feistel cryptosystems, 255
Bob (literature convention), 2, 22, 339, 340
Broadcast attack, RSA cryptosystem, 366
Brute-force approach
  DES attacks, 273
  elliptic curve discrete logarithm problem, 467
  irreducibility test for polynomials in $\mathbb{Z}_p[X]$, 394, 395
  knapsack problem, 374
  modular inverses, 87
  passive attacks on substitution cipher, 13
  points on modular elliptic curve, 452–456, 462
Byte, definition of, 276
Byte arithmetic/operations, AES, 432–434
  AES algorithm operations, 432, 433
  computer program for, 449
  exercises, 443
  nibble-byte subtransformations, 444–445
  sub transformation, encryption algorithm, 424, 436, 437, 439
C
  Caesar cipher, 9–11, 94
    evolution of codemaking, 101
    shift ciphers, 95
  Cardinality, 495, 496
  Carmichael, Robert, 311
  Carmichael numbers, 311–312
  Carries
    addition algorithm with base $b$ expansions, 229, 230
    multiplication algorithm with base $b$ expansion, 234, 235, 236, 238
  Cartesian product set, 496
  Cauchy, Augustus, 382
  CBC (cipher block chaining) mode, 275–276
  Ceiling function, definition of, 48
  Certification, primes, 309
  CFB (cipher feedback) mode, 276–278
  Chain matrix multiplication, 167–168
  Champollion, Jean-Francois, 92
  Change of base formula, 224
  Chiffre indechiffreable, le, 15, 108
  Chinese remainder theorem, 67–71, 359
    computer implementations and exercises, 89
    elliptic curve-based factoring algorithm, 476
    RSA cryptosystem, 341
Subject Index

Chor-Rivest cryptosystem, 356
Chosen ciphertext attacks, 12, 32
    affine ciphers, 99–100
    exercises, 133
    Hill cryptosystem, 164, 170
    RSA cryptosystem, 366
Chosen plaintext attacks, 12, 13, 99
    differential cryptanalysis, 272
    Hill cryptosystem, 164
    linear cryptanalysis, 273
Church, Alonzo, 207
Cipherblock chaining (CBC) mode,
    block cryptosystems, 275–276
Cipher feedback (CFB) mode, block
    cryptosystems, 276–278
Ciphergram, computer program
    for extracting data from ciphertext string, 216–218
Ciphers
    ADFGVX, 32–35
    versus code, 91
    Playfair, 18–25
    programming with integer arithmetic, 38–39
    standards, 2
    substitution, 8–11
    terminology, 94
    Vignière, 15–18
Ciphertext
    basic concepts, 2
    partial substitutions, program for, 215
    substitution ciphers, 8–11
Ciphertext attacks
    affine ciphers, 99–100
    chosen; See Chosen ciphertext attacks
    types of, 12
Ciphertext-only attacks, 12, 13
    affine ciphers, 98, 136
    frequency analysis-based, 186
    homophonic cryptosystems and, 106–107
    on shift cipher, 38
    Vigenère cipher, 200–201
Classical adjoint formula for matrix inversions, 159–162,
    171–172, 176
Clay foundation, 24
Closure, ring, 380
Cocks, Clifford, 22, 23
Code, versus cipher, 91
Codebreaking; See Decryption;
    Evolution of codebreaking till computer era
Codemaking; See Encryption;
    Evolution of codemaking till computer era
Coding theory
    congruency applications, 77–79
    Shannon’s contributions to, 25
Codomain, basic concepts, 4, 5
Coefficient formula, polynomials, 387
Coefficients, 385, 390
Cofactor expansion algorithm, 153–154,
    157, 160, 171–172, 529
    classical adjoint formula with, 159
    computer platform caveat, 161
    computer programs, 176
Cogitata Physica- Mathematica
    (Mersenne), 81
Cohen, Henri, 314
Coincidence, index of, 193–201
Column index, AES encryption algorithm, 437–438
Column matrix, 146
Combinatorics, 495
Common modulus attack, RSA cryptosystem, 365
Commutation, composition of functions
    and, 110
Commutative rings, 58
Commutativity
    addition, 378, 458
    elliptic curve
        abelian group, 458–460
        addition, 458
        exercises, 483
    matrix arithmetic, 148–149, 150
    ring multiplication, 379
    set theoretic identities, 495
Complementarity probability rule, 504
Complementary keys, DES, 284
Complementary plaintext, DES, 284
Complement bit strings, exercise, 279–280
Complements, set, 494, 495, 499
Complexity analysis of algorithms,
    assessing work required to execute, 246–247
Complexity of polynomials, RSA
    security guarantees, 357
Complex roots, elliptic curves over real numbers, 453
Composite integers, defined, 44
Compositeness
    Carmichael numbers, 311–312
    Miller–Rabin test, 314
    witness to, 309–310
Composite numbers, Lenstra’s algorithm application, 482
Composition of functions, 332–333
    dissection of Enigma machine into permutations, 119–120
    evolution of codemaking, 109–110
    inverse of, 429
    permutations, computer program for, 141
repeated, 117
scaled-down Enigma machine, 120–121
triple, 122
Computational number theory, 309
Computation issues
algorithm complexity analysis, assessing work required to execute, 246–247
floating point platform limitations, 85, 87, 161, 237, 240, 296, 314, 317–318, 325, 369, 483
elliptic curve operations, 483
Lenstra’s algorithm, 477
RSA cryptosystem, 341
Moore’s law, 440
public key cryptography, 334
vector representation of polynomials, 387–388
Computation of orders, 303
Computer-generated random numbers, 40, 41
Computer implementations and exercises
AES, 445–449
block cryptosystems, 286–292
codebreaking evolution, 214–220
Babbage/Kasiski attack, programs to aid in, 216–218
frequency analysis, programs to aid in, 214–215
Friedman attack, programs related to, 218–220
index of coincidence, 218
codemaking evolution, 136–143
cofactor expansion method, 89, 161, 176
DES, 287–292
division algorithm, 86
elliptic curve cryptography, 483–487
modular elliptic curves, 484, 485
nonsingular elliptic curve, 483–484, 485
fast modular exponentiation, 240
Feistel cryptosystems, 287
finite fields, 411–415
Hill cryptosystem, 177–178
integers in different bases, 224, 248–250
matrices and Hill cryptosystem, 174–179
fast matrix multiplication, 179
modular matrices, 175–177, 178–179
scalar multiplication, 175
square (invertible) matrix, 175–176
Strassen’s algorithm, 179
modular arithmetic, 85–89
Chinese remainder theorem, 89
congruences, 88
Euclidean algorithm, 86–88
prime factorization, 85–86
number theory and algorithms, 325–329
overview, 35–41
computer-generated random numbers, 39–41
integer/text conversions, 36–37
programming basic ciphers with integer arithmetic, 38–39
vector/string conversions, 35–36
public key cryptography, 369–375
random substitution ciphers, 220
readings in, 616
three-round Feistel systems, 287
XOR program, 287
Concatenation, 7
Conditional probability, 507–509
Conditioning, 195, 509–511
Confederate cipher disk, 11
Confusion
one-time pad, 25–26
Shannon’s properties of, 272, 419
Congruence classes, 54–55
Congruences
addition of elliptic curves over $\mathbb{Z}_p$, 464
basic properties, 54
Chinese remainder theorem, 67–71
computer implementations and exercises, 88
congruent mod $m$, 53
divisibility and modular arithmetic, 52–58
exercises
credit card error detecting codes, 79–80
divisibility criteria, 82–83
ISBN error detecting codes, 77–79
round robin tournaments, 80
modular elliptic curves, 461–462
solving, 61, 64–66
validity of congruent substitutions in modular arithmetic, 56–57
in $\mathbb{Z}_p[X]$ modulo, 395–396
Conjugates, of permutation, 123
Constant polynomial, 385
Continuous infinite sets, 4
Contrapositive, Fermat’s little theorem, 309
Convergence, Gauss’s primitive root finding algorithm, 325
Conversions
integer/text, 36–37
vector/string and string/vector, 35–36, 286
Coppersmith, Don, 150, 272
Correspondence, English alphabet, 95
Counter mode of operation, block cryptosystems, 285–286
Counting principles, 495–499
Credit card error-detecting codes, 79–80, 89
Cryptanalysis
basic concepts, 3
linear and differential, 272–273
Cryptography, 1–2
Cryptosystems
basic concepts, 1–2
block; See Block cryptosystems formal definition, 94–96
Cycle decomposition form invariance, 205–206
Cyclic permutations/cycles, evolution of codemaking, 114–119

