INDEX 517

Cribbing, 21
examples of, 25–30
using isomorphs for, 66
Cryptanalysis, 4, 6
Kerckhoffs’ principles of, 4
CRYPTO ’N, 15, 358
Cryptographic salt, 480–481
Cryptographic system(s), 4, 12
Cryptosystem, 4
knapsack-like, 371
weaknesses in a, 136

Data Encryption Standard (DES), 288–311
chaining in, 295–297
components of
initial permutation (IP), 292
key schedule (PC-1, PC-3, KS), 292–293
P-box, 292
S-box(es), 289–292
cryptanalysis of, 300–309
DES-cracker, 308–310
architecture of, 309
key search algorithm of, 309–310
operation of, 310
differential cryptanalysis of, 302–309
DES-cracker, 308–310
architecture of, 309
key search algorithm of, 309–310
operation of, 310
differential cryptanalysis of, 302–309
output-feedback mode (OFB) of, 299–300
initial seed in, 299
randomness of, 297–299
sample encipherment of, 296
semi-weak keys of, 294
weak keys of, 293–294
Decipherment, 2
Decryption, 2
Diagnosis, 139–149
Diffie, Whitfield, 334, 337, 339–340
Diffie–Hellman key-exchange, 448–450
El Gamal’s extension of, 450–451
Digital signature(s) (SIG), 3, 337, 465–470
desiderata of, 466
message digest, 470–471
using elliptic curve cryptosystems, 444–445
Digital signature system(s), 467–470
El Gamal’s signature protocol, 475
MD5, 471–473

NIST’s digital signature algorithm, 474–475
public key cryptography and, 467–468
Rabin’s quadratic residue, 468–470
TRAnSactions in a Secure manner (TRASEC), 494–495
authentication scheme in, 494
Diophantine approximation, 364
simultaneous, 366–370
unusually good
(UGSDA), 367–370
Diophantine equations, 364
Diophantus of Alexandria (c. 200/214–c. 284/298), 364
Dirichlet L-series, 407
Discrete logarithm problem (DLP), 16, 414–426
Adelman’s subexponential algorithm for, 419
current state of research on, 428
in a group, 414, 420–426
modulo p, 414–419
Pohlig–Hellman’s solution of, 415–418
solution by index-calculus method, 422–424
Display of plain- and ciphertext, convention on, 20
Division algorithm for integers, 346
digital signature system for, 444–445
integrated encryption standard (ECIES), 444
NSA’s case for, 445
Elliptic curve(s), 429
Bezout’s Theorem for, 431
chord-tangent group law of, 431
Diffie–Hellman key exchange, 442
discriminant of, 429
Lenstra’s factorization algorithm on, 432
supersingular, 441
Elliptic group over the field $\mathbb{Z}_{m,2}$, 436–437
over the reals, 431–432
over the $\mathbb{Z}_p$, 434–436
computations in the elliptic group $\mathbb{Z}_{m,2}(a,b)$, 438–441
Ellis, James H., 342
Encipherment, 2
Encryption, 2
Enigma machine, 7, 160–170
components of, 160
cryptanalysis of Enigma ciphertext, 166–170
by cribbing, 167–170
using double-ended
Enigmas, 168–170
cryptanalysis of Enigma by
Rejewski, Marian
(1903–1990), 166
Rozycki, Jerzy
(1909–1942), 166
Welchman, Gordon
(1906–1985), 166–167
Zygalas, Henryk
(1906–1978), 166
encypherment equation of
the, 165–166
key distribution protocol for the, 163–164
message indicator, indicator setting, and discriminant of
Enigma ciphertext, 164–165
plugboard of the, 162–163
reflecting rotor (stator), 161–163
Eratosthenes (276 BC–194 BC), 390–391
measurement of earth’s circumference, 390–391
sieve of, 390–393
Euclidean algorithm, 348–350
for polynomials, 398–399
Euler’s theorem, 378
Euler totient function $\phi(n)$, 350
Expectation method (EM), 81
Extension field, 421, 426–428
Facility keyed-access cards (IBM Series/1), 491
cryptographic algorithm for, 329–330, 491
Factorization of integers, 339, 391, 393–394
Pollard’s p-algorithm for, 394–396
Feedback shift register (FSR), 245
Feige, Uriel, 477
Feistel, Horst (1915–1990), 283
Fermat’s little theorem, 377
Fermat’s primality test, 405
Fiat, Amos, 476–478
Japanese RED machine, (Continued) plugboard of, 194 stepping sequence of, 194–196 stepping shifts of, 195