D
Daemen, Joan, 418
Data encryption standard (DES), 20–21, 265–272
adoption of, 252–254
AES development, 417–419
computer programs, 287–292
exercises, 282–283
fall of, 272–273
public key cryptography, 333
scaled-down version, 258–265
self-decryption proof, 285
triple, 273–274
Decimal expansion, integers in different bases, 222
Decomposition, disjoint cycle, 115–116, 117, 124
Decryption; See also specific systems
basic concepts, 2–3
codebreaking; See Evolution of codebreaking till computer era
Playfair and Vignère ciphers, 39
Decryption algorithm
AES, 439–440
self-decryption proof, three-round Feistel systems, 285
Decryption exponent, 551, 552, 605, 606
ElGamal cryptosystem, 345–346, 347
RSA cryptosystem
computer programs for, 370, 371, 372
probabilistic factoring algorithms for RSA modulus, 358
public key, 340–341, 342
security guarantee, 357
Decryption functions
cryptosystem components, 94
substitution ciphers, English alphabet, 96
Definitions of basic concepts, 1–4
De Morgan’s Laws, 495
Density, primes, 308
Dependent events, 508
DES; See Data encryption standard
DES algorithm, 262, 264, 265, 267
computer programs for, 290
scaled-down DES, 258–259
Descartes, René, 295
Determinant, square (invertible) matrix, 153–155
Differential cryptanalysis, 272, 273
Diffie, Whit, 21, 22, 331, 333
Diffie–Hellman key exchange, 21, 22, 331, 346
computer program for, 369–370
discrete logarithms, 334
elliptic curve version, 467–468, 474
computer implementations and exercises, 486
exercises, 481
exercises, 360–361, 366–367
with groups, 459
public key cryptography, 336–337
Diffusion
one-time pad, 26
Shannon’s properties of, 272, 419
Digital signatures and authentication,
25
ElGamal cryptosystem, 347–349, 373
public key cryptography, 343–345
RSA cryptosystem, 340, 370–371
Digital Signature Standard (DSS), 345
Digraphs, 107, 132–133
Dimensions, matrix, 145
Direct method, modular exponentiation, 247
Discrete infinite sets, 4
Discrete logarithm problem, 303, 306
exercises, 367
on modular elliptic curves, 466–467
modular elliptic curves, 480
public key cryptosystems, 338
review of, 334–335
Discrete random variable, defined, 511
Discriminant, elliptic curve, 452
Disjoint cases, multiplication principle, 498
Disjoint ciphertext character sets, 189
Disjoint cycle decomposition, 115–116, 124, 205–206
Disjoint probabilities, addition to Kolmogorov’s axiom, 510
Disjoint sets, 492
Disjoint union, sets, 509–510
Distinct primes, square root modulo $m$, 84
Distributive laws
finite fields, 384
division algorithm, 392
polynomial multiplication, 387, 388
rings, 379, 380, 384
matrix arithmetic, 149, 171
multiplication algorithm in base $b$ expansions, 236
Venn diagrams, 494
Distributivity, set theoretic identities, 495
Dividend
definition of, 47
division algorithm for $\mathbb{Z}_p[X]$, 391, 392
Divisibility and modular arithmetic, 43–89
Chinese remainder theorem, 67–71
divisibility definition and examples, 43–44
division algorithm, 47–48
Euclidean algorithm, 48–52
exercises, 71–85
exercise solutions, 517–522, 572–581
extended Euclidean algorithm, 61–64
greatest common divisors and relatively prime integers, 46–47
modular arithmetic and congruences, 52–58
modular integer systems, 58–60
modular inverses, 60–61
primes, 44–46
solving linear congruences, 64–66
Divisibility criteria, application of congruences, 82–83
Division, polynomial; See Polynomials, division
Division algorithm, 519, 556–557, 563, 584
AES, 421, 434, 445
computer implementations and exercises, 86
congruences, 55–56
conversions among bases and integer equivalents, 223
addition algorithm with base $b$ expansions, 229
subtraction algorithm with base $b$ expansions, 232
Euclidean algorithm and, 48–50
extended, 158
Fermat’s little theorem, 297, 298, 546
matrix arithmetic, 158
modular arithmetic, 47–48, 87, 547
computer programs for, 80, 86
congruences and remainders, 55, 56, 80
Euclidean algorithm, 49, 50–51, 64
exercises, 72
nibbles, 421, 445
polynomial, 391–395, 421, 434
computer programs for, 412
Euclidean algorithm, 404, 405
exercises, 407, 408, 411
Divisor
definition of, 47
division algorithm for $\mathbb{Z}_p[X]$, 391, 392
Domain, basic concepts, 4, 5
Dominance laws, set theoretic identities, 495
Dot product
horizontal shifted, computer program for, 218
matrix operations, 146, 148
vectors, 199–200
Double complementation, set theoretic identities, 495
Double DES, 273
E
ECB (electronic codebook) mode, 274–275
Eckert, J. Presper, 252
Egyptian hieroglyphics, 92, 93, 95
Electronic codebook (ECB) mode, block cryptosystems, 274–275
Electronic Numerical Integrator and Calculator (ENIAC), 252
Elements
matrix, 145
sets, 491
Elements, The (Euclid), 45–46, 503
ElGamal, Taher, 345
ElGamal cryptosystem, 345–347
computer programs, 372–373
digital signatures with, 347–349
discrete logarithms, 334
elliptic curve addition, 466
elliptic curve version, 481
computer implementations and exercises, 486
plaintext representation, 471–473
procedure, 473–475
exercises, 363–364, 366–367
with groups, 459
mathematical problems providing security, 338
modular exponentiation, 301
Subject Index

Elliptic curve cryptography, 25, 451–487
addition of elliptic curves over \( \mathbb{Z}_p \), 463–466
addition operation for, 454–458
computer implementations and exercises, 483–487
Diffie–Hellman key exchange version, 467–468
ElGamal cryptosystem version, 473–475
elliptic curves over finite fields, 463
elliptic curves over real numbers, 452–454
elliptic curves over \( \mathbb{Z}_p \), 460–462
exercises, 477–483
exercise solutions, 563–567, 611–613
factoring algorithm based on, 475–477
groups, 458–462
modular
discrete logarithm problem on, 466–467
fast integer multiplication of points on, 470–471
plaintext representation on, 471–473
sizes of, 462–463
readings in, 616
selections for further reading, 616
Ellis, James, 22–23
Empty sets, 493
Empty strings, 3, 7
Encryption; See also specific systems
basic concepts, 2–3
codemaking evolution; See
Evolution of codemaking till computer era
cryptosystem components, 94
Encryption algorithm, AES, 435–439
128 bit keys, 437–439
scaled-down, 435–437
Encryption exercises, block
cryptosystems, 282–283
Encryption key, basic concepts, 2
Encryption mapping, two-round, 541–543
Encryption programs
AES, scaled-down, 421–425
DES, scaled-down, 288
public key cryptography
ElGamal cryptosystem, 372–373
Merkle–Hellman knapsack cryptosystem, 374–375
RSA cryptosystem, 370
three-round Feistel systems, 287
English alphabet, 13–14, 95
ENIAC (Electronic Numerical Integrator and Calculator), 252
Enigma machines
attack methods, 201–205
German usage protocols, 202–203
Polish codebreakers, 203, 204
Rejewski’s attack, 203–205
evolution of codemaking, 111–114
computer programs, 141–143
dissection into permutations, 119–126
scaled-down, 120–121
special properties of, 126–127
Entropy, 21
Entry, matrix, 145
Equal difference property, 444–445
Equality, polynomials in \( \mathbb{Z}_p[X] \), 385
Equivalence relations, 54
Error-detecting codes
credit card, 79–80, 89
ISBN, 77–79, 88–89
Error propagation, block
cryptosystems, 285
Euclid, 45, 503
Euclidean algorithm
computer implementations and exercises, 86–88
divisibility and modular arithmetic, 48–52
extended, 61–64, 347, 552
addition of elliptic curves over \( \mathbb{Z}_p \), 464
computer implementations and exercises, 414
polynomials, 404–405, 408–409, 414
RSA cryptosystem, 342
cryptosystem, 404–405, 408–409, 414
RSA security guarantees, 360
Euclid’s lemma, 51, 312, 461
Euler, Leonhard, 298, 299
Euler’s little theorem, 297–298
Euler’s phi function, 298–299, 303, 320, 326
Euler’s theorem, 300–301, 302, 359
cryptosystem, 320, 326
proof of, 546–547
Eve (literature convention), 2, 23
Event, sample space subset, 502
Evolution of codebreaking till computer era, 181–200
cryptosystem, 214–220
computer implementations and exercises, 214–220
Babbage/Kasiski attack, programs to aid in, 216–218
frequency analysis, programs to aid in, 214–215
Friedman attack, programs related to, 218–220
Enigmas, attack methods, 201–205
German usage protocols, 202–203
Polish codebreakers, 203, 204
Rejewski’s attack, 203–205
exercises, 208–214
exercise solutions, 530–536, 592–595
frequency analysis attacks, 181–186
index of coincidence, 193–201
invariance of cycle decomposition form, 205–208
Turing and Bletchley Park, 206–208
Vigenère cipher demise, 187–192
Babbage/Kasiski attack, 188–192
Friedman attack, 192
Evolution of codemaking till computer era, 91–143
affine ciphers, 96–100
ancient codes, 91–94
composition of functions, 109–110
computer implementations and exercises, 136–143
cyclic permutations/cycles, 114–119
enigma machines, 111–114
dissection into permutations, 119–126
special properties of, 126–127
exercise solutions, 522–526, 581–587
formal definition of cryptosystem, 94–96
homophones, 105–109
nulls, 102–105
permutations
computer representations of, 140–143
cyclic, 114–119
enigma machine dissection into, 119–126
tabular form notation for, 110–111
steganography, 100–102
tabular form notation for permutations, 110–111
Exercise solutions, 451–487, 515–567
Expansion function, DES, 266, 267
Expansions
DES, 261, 269
integers in different bases, 221, 222, 223, 224–227
addition algorithm with base $b$ expansions, 229–231
multiplication algorithm with base $b$ expansions, 234–237
subtraction algorithm with base $b$ expansions, 231–234
Expected value, binomial random variable, 512–513
Experiment, defined, 501
Exponentiation
algorithm complexity analysis, assessing work required to execute, 247
discrete logarithms, 334, 335
fast modular, 239–240, 545–546
squaring algorithm for, 250
Exponents
decryption; See Decryption exponent
magic, Fermat’s little theorem, 297, 298, 300
modular exponentiation; See Fast modular exponentiation; Modular exponentiation
RSA cryptosystem, 340, 341, 342
signature, ElGamal cryptosystem, 347
Extended Euclidean algorithm, 88, 347, 552
addition of elliptic curves over $\mathbb{Z}_p$, 464
divisibility and modular arithmetic, 61–64
polynomials, 404

F

Factorialization, prime; See Prime factorialization
Factorials, 13
Factoring
elliptic curve arithmetic-based, 482
elliptic curve cryptography-based algorithm, 451, 475–477
Miller–Rabin test with factoring enhancement, 315–316, 328–329
Pollard p-1 factoring algorithm, 316–319
public key cryptosystems
computer implementations and exercises, 371–372
elementary factoring method, 368
one-way functions, 333
RSA cryptosystem, 342
RSA security guarantees, 358
spread 331–368, 338
Factoring problem, 309
Factorization