Key, 4

Diffie–Hellman protocol, 448–450
El Gamal’s extension of, 450–451
Shamir’s autonomous protocol, 451–453

Space, 4

stream, 244–282

Knapsack cryptosystem, 350–371

trapdoor, 350–371

Knapsack problem (subset sum problem), 338–340 with modular arithmetic, 350–371

Knapsack problem (modulo m), 350

Knapsack vector, 344

super-increasing, 345, 350–354

Kolmogorov–Smirnov test, 136–138 evaluation using, 138 significance level in, 137

Kohnfelder, Lauren, 341–342, 467, 495 certificates of, 495

Kullback, Dr. Solomon (1903–1994), 11, 85

Lattice, 368–370

short vectors in, 368–370

Least common multiple lcm(), 385

Leibler, Richard A. (1914–2003), 85

Letters (of text), 1, 2

Lena’s factorization algorithm on elliptic curves, 432–433

Letter counts and probabilities, 32

Linear feedback shift register (LFSR), 245–246, 254–273 irregular clocking of, 274–278 characteristic polynomial of a, 251–253

combining, 259

cribbing of LFSR-enciphered ASCII plaintext, 260–271 sequences of, 254

matrix representation of, 260–261

maximal length LFSR sequences, 254–258 autocorrelation function of, 255–258

linear complexity (equivalence) of, 258 properties of, 258

Lorenz Schlüsselsatz (SZ40/fish), 170–190

cribbing of ciphertext, 176–190
cryptanalysis problems for, 173 finding the active pins of, 171 key of, 173

key stream generated by, 170 move indicator of, 183–190

pin wheels of, 171–173 statistical model of pin motion, 177–183 steps in encipherment, 174

LUCIFER, 283–287

implementation in IBM 2984, 284–287

key schedule of, 285–286 operations in, 286–287

P-Box of, 286–287

S-box of, 285–286

M-94 (CSP-488), 6, 7

Magnetic stripe technology, 482–483

protecting recording in, 482–483

Making a secure credit card payment on the Web, 502–505

Markman hearing, 514

Markov log-odds score, 38

Markov parameters

Gmarkov, 34

Hmarkov, 34

Smarkov, 34

Markov score, 34

Markov scoring, 34

Markov source, 31, 32

homogeneous, 31

Law of large numbers for, 40

Matyas, Stephen M., 455

Mauborgne, Joseph Oswald (1881–1971), 119

Maximum likelihood estimation (MLE), 81

partial maximum likelihood estimation, 73–78

Menezes–Vanstone elliptic curve cryptosystem, 443

Merkle, Ralph C., 15, 512

Merkle–Hellman trapdoor knapsack cryptosystem, 350–371

ASCII-text decipherment of, 357–358

ASCII-text encipherment of, 355–356

cryptanalysis of, 358–372

Mersenne, Marin (1588–1648), 409

Mersenne primes, 408–409

Message authentication, 3

Message authentication code (MAC), 3, 466, 498–500

MD5, 471–473

message digest, 471

Meyer, Carl H., 455

Miller–Rabin primality test, 406–407

Miller–Rabin theorem, 405–406

Modular arithmetic $\mathbb{Z}_p$, 346–347

multiplicative inverse in, 347, 378 polynomial, 248–250

residues in, 346–347

Modular exponentiation, 338–339, 376–377

program for, 376

Monoalphabetic substitution, 1

cryptanalysis of, 73

examples of, 68–73 table for a, 64

Multiprecision modular arithmetic, 387–389

basic modular operations, 387

internal representation of numbers, 387

Myer, Albert J. (1828–1880), 63–64

n-gram, 1

National Security Agency (NSA), 9, 10

Needham, Roger M., 335, 456

Needham–Schroeder protocol, 335, 456–462

using a symmetric key crypto system, 456–459

using a public key cryptosystem, 459–462

NIST’s digital signature algorithm, 474–475

NIST’s secure hash algorithm, 473–474

NIST’s statistical tests, 138–139

NIST’s monobit test, 138

NIST’s poker test, 138

NIST’s runs test, 139

NIST’s long run test, 139

Nonlinear feedback shift registers, 271–273

Nonlinear key stream generation, 273–274

Nonpatentable subjects, 508

Number theory and cryptography, 391

Oblivious transfer, 478

Odlyzko, Andrew M., 428

One-gram scoring using a Markov language model, 75
One-gram scoring using a one-gram language model, 74
One-time pad (tape), 119–120, 128–129
detecting reuse of Soviet, 130–131
Soviet RGB protocol for, 128–129
One-way function, 340, 480–481
trapdoor, 340
Parameters of a Markov model,
deriving the, 34
Password cracking, 481–482
Patents, 506–509
claims of, 507–508
anticipated, 508
invalid, 508
means plus function, 508
obvious, 508
equivalent structures/acts
of a, 509
file history, 508
format of, 507–508
invalid, 508
prior art, 507
requirements of, 507
enablement, 507
novelty, 507
obviousness/
nonobviousness, 507
written description, 508
utility, 507
role in cryptography, 509
specification of, 507
submarine, 515
validity of, 508
3 C’s, 507
subjects, Nonpatentable, 507–508
Perfect numbers, 408–409
Plaintext, 2, 6
Plaintext language models, 30, 31
Pohlig–Hellman algorithm, 415–418
Pollard’s p − 1 method, 391,
393–394
Pollard’s ρ-algorithm, 394, 424–426
for discrete logarithm
problem, 424–426
for integer factorization, 394
Polyalphabetic substitution, 116
periodic, 117
correlation analysis of,
120–124
estimating the period of
periodic polyalphabetic
substitution using
coincidence, 126–127
using correlation to find the
Vernam–Vigenère key
of, 120–124
using the κ-value for the
cryptanalysis of,
127–128
Polynomials over $\mathbb{Z}_2$, 247–250
division algorithm for, 247–248
exponent of, 249
factorization of, 249
irreducible polynomials, 247
modular arithmetic for, 248–250
reducible polynomials, 247
Porta, Giambattista della
(1538–1615), 117
Primality testing, 405
Primes, factorization of integers
into, 390
Prime number theorem, 391
Primitive roots modulo $p$, 397, 414
Privacy, 3
Private information (about a
cryptographic system), 5
Private key, 337–340, 354
Product block-cipher, 283
Feistel-like, 283
Project Gutenberg Free eBook
Library, 34
Pseudorandom sequence, 257
Pseudo-random bit generator
(PRBG), 502
Pseudo-random number generator
(PRBG), 257–258
next bit test of, 257, 502
Public information (about a
cryptographic system), 5
Public key, 337–340, 354
Public key cryptography, 334–341
Public key cryptosystem(s), 334–341
Public key certificates, 342, 449,
495–497
Purdy, George B., 480
Pythagorean triples, 428
Quadratic residue, 396–401
sieve, 403–405
factor base in, 404
steps in, 403
Quantum computers, 428
RSA’s, 502
Rabin, Michael O., 468–470
Rabin’s quadratic residue signature
protocol, 468–470
Random factorization (Dixon),
401–403
RC4, 278–280
key scheduling algorithm
of, 278–279
pseudorandom number generator
(PRGA) of, 278–280
Relatively prime numbers, 377
Riemann hypothesis, 407
generalized, 407
Riemann zeta function $\zeta(t)$, 407
Rijndael, 312–326
activity pattern, 323–325
block sizes of, 313
key sizes of, 313
operations of, 314–323
AddRoundKey, 321–323
ByteSub and
InvByteSub, 316–317
MixColumn and
InvMixColumn, 320
ShiftRow and
InvShiftRow, 317–318
propagation of patterns, 323–326
Ring, 10
Rivest, Ronald, 340, 378
Rotor, 150–151
displacement sequence (of a
rotor), 158–160
rotational displacement function
of, 153
wiring by interval method,
158–160
Rotor system(s), 152–153
patents of, 153–154
Hebern’s straight-through rotor
system, 152, 161
Rowlett, Frank B., 11, 12, 218, 243
RSA cryptosystem, 16, 340,
378–382
attacks on, 382–383
deciphering exponent, 378
ingeneric exponent, 378
decipherment/decipherment
transformation, 378
decipherment/decipherment
of ASCII-Plaintext, 379–382
parameter set, 378
Williams quadratic encipher-
ment, 384–387
William’s variation of, 383–387
RSA challenge, 16, 407–408
RSA-129, 408
Scherbius, Arthur
(1878–1929), 160–161
Schroeder, Michael D., 335
Secrecy, 2
digital signatures and
authentication, comparison
of, 468
in GSM, 276–278
secrecy systems, 465
Secure socket layer (SSL), 497–502