fundamental theorem of arithmetic, 44
primes, 44, 45, 85–86, 357, 358
RSA cryptosystem, 342
RSA security guarantees, 342, 357, 358
Factors, divisibility, 43, 389
<table>
<thead>
<tr>
<th>Subject</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fair, probability concepts</td>
<td>502</td>
</tr>
<tr>
<td>Fast integer multiplication</td>
<td>470–471, 485–486</td>
</tr>
<tr>
<td>of points, elliptic curve</td>
<td></td>
</tr>
<tr>
<td>Fast matrix multiplication</td>
<td>150, 179</td>
</tr>
<tr>
<td>296–297, 545–546</td>
<td></td>
</tr>
<tr>
<td>Fast modular exponentiation</td>
<td>239–240, 296–297, 545–546</td>
</tr>
<tr>
<td>Diffie–Hellman key exchange,</td>
<td></td>
</tr>
<tr>
<td>elliptic curve protocol</td>
<td>469</td>
</tr>
<tr>
<td>discrete logarithms</td>
<td>335</td>
</tr>
<tr>
<td>Koblitz’s algorithm</td>
<td>472, 473</td>
</tr>
<tr>
<td>Feedback modes, block</td>
<td></td>
</tr>
<tr>
<td>cryptosystems</td>
<td></td>
</tr>
<tr>
<td>cipher feedback (CFB) mode</td>
<td>276–278</td>
</tr>
<tr>
<td>output feedback (OFB) mode</td>
<td>278–279</td>
</tr>
<tr>
<td>Feistel, Horst, 253</td>
<td></td>
</tr>
<tr>
<td>computer implementations and</td>
<td></td>
</tr>
<tr>
<td>exercises, 287</td>
<td></td>
</tr>
<tr>
<td>DES, 265</td>
<td></td>
</tr>
<tr>
<td>exercises, 280–281</td>
<td></td>
</tr>
<tr>
<td>self-decryption proof, 285</td>
<td></td>
</tr>
<tr>
<td>Fermat, Pierre de, 295, 296</td>
<td></td>
</tr>
<tr>
<td>Fermat’s little theorem</td>
<td>295–298, 546</td>
</tr>
<tr>
<td>exercises, 319, 320</td>
<td></td>
</tr>
<tr>
<td>Pollard p-1 factoring algorithm</td>
<td></td>
</tr>
<tr>
<td>basis, 317</td>
<td></td>
</tr>
<tr>
<td>Fermat’s primality test</td>
<td>309–311</td>
</tr>
<tr>
<td>computer programs for, 328</td>
<td></td>
</tr>
<tr>
<td>exercises, 323</td>
<td></td>
</tr>
<tr>
<td>Feynman, Richard, 357</td>
<td></td>
</tr>
<tr>
<td>Field isomorphism, 382</td>
<td></td>
</tr>
<tr>
<td>Finite fields, 377–415</td>
<td></td>
</tr>
<tr>
<td>AES; See Advanced encryption</td>
<td></td>
</tr>
<tr>
<td>standard protocol</td>
<td></td>
</tr>
<tr>
<td>binary operations, 377–378</td>
<td></td>
</tr>
<tr>
<td>building from ( \mathbb{Z}[X] ), 396–399</td>
<td></td>
</tr>
<tr>
<td>computer implementations and</td>
<td></td>
</tr>
<tr>
<td>exercises, 411–415</td>
<td></td>
</tr>
<tr>
<td>definition of, 381</td>
<td></td>
</tr>
<tr>
<td>elliptic curves over, 463</td>
<td></td>
</tr>
<tr>
<td>exercises, 406–411</td>
<td></td>
</tr>
<tr>
<td>exercise solutions, 554–560, 608–609</td>
<td></td>
</tr>
<tr>
<td>fields, 381–384</td>
<td></td>
</tr>
<tr>
<td>addition and multiplication</td>
<td></td>
</tr>
<tr>
<td>tables, 384</td>
<td></td>
</tr>
<tr>
<td>definition of, 381</td>
<td></td>
</tr>
<tr>
<td>inventory of, 382</td>
<td></td>
</tr>
<tr>
<td>Galois fields, 382, 399–403</td>
<td></td>
</tr>
<tr>
<td>polynomials in ( \mathbb{Z}_p[X] )</td>
<td></td>
</tr>
<tr>
<td>addition and multiplication of,</td>
<td></td>
</tr>
<tr>
<td>386–387</td>
<td></td>
</tr>
<tr>
<td>congruences in modulo as fixed polynomial, 395–396</td>
<td></td>
</tr>
<tr>
<td>divisibility in, 389–390</td>
<td></td>
</tr>
<tr>
<td>division algorithm for, 391–395</td>
<td></td>
</tr>
<tr>
<td>as ring, 388–389</td>
<td></td>
</tr>
<tr>
<td>polynomials with coefficients in ( \mathbb{Z}_p ), 385</td>
<td></td>
</tr>
<tr>
<td>rings, 378–380</td>
<td></td>
</tr>
<tr>
<td>Finite sets, 4, 452, 491</td>
<td></td>
</tr>
<tr>
<td>Finite strings, 7</td>
<td></td>
</tr>
<tr>
<td>First on, first off, 333</td>
<td></td>
</tr>
<tr>
<td>Fixed elements, cyclic</td>
<td></td>
</tr>
<tr>
<td>permutation, 115</td>
<td></td>
</tr>
<tr>
<td>Floating point platform</td>
<td></td>
</tr>
<tr>
<td>limitations, 240, 325; See also Computation issues</td>
<td></td>
</tr>
<tr>
<td>Floor function, 40, 47–48</td>
<td></td>
</tr>
<tr>
<td>Flowers, Tommy, 252</td>
<td></td>
</tr>
<tr>
<td>FORTRAN, 252</td>
<td></td>
</tr>
<tr>
<td>Frequency analysis</td>
<td></td>
</tr>
<tr>
<td>computer program for modular</td>
<td></td>
</tr>
<tr>
<td>frequency counts, 216</td>
<td></td>
</tr>
<tr>
<td>computer programs to aid in,</td>
<td></td>
</tr>
<tr>
<td>214–215</td>
<td></td>
</tr>
<tr>
<td>Frequency analysis attacks</td>
<td></td>
</tr>
<tr>
<td>evolution of codebreaking, 181–186</td>
<td></td>
</tr>
<tr>
<td>homophonic cryptosystems and, 106–107</td>
<td></td>
</tr>
<tr>
<td>Vignère cipher, 189–190</td>
<td></td>
</tr>
<tr>
<td>Frequency vector, Friedman</td>
<td></td>
</tr>
<tr>
<td>attack, 199</td>
<td></td>
</tr>
<tr>
<td>Friedman, William F., 188</td>
<td></td>
</tr>
<tr>
<td>Friedman attack, 197–201</td>
<td></td>
</tr>
<tr>
<td>computer programs related to, 218–220</td>
<td></td>
</tr>
<tr>
<td>index of coincidence, 194</td>
<td></td>
</tr>
<tr>
<td>Vignère cipher demise, 192</td>
<td></td>
</tr>
<tr>
<td>Functions; See also Mapping</td>
<td></td>
</tr>
<tr>
<td>basic concepts, 3</td>
<td></td>
</tr>
<tr>
<td>composition of, evolution of  codemaking, 109–110</td>
<td></td>
</tr>
<tr>
<td>cryptosystem components, 94</td>
<td></td>
</tr>
<tr>
<td>overview, 4–8</td>
<td></td>
</tr>
<tr>
<td>inverse, 7–8</td>
<td></td>
</tr>
<tr>
<td>one-to-one and onto, bijections, 5–7</td>
<td></td>
</tr>
<tr>
<td>substitution ciphers, 8–11</td>
<td></td>
</tr>
<tr>
<td>Fundamental theorem of algebra, 453</td>
<td></td>
</tr>
<tr>
<td>Fundamental theorem of arithmetic, 44, 46, 51–52</td>
<td></td>
</tr>
</tbody>
</table>