cryptographically secure random number generator for, 502

master secret in, 500–501

message authentication code in, 499–500

message digest algorithm of, 498, 499–500

messages in, 497–499

Client_Hello, 497–498

Server_Hello, 498

record protocol of, 499

SessionID of, 498

transaction, 497–499

data encipherment algorithm in, 498

handshake protocol in, 497

key exchange protocol of, 498, 500

anonymous Diffie–Hellman, 500

ephemeral Diffie–Hellman, 500

fixed Diffie–Hellman, 500

RSA, 500

SEEK cryptosystem, 450–451


Shannon, Claude (1916–2001), 5, 16, 18

confusion or substitution, 18

diffusion or transposition, 18

Shor, Peter W., 428

Side information, 6

Sieving, 390

SIGINT (Signals Intelligence), 9

Sinkov, Dr. Abraham (1907–1998), 12

Smart cards, 491–493

external interface of, 492–493

functionality of, 493

ISO standards for, 491–492

memory of, 492

processing capability, 493

Spoofing, 448–449

Statistical plaintext language source, 30

Stamler, Leon, 514–515

infringement: Diebold Incorporated, NCR Corporation and Manufacturers Hanover Trust vs., 514

infringement: RSA and VeriSign vs., 514–515

U. S. Patent No. 5,793,302, 514

U. S. Patent No. 5,936,541, 514

U. S. Patent No. 5,974,148, 515

Steganography, 9

Stream ciphers, 245

Stream encipherment, 245

Strong pseudoprime to the base a, 405

Threats to network transactions, 465

spoofing, 448–449

TRAnsactions in a SECure manner (TRASEC), 494–495

authentication scheme for, 494

Trapdoor knapsack problem, Merkle–Hellman, 350–358
cryptanalysis of, 358–370

encipherment/decipherment of ASCII-Plaintext, 355–358

information rate of, 354

modular mapping of, 358–360

modulus of, 350

multiplier in, 350

Trusted authority, 335

UNIX password, 480–481

United States Armed Forces Security Agency, 130

United States Patent Office classification code, 507

U.S. Patent No. 4,200,770, 448–449, 511–512

infringement: National Cash Register Corporation vs.

Chubb Integrated Systems, 510–511

U. S. Patent No. 3,543,904, 509–510

U. S. Patent No. 4,218,582, 512

U. S. Patent No. 4,405,829, 513

infringement: Public Key Partners vs. RSA Data Security Incorporated, 514

PKS/RSADI litigation, 514

User identifier, 335

User secret key, 335

VENONA (aka BRIDE, DRUG), 128–132

and Julius Rosenberg (aka LIBERAL), 132

VeriSign, 514

Vernam, Gilbert S. (1890–1960), 117–118

de Vigenère, Blaise (1523–1596), 117

Vigenère tableaux, 117

Williamson, Malcolm J. (1931–2003), 342

Wire code-wheel, 150

Wire-tapper, 465

Work function, 5

X.509 certificates, 493–497

advantages of, 496

certificate authority (CA), issuance by, 496, 503–505

example of, 497

structure of, 496–497

X9.17 protocol, 453–456

key exchange architecture, 453–455

data key, 453

distribution of, 455

hierarchy of keys of, 453

key encrypting key, 453

protocol mechanisms, 455–456