**G**

Gadsby (Wright), 14
Galois, Evariste, 382, 383
Galois fields, 254, 382, 399–403, 404
AES; See also Advanced encryption standard protocol
AES algorithm operations, 432, 433
encryption, 423–424, 432
Mix Column mapping, 430
nibble addition and multiplication, 419, 420
building finite fields from \( \mathbb{Z}_p[X] \), 396–399
computer programs for addition/multiplication, 413
computation of inverses, 414
Gauss, Carl Friedrich, 52–53, 382
Gaussian elimination, 159
Gauss's algorithm
computer program for, 326
exercises, 322, 325
primitive roots, 307–308
General substitution cipher, known plaintext attack, 13
Geometric algorithm, elliptic curve addition, 455, 456
German usage protocols for Enigmas, 202–203
Government Communications Headquarters (GCHQ), 22, 23
Governments, 3, 356–357
Gram, 190
Graphs, elliptic curve, 453, 454, 455
Greatest common divisors and relatively prime integers, 46–47
Great Internet Mersenne Prime Search (GIMPS), 82
Groups
DES, 273
elliptic curve cryptography, 458–462
Group theory, 459–460

H
Hackers, 2
Hadamard, Jacques, 294
Hardy, Godfrey, 294
Hasse's Theorem, 463, 468
Hawaiian alphabet, 210
Hellman, Martin, 21, 22, 273, 331, 333, 352, 353
Hexadecimal form
AES algorithm operations, 432, 433, 434
DES, 282
computer programs, 290
decryption program, 291

Galois field computations, 400, 401, 402, 403, 408
integers in different bases, 221, 224–227
addition algorithm with base \( b \) expansions, 231–234
multiplication algorithm in base \( b \) expansions, 234–237
nibble operations, 420
Hieroglyphics, 92, 93, 95
Hill, Lester, 162
Hill cryptosystem, 162–166, 169
computer programs, 177–178
exercises, 169–171
Hindu puzzle, 67–71
History of cryptography
ADFGVX cipher, 33–34
Caesar cipher, 9–11
codebreaking; See Evolution of codebreaking till computer era
codemaking; See Evolution of codemaking till computer era
communications technology, 108–109
Mersenne primes, 81–82
one-time pad, 25–28
public key cryptography, 21–25
readings in, 615
selections for further reading, 615
Homophones, 523–524, 593–594
affine ciphers with, 138–140
evolution of codemaking, 105–109
randomized encryption system, 106–107
Horizontal shifted dot products, 218
Horizontal shifted match counts, 218

I
IBM, 252, 418, 419
Identity
abelian group, 459
additive, 379, 383, 410
elliptic curve addition, 458
multiplicative, 379, 380, 383, 410
polynomial, 390
Identity function, 110, 123
Identity matrix, 151, 152
Identity permutation, 96
Image, basic concepts, 4
Inclusion Exclusion principle, probability rules, 504
Independent events, 508
Indeterminate X, 385
Index of coincidence, 193–201, 218
Indian culture, cryptography in, 102
Industrial-grade primes, 314, 372
Infinite sets, 4, 491
Infinity
  elliptic curves over modular integers, 460, 462
  elliptic curves over real numbers, 452
Initial permutation, DES, 265, 266, 270, 271
  computer program for, 289
  inverse, 264, 265, 289
  scaled-down, 259, 260, 263, 264
Input set, basic concepts, 5
Institute of Electrical and Electronics Engineers (IEEE), 238
Integer arithmetic, overview, 38–39
Integers
  alphabets, 95–96
  divisibility and modular arithmetic; See Divisibility and modular arithmetic
  floor function, 40
  modular orders of invertible modular integers, 301–302
  number theory, 43
Integers in different bases, 221–250
  arithmetic with large integers, 237–239
  computer implementations and exercises, 248–250
  exercises, 241–247
  exercise solutions, 536–540, 595–599
  fast modular exponentiation, 239–240
  hexadecimal and binary expansions, 224–227
  addition algorithm with base b expansions, 231–234
  multiplication algorithm in base b expansions, 234–237
  representation of, 221–224
Integer size
  RSA cryptosystem, 341
  symbolic versus floating point systems, 240, 314
Integers modulo m, 58
Integer systems
  modular, 58–60
  relatively prime integers, 46–47
Integer/text conversions, 36–37
Integral domains, 409–410
Integrity, basic concepts, 1
Intersection, sets, 492–495
Invariance of cycle decomposition form, 205–208
Inverse functions
  overview, 7–8
  S-box, 430
  shift permutation, 10
  substitution ciphers, English alphabet, 96
Inverse permutation
  computer program for, 141
  cycle, 116
  DES, 289
  substitution ciphers, English alphabet, 96
Inverse problem, 24
Inverses/inversion/invertibility
  abelian group, 459
  AES computer programs for, 448
  S-box, 444, 448
  composition of functions, 332–333, 429
  elliptic curve addition, 458
  finite fields
    Galois fields, 414
    polynomial Euclidean algorithm for determination of, 408–409
    rings, 379–380, 407
    matrices, 176–177, 430
    classical adjoint for, 159–162
    computer implementations and exercises, 174–176, 178–179
    definition of, 151–153
    definition of invertible matrix, 151–152
    determinant of, 153–155
    Hill cryptosystem, 162–166
    square (invertible), 155–156
    square modular integer, 157–158
    modular, 60–61
    brute-force approach, 87
    extended Euclidean algorithm, 88
    modular orders of invertible modular integers, 301–302
    notation for, 332
  Invertible affine mapping, AES S-box description, 444
  Inv Mix Column, 440
  Inv Nibble Sub mapping, 430, 431, 439–440
  Inv Shift Row, 440
Irreducible polynomials; See Polynomials, irreducible/irreducibility
ISBN error detecting codes, 77–79, 88–89
Isomorphism, field, 382
J
Jacobi, Carl Gustav, 382
Japan, Enigma machine, 112
Jefferson, Thomas, 107–108
j-fold composition, 117
j-unit shift, 123
K
Kasiski, Friederich W., 187
Kayal, Neeraj, 309
k-cycle, 116
Keyboard, Enigma machine elements, 112, 113, 121
Key exchange
Diffie–Hellman, 336–337
secure, quest for, 332–333
Key exchange protocols, 331
Key extraction permutation, DES, 261
Key generation matrix, AES encryption, 425, 426
Key k, AES encryption, 424
Key length
AES, 417, 419
DES cryptosystem, 253
one-time pad, 27, 40
Vigenère cipher, 189, 190, 191, 198, 572
Babbage/Kasiski attack, 216
Friedman attack, 201
Key permutation, English alphabet substitution cyphers, 96
Keys
basic concepts, 2
cryptosystem components, 94
one-time pad, program for creating, 40
private key cryptosystems, 21
public key cryptography, 23
substitution ciphers, 9
Key schedule, Feistel cryptosystems, 255
Key search, Moore’s law, 440
Key size
AES, 417, 421, 432
DES, 254
scaled-down, 258
triple, 273–274
Keyspace
DES, 265
Diffie–Hellman key exchange, 336, 337
RSA cryptosystem, 340
Knapsack problems/cryptosystems, 349–352
computer programs for, 374–375
mathematical problems providing security, 338
Merkle–Hellman, 352–356
public key cryptosystems, 338
Known plaintext attacks, 12, 13, 32, 132, 583
AES Nibble/Byte Sub Transformations and, 445
affine ciphers, 98–99
ElGamal cryptosystem, 367
Hill cipher, 177–178
Koblitz, Neal, 158, 451
Koblitz’s algorithm, 472, 473, 481, 486
Kolmogorov, Andrey, 503
Kolmogorov axioms, 503–504, 505, 510
Kolmogorov probability functions, 507
Kronecker delta, 192
L
Lampboard, Enigma machine elements, 112, 113
Large integers, arithmetic with, 24, 237–239
Leading term, polynomials in \(Z_p[X]\), 387
Lenstra, Hendrik, 451
Lenstra’s algorithm, 476–477, 482, 487
Letter frequency, English alphabet, 13–14, 107
Linear congruences
Chinese remainder theorem, 67–71
solving, 64–66
Linear cryptanalysis, 272, 273
Linguistic properties of language, and frequency-based attacks, 182
Logarithms, discrete, 334–335
Lorenz cipher, 252
Lorenz encryption machines, 252
Lucifer system, 95
M
Magic exponent, Fermat’s little theorem, 297, 298, 300
Mallory (literature convention), 2, 23
Mapping, 4; See also Functions AES
decryption, 429–432
affine function; See Affine function/mapping
two-round, 541–543
MARS, 418
Match counts, horizontal shifted, 218
Mathematical description, AES S-box, 443–444
Mathematical foundations of cryptography, 2, 3
readings in, 615–616
selections for further reading, 615–616
Matrices, 145–179
AES, 424–425, 437, 444
anatomy of matrix, 145–146
arithmetic operations, 149–151
addition, subtraction, and scalar multiplication, 146–147, 149, 150, 175
multiplication; See also Matrix multiplication
Subject Index

classic adjoint for matrix inversions, 159–162
computer implementations and exercises, 174–179
definition of, 147–148
exercises, 166–174
exercise solutions, 526–530, 587–592
Hill cryptosystem, 162–166
modular integer systems, 156–158, 161
multiplication, 147–149
nibble, 424–425, 427
exercises, 441
scaled-down AES encryption, 422
noncommutative ring, 379
noncommutativity of, 148–149
square (invertible) matrix
definition of, 151–153
determinant of, 153–155
inverses of 2x2 matrices, 155–156
transpose of matrix, 156
Matrix distributive law, 171
Matrix multiplication, 147–149
AES decryption, 440
AES encryption, 423
associativity property, 149
block, 172–173
chain, 167–168
computer implementations and exercises, 179
definition of, 147–148
Mix Column mapping, 430
nibble, 441
noncommutativity of, 148–149
ring axioms and, 379
scalar; See Scalar multiplication
Strassen's algorithm, 173–174
Matsui, Mitsuru, 273
Mauchly, John W., 252
Members, set, 491
Menezes, Alfred, 273, 616, 617
Merkle, Ralph, 22, 273, 331, 352, 353
Merkle–Hellman knapsack cryptosystem, 352–356
computer program for, 374–375
exercises, 364–365
Mersenne, Marin, 81
Mersenne primes, 342
Microdots, 100
Miller, Gary, 312
Miller, Victor, 451
Miller–Rabin test, 312–314
computer program for, 327–329
exercises, 323
with factoring enhancement, 315–316, 323
Minoan script, 93, 94
Mix Column Transformation, AES, 440
computer programs for, 447, 448
decryption, 431, 440, 448
encryption, 422–423, 424, 428, 436–437
exercises, 444–445
inverse, 431, 440
Modes of operation, block cryptosystems, 274–279, 285
mod function, computer, 57, 86–87, 161
Mod n primitive roots, exercises, 321–322
Modular arithmetic; See also Divisibility and modular arithmetic
AES algorithm operations, 433, 434
Chinese remainder theorem, 67–71
computer implementations and exercises, 175–179
and congruences, 52–58
elliptic curve-based factoring algorithm, 476
exercises, 321
integer systems, 58–60
inverses, 60–61
matrix, 175
Mix Column mapping, 430
public key cryptography; See Public key cryptography
solving linear congruences, 64–66
square root modulo m, 83–84
Modular elliptic curves
addition of elliptic curves over $\mathbb{Z}_p$, 463–466
computer implementations and exercises, 484, 485
Diffie–Hellman key exchange, 467–470
discrete logarithm problem on, 466–467
exercises, 478, 479, 480, 481, 482–483
fast integer multiplication of points on, 470–471
plaintext representation on, 471–473
properties of, 460–462
sizes of, 462–463
Modular exponentiation
algorithm complexity analysis, assessing work required to execute, 247
discrete logarithms, 334, 335
Euler's theorem, 300–301
exercises, 319, 320
fast, 239–240, 296–297, 545–546;
See also Fast modular exponentiation
squaring algorithm for, 250
Modular frequency counts, computer program for, 216
Modular integer matrices, 156–158
computer implementations and exercises, 175–177, 178–179
addition and scalar multiplication, 175
determinant of, computing using cofactor expansion, 176

Modular integers
alphabets, 95–96
elliptic curve-based factoring algorithm, 476
elliptic curves over, 459, 460–462
invertible, modular orders of, 301–302
rings, 379

Modular inverses
brute-force approach, 87
Hill cryptosystem decryption, 164
Modular orders of invertible modular integers, 301–302
Modular polynomials, 402–403, 406, 411, 443
Modular powers, 321
Modulus attacks, RSA cryptosystem, 342, 365
Monoalphabetic ciphers, passive attacks on substitution cipher, 12–15
Monotonicity, probability rules, 504
Moore, Gordon, 356
Moore’s law, 356–357, 440
Multiples, divisibility, 43, 389
Multiple solutions, knapsack problems, 349–350

Multiplication
AES algorithm operations, 433, 434
algorithm complexity analysis, assessing work required to execute, 246, 247
algorithm with base b expansions, 234–237
counting principles, 495–499
fast integer multiplication of points on modular elliptic curves, 470–471
fields, 383
finite fields, 384
Galois fields, 399, 400, 401, 402
AES encryption, scaled-down version, 423
AES security, 417
computer program for, 413
matrix; See Matrix multiplication
modular integer systems, 59
mutativity of, 380
nibble, 419, 446
polynomials; See Polynomials, multiplication
rings, 378, 380, 381, 406–407, 410
scalar; See Scalar multiplication
vector, polynomials in $\mathbb{Z}_p[X]$, 388

Multiplication principle, 13, 495–499
Multiplication rule, 509
Multiplicative functions, exercises, 324–325
Multiplicative groups, 459
Multiplicative identity, 379, 383, 410
Multiplicative inverse, rings, 379–380
Mutativity of multiplication, and distributive law, 380
Mutually exclusive events, 503, 509–510
Mutually exclusive (disjoint) sets, 493

N

Nagell, Trygve, 294
National Bureau of Standards (NB), 253
National Institute of Standards and Technology (NIST), 251, 253, 254, 345, 417, 418
National Security Agency (NSA), 3, 252–253, 357
Native American languages, 93–94
Navajo speakers in WWII, 93
n-gram, 190
Nibbles, AES, 419–421
computer implementations and exercises, 445–446
encryption, 424–425, 427
exercises, 441, 444–445
Nibble Sub mapping, inverse of, 430, 439–440
Nibble Sub Transformation, AES computer programs for, 447
decryption, 431
encryption, 422, 424, 428
exercises, 445
Nicolas, Jean Gustave, Baron de la Vallée Poussin, 294
Noncommutative ring, 379
Nonrepudiation, 25, 340
Nonsingular elliptic curve as abelian group under addition operation, 465
computer implementations and exercises, 483–484, 485
definition of, 452
exercises, 478, 479, 480, 481, 483
fast integer multiplication of points on, 470–471
graphs, 453, 454
over modular integers, 460–461
over real numbers, 452
Waterhouse’s Theorem, 463
NP complete problems, 24, 350
Nulls
  affine ciphers with, computer programs, 137–138
  evolution of codemaking, 102–105
  homophones combined with, 107
Number of rounds
  DES, scaled-down, 258
  Feistel cryptosystems, 255
Numbers, matrix terminology, 146
Number systems, abelian group, 458–460
Number theory and algorithms, 43, 293–299
  Carmichael numbers, 311–312
  computer implementations and exercises, 325–329
  divisibility and modular arithmetic;
  See Divisibility and modular arithmetic
  Euler phi function, 298–299
  Euler’s theorem, 300–301
  exercises, 319–325
  exercise solutions, 545–550, 601–604
  Fermat’s little theorem, 295–298
  Fermat’s primality test, 309–311
  Miller–Rabin test, 312–316
  with factoring enhancement, 315–316
  modular orders of invertible modular integers, 301–302
  order of powers formula, 305–308
  Pollard p-1 factoring algorithm, 316–319
  prime number generation, 308–309
  prime number theorem, 293–295
  primitive roots, 302–305
    determination of, 304–305
    existence of, 304
O
  Object weights, knapsack problems, 349, 350–352
    computer programs for, 374
    Merkle–Hellman knapsack cryptosystem, 352–356
  Octal expansions, 225
  OFB (output feedback) mode, 278–279
  One, multiplicative identity in R, 379
  One-time pad, 25–28, 40
    one-to-one functions
      overview, 5–7
      substitution ciphers, 8–11
  One-unit shift permutations, 119
  One-way functions
    Merkle–Hellman knapsack cryptosystem, 353
    public key cryptography, 333–334
Onto functions
  overview, 5–7
  substitution ciphers, 8–11
Ordered lists, Cartesian product set, 496
Ordered pairs, 20, 378, 564, 583
  binary operations, 377, 378
  elliptic curves
    modular, 460, 461, 462
    over real numbers, 452
  Order of powers formula, 305–308
Orders, 293
  computer program for, 326
  computing, 303
  elliptic curve
    addition of elliptic curves over \( \mathbb{Z}_p \), 465, 466
    computer implementations and exercises, 485
  exercises, 321
  modular, of invertible modular integers, 301–302
Outcome, experiment definition, 501
Output feedback (OFB) mode
  active attack on, 285
  block cryptosystems, 278–279
Output target set, basic concepts, 5
Overview, 1–41
  attacks on cryptosystems, 12–15
  computer implementations and exercises, 35–41
  computer-generated random numbers, 39–41
  integer/text conversions, 36–37
  integer arithmetic, 38–39
  programming basic ciphers with
    vector/string conversions, 35–36
  definitions of basic concepts, 1–4
  exercises, 28–35
  ADFGVX cipher, 32–35
  solutions, 515–517, 569–572
  functions, 4–8
    inverse, 7–8
    one-to-one and onto, bijections, 5–7
    one-time pad, perfect secrecy, 25–28
    one-time pad, perfect secrecy, 25–28
  Playfair cipher, 18–25
  substitution ciphers, 8–11
  Vigenère cipher, 15–18
P
  P = NP question, 24
  Painvin, Georges, 33–34
  pairwise mutually exclusive events, 503, 509–510
  Paradoxes, set definition, 491
  Partial substitutions, computer program for, 215
Pascal, Blaise, 295
Passive attacks
  on affine ciphers, 98–100
  basic concepts, 12
  on substitution cipher, 12–15
Perfect secrecy, 26
Performance guarantee, Miller–Rabin test, 314
Periodicity, powers of mod integers, 293
Periodic substitution ciphers, Friedman attack, 192
Permutation ciphers, 101
Permutations
  conjugates of, 123
  evolution of codemaking
    computer representations of, 140–143
    cyclic, 114–119
    enigma machine dissection into, 119–126
    tabular form notation for, 110–111
  random, computer program for generating, 219–220
  substitution ciphers, 9
Phaistos disk, 92–93, 94
Phi function, Euler’s, 298–299, 303, 320
Plaintext
  basic concepts, 2, 3
  conversion to numerical equivalents, 225–228
  cryptosystem components, 94
  Enigma machine properties, 126
  monoalphabetic and polyalphabetic ciphers, 12–13
  representation on modular elliptic curves, 471–473
  computer implementations and exercises, 486
  exercises, 481, 482
  scytale cipher, 101–102
  substitution ciphers, 8–11
Plaintext attacks, 12
  affine ciphers, 98–99
  chosen; See Chosen plaintext attacks
  known; See Known plaintext attacks
Playfair, Lyon, 18
Playfair cipher
  overview, 18–25
  programming with integer arithmetic, 39
Plugboard, Enigma machine elements, 112, 113, 121
Points, elliptic curve, 451
  addition, 455
  computer implementations and exercises, 484, 485–486
  Diffie–Hellman key exchange, 468
  elliptic curves over real numbers, 452
  modular, determination of number of, 462, 463
  Polish codebreakers, Enigma attack methods, 203, 204
Pollard, John, 317
Pollard p-1 factoring algorithm, 316–319
  comparison with Lenstra’s algorithm, 487
  computer program for, 329
  exercises, 323
Polyalphabetic ciphers, passive attacks on substitution cipher, 12–15
Polynomial complexity, RSA security guarantees, 357
Polynomials
  addition, 388, 398
    computer program for, 411
    exercises, 407
    nibble, 419, 420
  polynomials in \( \mathbb{Z}_p[X] \), 386–387
  AES algorithm operations, 432, 433–434
  Ben-Or’s irreducibility determination algorithm, 410–411
  building finite fields from, 396–399
  with coefficients in \( \mathbb{Z}_p \), 385
  computer programs
    for checking irreducibility, 412
    for extended and regular Euclidean algorithm for, 414
    for multiplication, 413
  congruences in \( \mathbb{Z}_p[X] \) modulo as fixed polynomial, 395–396
  constant, 385
  divisibility in, 389–390
  division, 407, 408
    computer program for, 412
    division algorithm for, 391–395
    nibble operations, 421
  elliptic curves over, 460–462
  Euclidean algorithm, 404–406, 408–409
  fundamental theorem of algebra, 453
  Galois fields, 382, 399–403
  irreducible/irreducibility, 405
  Ben-Or’s irreducibility determination algorithm, 410–411, 414–415
  computer program for checking, 412
  computer programs for checking, 412
  defined, 390
  exercises, 408
  test of, 394, 395
  modular, 402–403, 406, 411, 443
multiplication, 386–387, 388, 398, 407
AES algorithm operations, 433, 434
computer programs for, 412, 413
nibble, 419, 420
in \(\mathbb{Z}_p[X]\), 386–387
in \(\mathbb{Z}_p[X] \mod m\), 413
nibble addition and multiplication, 419, 420
as ring, 388–389
vector representation of, 387–388
Polynomial time algorithms, 309, 355–356
Schoof’s, 468
Polynomial time prime factorization algorithm, 357
Positive integers, number theory, 43
Positive integer solutions, 70, 295, 320
Powers
exercises, 321
modular orders of invertible
modular integers, 301–302
order of powers formula, 305–308
periodicity in, 293
P problems, 24
Prime certification tests, 309
Prime factorization, 24, 309, 357
computer implementations and exercises, 85–86
elliptic curve arithmetic-based
algorithms, 451
Prime factors, 45, 46
elliptic curves, 476
modular inverses, 60–61
Pollard p-1 factoring algorithm, 317, 318
prime factorization program, 85–86
prime number theorem, 294
public key cryptography, 605
RSA cryptosystem, 347, 368
Prime modulus
elliptic curve points, 478
elliptic curves over modular
integers, 459, 460–462
Prime numbers
Diffie–Hellman key exchange, 336, 337
ElGamal cryptosystem, 347
Fermat’s primality test, 309–311
finite fields, 377
generation of, 308–309
industrial-grade, 314
modular arithmetic, 44–46
computer implementations and exercises, 85
factorizations, 44, 45
fundamental theorem of arithmetic, 44
Mersenne primes, 81–82
relatively prime integers, 46–47
square root modulo, 83–84
Wilson’s theorem, 84–85
modular powers, 321
Pollard p-1 factoring algorithm, 316–319
primitive roots, 303
RSA cryptosystem, 340, 342
Sophie Germain primes, 337
tests of primality
Carmichael numbers, 311–312
computer programs for, 327–329
exercises, 323–324
Fermat’s little theorem, 309–311
Fermat’s primality test, 309–311, 327
Miller–Rabin test, 312–316, 327–329
Pollard p-1 factoring algorithm, 316–319
Prime number theorem, 293–295
exercises, 319, 545
prime number generation, 308
Primitive roots
elliptic curve analogues, 466
modular elliptic curves, 461
number theory, 293, 302–305, 547–548
public key cryptography
computer programs for, 326
determination of, 304–305
Diffie–Hellman key exchange, 336, 337
exercises, 321–322
equivalence of, 304
Gauss’s algorithm, 307–308
number theory concepts, 302–305
Private key
Diffie–Hellman key exchange, 469, 470
public key cryptography, 23, 24, 338
ElGamal cryptosystem, 346
Merkle–Hellman knapsack
cryptosystem, 353
Private key cryptosystems, 21
Probabilistic factoring algorithm, RSA
security guarantees, 358
Probabilistic primality test, 308
Probability, 295; See also Randomness
and probability
Probability function, 502, 504, 507
Probability rules, 504
Product
matrix multiplication, 148
nibble, 419
polynomials in \(\mathbb{Z}_p[X]\), 386
rings, 410
Proper subsets, 493
Pseudoprime generating program, 329
Pseudorandom numbers, 27
Public key
ElGamal cryptosystem, 346
Merkle–Hellman knapsack cryptosystem, 353
public key cryptography, 23, 338
RSA security guarantees, 357
Public key cryptography, 21–22, 331–375
computer implementations and exercises, 369–375
definition of, 94
Diffie–Hellman key exchange, 336–337
digital signatures and authentication, 343–345
discrete logarithm problem, review of, 334–335
ElGamal cryptosystem, 345–349
digital signatures with, 347–349
exercises, 360–369
exercise solutions, 550–554, 604–607
features of cryptosystems, 24–25
government controls on cryptography, 331–332
informal analogy for cryptosystem, 331–332
knapsack problems, 349–356
Merkle–Hellman knapsack cryptosystem, 352–356
number theory concepts
orders, 301–302
primitive roots, 302–305
one-way functions, 333–334
quest for complete public key cryptosystem, 337–338
quest for secure electronic key exchange, 332–333
RSA cryptosystem, 338–343
RSA security guarantees, 357–360
Puzzles, Chinese remainder theorem, 67–71

Q
Quality control, 510–511
Quantum computers, 357
Quotient
definition of, 47
division algorithm for \(\mathbb{Z}_p[X]\), 391, 392

R
Rabin, Michael, 312
rand, random integer generation, 40
Randomized encryption
homophones, 106–107
nulls, 104–105
Randomly generated matrix,
computation of invertibility probability, 178–179
Randomness and probability, 501–513
binomial random variables, 511–513
birthday problem, 505–507
conditional probability, 507–509
conditioning and Bayes’ formula, 509–511
pseudorandom number generation algorithm, 27
random variables, 511–513
terminology and axioms, 501–507
Random numbers, computer-generated, 28, 39–41
Random permutations, computer-generated program for generating, 219–220
Random substitution ciphers, 220
Random variables
binomial, 511–513
discrete, 511
Range, functions, 4, 5
RC6, 418
Real numbers
elliptic curves over, 452–454, 478, 483–484
floor function, 40
Rijndael, 418
Rijndael, 418–419

Rings
AES S-box, 444
building finite fields from \(\mathbb{Z}_p[X]\), 391, 392
Rijm, Vincent, 418
Rijndael, 418–419
Rings
AES S-box, 444
building finite fields from \(\mathbb{Z}_p[X]\), 396–399
commutative, 58
congruences in \(\mathbb{Z}_p[X]\) modulo as fixed polynomial, 395–396
exercises, 406–407, 408
finite fields, 378–380, 381, 383, 384
integral domains, 409–410
polynomials in \( \mathbb{Z}_p[X] \) as, 388–389
Ritter, Richard, 111
Rivest, Ronald, 22, 331, 338, 339
Root cubic equation, elliptic curve graphs, 453
Roots
elliptic curves over real numbers, 453
Gauss’s algorithm, 325
matrix, computer implementations and exercises, 174
modular elliptic curves, 461
polynomials in \( \mathbb{Z}_p[X] \), 409
primitive; See Primitive roots
Rosetta stone, 92
rot13 cipher shift, 10
Rotate Nibble operator, 425
Rotors, Enigma machine elements, 112, 113, 120, 121–122
Rotor window, Enigma machine elements, 113
Round constants, AES encryption, 425, 439
Round key function
DES, 267, 269
computer programs for, 288, 289–290
scaled-down, 263, 281
Feistel cryptosystems, 255
Round keys
AES, 422, 424
computer program for, 446
exercises, 441, 442
DES, 259, 265, 271, 282
computer programs for, 287–288, 289
generation of, 259
Round-off errors, 161
Round robin tournaments, application of congruences, 80
Rounds
AES, 421, 422, 440
DES, 258, 260, 261, 264
Feistel cryptosystems, 255
Row matrix, 146
Różycki, Jerzy, 203, 204
RSA (Rivest, Shamir, Adleman) cryptosystem, 24, 273, 339
computer programs for, 370–371, 372
development of, 22
digital signatures, 344–345
mathematical problems providing security, 338
Public key cryptography, 338–343
security guarantees, 357–360
RSA RC6, 418
RSA Security, 45, 294, 345
RSA-640, 327, 372
Russian alphabet, 95
S
Sample space, experiment, 501–503
partitioned, 509–510
reduced, conditional probability, 507
Saxena, Nitin, 309
S-box
AES
computer programs for, 446–447, 448, 449
cryptography, 437, 439
exercises, 441, 443–444
inverse, 430, 448
DES, 267, 268
computer programs for, 288, 289
exercises, 281–282
scaled-down, 261–262, 281, 282
S-box table, AES, 423
Scalar multiplication
computer implementations and exercises, 175
elliptic curve exercises, 480
matrix, 146–147
polynomials in \( \mathbb{Z}_p[X] \), 388
Scalars, defined, 146, 147
Scaled-down AES; See Advanced encryption standard protocol
Scaled-down DES
computer programs for, 287–289
exercises, 281–282
Scaled-down Enigma machines
composition of functions, 120–121
computer programs, 141–143
Scherbius, Arthur, 111
School algorithm, 468
Scytale, 101
Scytale cipher, 101–102, 128, 136–137
Second quotient, division algorithm for \( \mathbb{Z}_p[X] \), 391
Self-cancelling properties, XOR, 255, 429
Self-decryption proof, DES and Feistel cryptosystems, 285
Serpent, 419
Set differences, 494
Sets
basic concepts, 4, 5
basic counting principles, 495–499
binary operations, 377
concepts and notations, 491–495
finite fields, 377
modular elliptic curves, 452
Set theory, probability theory and, 503
Shannon, Claude, 25, 26
Shannon’s properties of diffusion and confusion, 272, 419
Shift cipher, 38, 95
Shift permutation, 189
  Caesar cipher, 10
  one-unit, 119
Shift register, cipher feedback (CFB) mode, 276
Shift Row mapping
  inverse of, 440
  reverse order, 429
Shift Row Transformation, AES
  decryption, 431
  encryption, 422, 424, 428, 429, 436
  exercises, 444–445
Shor, Peter, 357
Signature exponent, ElGamal cryptosystem, 347
Significant digits, computing platforms and, 325; See also Computation issues
Simultaneous congruences, Hindu puzzle, 67–71
Single linear congruence, solving, 66
Singleton set, 492
Singular elliptic curve
  definition of, 452
  graphs, 454
  over modular integers, 460
  over real numbers, 452
Sizes
  matrix, 145
  of modular elliptic curves, 462–463
Sophie Germain primes, 337
Spaces
  frequency analysis-based attacks, 183
  RSA cryptosystem, 340
  substitution ciphers, 10
Spinner, randomized encryption, 104–105
Square (invertible) matrix
  computer implementations and exercises, 175–176
  definition of, 146, 151–153
  determinant computation, 159
  determinant of, 153–155
  general cofactor expansions, 171–172
  inverses of 2x2 matrices, 155–156, 174–175
Square roots
  modular elliptic curves, 461, 462
  modulo m, 83–84
Standards, 2
  Digital Signature Standard (DSS), 345
  encryption; See Advanced encryption standard protocol;
  Data encryption standard
State matrix, Mix Column mapping, 430
State transformations (mappings); See Mapping
Statistical frequency counts, 13–14
Steganography, 100–102
Storage
  two’s complement representation scheme, 245–246
  as vectors or strings, 248
Strassen, Volker, 150
Strassen’s algorithm, 150–151, 173–174, 179
Stream modes, block cryptosystems, 276–279
Strings, 254
  basic concepts, 3
  computer programs for extracting ciphertext data from ciphertext string, 216–218
  XOR operation, 287
  integers in different bases, 248–250
  vector/string conversions, 35–36
String size, AES, 417
Strong avalanche condition, AES, 419
Subblocks, cipher feedback (CFB) mode, 276
Submatrix, 154
Sub Nibble operator, 425
Subsets, 5, 492
Substitution box, DES, 261–262, 267, 268
Substitution ciphers
  Caesar cipher, 9–11
  evolution of codemaking, 102
  cryptosystem components, 95
  homophonic, 107
  steganography, 100–101
  frequency analysis-based attacks, 183–186
  overview, 8–11
  passive attack example, 12–15
  random, computer implementations and exercises, 220
Substitution permutation network, 419
Substitutions
  congruent, 56–57
  partial, computer program for, 215
Subtraction
  algorithm complexity analysis, assessing work required to execute, 246–247
  matrix, 146–147
  rings, 379
Subtraction algorithm with base b expansions, 231–234
Sum
  addition of elliptic curves over $\mathbb{Z}_p$, 464
  elliptic curve addition, 455
nibble, 419
polynomials in $\mathbb{Z}_p[X]$, 386
Superincreasing weights, knapsack problem, 350–352
computer programs for, 374
exercises, 364–365
Merkle–Hellman knapsack cryptosystem, 352–356
*Symbolic Analysis of Relay and Switching Circuits, A.* (Shannon), 25
Symbolic computing platforms, 296, 314, 325, 334, 369
elliptic curve operations, 483
Lenstra’s algorithm, 477
public key cryptography, 334
RSA cryptosystem, 341
Symmetric key cryptosystems, 21, 23, 24; See also Private key cryptosystems
definition of, 94
DES development, 95
substitution ciphers, English alphabet, 96
Symmetry
congruency properties, 54
matrix, 156

T

Tables
basic concepts, 3–4
tabular form notation for permutations, 110–111, 220
Tangent line, elliptic curve properties, 453
T-attack, 272–273
Tempest devices, 357
Ternary expansions, 225
Text
integer/text conversions, 36–37
plaintext; See Plaintext
Three-round Feistel systems, 280–281
computer implementations and exercises, 287
self-decryption proof, 285
Time algorithm, School’s, 468
*Traité des Chiffres ou Secrètes Manières d’Ecrire* (Vignère), 15
Transitivity
congruency properties, 54
divisibility, 44, 68, 389
Transpose of matrix, 156, 171
Transposition ciphers, 101–102
Trapdoor (one-way) function, 333–334, 353
* Treatise on Numerals and Secret Ways of Writing* (Vignère), 15
Tree diagram, counting principles, 496
Trial (experiment), defined, 501
Trigram, 190
Trigraphs, 107
Triple composition, 122
Triple DES, 273–274, 291–292, 333
Trithemius, Johannes, 15
Trivial cycle, 115, 116
Turing, Alan, 206–208
Twofish, 419
Two-round encryption mapping, 541–543
Two-round Feistel systems, 258, 259, 263, 280
Two’s complement representation scheme, 245–246

U

Union, sets, 491, 492–495
Unique factorization, in $\mathbb{Z}_p[X]$, 405
Universal set, 494

V

Vacuously true, 493
van Oorschot, Paul, 273, 617
Vanstone, Scott, 273, 616, 617
Vatican ciphers, 102
Vaudenay, Serge, 356
Vector addition, 457
Vector multiplication, polynomials in $\mathbb{Z}_p[X]$, 388
Vectors, 254
Cartesian product set, 496
conversion programs, 286
dot product formula, 199–200
integers in different bases, 248–250
knapsack problem reformulation, 350
nibble addition and multiplication, 419
polynomial representations, 387–388
rings, 406–407
XOR program, 287
Vector/string conversions, 35–36
Venn diagrams, 492–495, 505
Vernam, Gilbert S., 26
Vernam cipher, 26
Verser, Rocke, 273
Vignère, Blaise de, 15
Vignère cipher, 107
demise of, 187–192
Babbage/Kasiski attack, 188–192
Friedman attack, 192
Friedman attack, 197–201
ciphertext-only, 200–201

Hill cryptosystem with, 166
one-time pad as, 28
overview, 15–18
programming with integer
arithmetic, 38–39
Vignère tableau, 16, 17

W
Waterhouse's theorem, 463, 476
Weak keys, DES, 284
Weights, object; See Object weights,
knapsack problems
Wheatstone, Charles, 18
Wilson's theorem, 84–85
Winograd, Shmuel, 150
Witness, primality test, 309–311, 314
Word length, 10, 240
Word size, 238
Wright, Edward V., 294
Wright, Ernest Vincent, 14

X
XOR operation, 254–255, 383, 407
AES, 428, 445
crcomputer implementations and
exercises, 447, 449
cryptonfire, 427
eexercise, 285
self-cancelling properties, 255, 429

Y
Young, Thomas, 92

Z
Zero, 378
Zero polynomial, 385, 387, 394
Zuse, Konrad, 251, 252
Zygalski, Henryk, 203, 204