

Index.....	631
Editor s Biography	648

Index

Acme Commodity and Phrase Code, 383

Algebraic normal form transform, 79-80

Algorithm:

Berlekamp-Massey shift register synthesis, 80, 84

Coppersmith (discrete logarithm), 296-303

DES, 22

elliptic curve (factoring), 309

Euclid's (GCD), 261-62

fast data encipherment

(FEAL), 529

invertible secret key, 590-91

MD2 and MD4 (hashing), 367

number field sieve (factoring), 308-310, 520

probabilistic, 238

quadratic sieve (factoring), 250, 303-4

semi-invertible secret-key, 590

Telepass!, 588

Telepass2, 590-91

twisted double field (TDF), 590

Videopass, 590-91

Snefru (hashing), 368

American Bankers Association (ABA), standards, 5 I

American National Standards Institute (ANSI), 329

Committee X 12 (Electronic Business Data Interchange), 58

standards, 5 I-52

American Telephone & Telegraph (AT&T):

cryptographic device for protecting common carrier interoffice signaling (CCIS), 157

Vernam ciphers, 7

Arbitrated signatures, 333-34, 395-97, 413-16

Architecture (computer), relation to algorithms, 247-52

Arguments (zero-knowledge protocols), definition, 426, 434

Arms Control and Disarmament Agency (ACDA), 618

Arthur-Merlin interactive protocol, 428

Authentication 14-20, 381-419, (see *also* Authentication schemes)

appended authenticator, 384-86

authentication function, 16

Cartesian product construction for authentication codes, 395-96

channel bound (Gilbert-McWilliams-Sloan), 401

channel capacity (Simmons), 406-7

classification, 391-403

codes, 395-96, 398-401

and cryptography, 383

definition, 180, 382

and DES, 57, 385

desensitized, 387

digital signatures, using, 27-29, 138-39, 155, 166, 187, 195-99, 369-70

electronic funds transfer (EFT), 53, 58, 384-85

essential notions involved, 383

game theory model, 403-4

impersonation attack, 14

of information (messages), 379-419

LAN, 235

message authentication code (MAC), 329, 385, 396, 594, 622

model, 404

participants (characterization), 388-91

perfect authentication, 18

practice, 408-16

process, 382-87

relation to coding theory, 397-403

requirements, 182-83

RSA authentication channel, 393-94

substitution attack, 15

theoretical security of authentication, 18

threats, 388-91

U. S. military protocol, 383-84

with/without secrecy, 395-96, 407-8, 622-25

See also Information authentication

Authentication framework, 231-32

DARPA-Internet, 227

ISO, 219-24

Authentication schemes:

classification, 391-403

computationally secure schemes, 392, 395

encoding rules, 398-99

provably secure schemes, 392, 395, 397

Rabin's scheme, 394

Rabin-Williams' scheme, 394-95

redundancy, 397-98

RSA cryptosystem, 393-94

taxonomy, 395-96

unconditionally secure schemes, 397-98, 403-8

Authenticator (appended), 384-86

Automated teller machines (ATMs), and smart cards, 409, 444

Base *b* pseudoprime, 30

Basic security standards, 46

Berlekamp-Massey shift register synthesis algorithm, 81, 84

Binary additive stream ciphers, 23

Binary functions:

bent, 99

distance between, 97

generalized bent, 100

perfect nonlinear, 99

Birthday attacks, 202, 214-15, 257-58, 528, 603-4

"Black Chamber" (U. S. State Department), 5

Blahut's theorem, 77

Block cipher-based hash functions, 357-65

bidirectional message authentication code, 358-60

cipher block chaining-message authentication code, 357-58

Davies-Meyer (DM) scheme, 360-61

insecure schemes, 36 I-63

Merkle's block cipher-based hash functions, 363-64

Block ciphers, 21-22, 67

Blum integers, 275-77

Blum-Micali generator, 119-20

Boolean functions, see Binary functions

Brooks Act (PL89-306), 45

Brute-force attack, 22, 48, 526

Bulk encryption, and public key cryptography, 187

Cade cryptosystem, 517

Caesar cipher, 6-7, 21

CBC, see Cipher block chaining (CBC)

Cartesian product construction for authentication codes, 395-396

CCEP, see Commercial COMSEC Endorsement Program (CCEP)

- Cellular automata, 167
- Certificate-based key management protocols, 193-95, 226, 234
 - central issuing authority, 193-94
 - decentralized management, 194-95
 - and digital signatures, 202
 - phonebook approach to certificates, 195
- Certificates:
 - certification paths, 221-22
 - DARPA-Internet, 226-27
 - expiration/revocation, 22, 222, 228
 - ISO authentication framework, 219-24
 - issuance/distribution, 234-35
 - for key management, 193-95
 - LAN, 229-34
 - compromised/invalidated certificates, 235
 - issuance/distribution, 234-35
 - personnel identification, 41 1-14
 - pseudosignature, 589
 - use, 190
- Certified public directory (CPD), 26
- CFB, *see* Cipher feedback (CFB) mode
- Checker, and program **checkability**, 434
- Chinese **remainder** theorem, 262-63
- Chor-Rivest knapsack cryptosystem, 513-14
- Chosen-ciphertext attack, 4, 31
- Chosen-plaintext attack, 4, 31
- Chosen-text attack, 4
- Cipher:
 - block, 21
 - conventional:
 - DES, 183
 - exponentiation, 184
 - Diffie's randomized stream, 124
 - homophonic, 9
 - Maurer's randomized stream, 125-26
 - Pohlig-Hellman**, 184
 - practical** security, 20-21, 24
 - product, 21
 - provably secure, 24
 - randomized stream, 68
 - Rip van Winkle, 24, 124-125
 - stream, 22, 67-134
 - substitution, 21
 - synchronous stream, 70
 - transposition, 21
 - use of term, 384, 386
 - Vernam, 7
- Cipher block chaining (CBC), 23, 54-55, 192, 594
- Cipher feedback (CFB) mode, 54, 56, 192
 - and self-synchronous stream ciphers, 71
- Ciphertext, 4, 46, 119, 180, 213
- Ciphertext message, *see* Ciphertext
- Ciphertext-only attack, 4
- Circulant matrix, 77
- Clearing House Interbank Payments System (CHIPS), and DES, 51
- Clock-controlled shift registers, 101-6
 - feedback clock control, 105-6
 - forward clock control, 101-5
- CMOS technology, and smart cards, 575-77, 583-84
- Codebreakers** (Kahn), 4
- Cohen-Lenstra primality test, 268
- Collusion, 460
- Combination generators, 84, 86-88
 - correlation attacks, 88-92
- Commercial COMSEC Endorsement Program (CEP), 59-60
 - unresolved issues, 60
- Commitments and disputes, 340-44
- Common modulus protocol failure, 546-49
- Communication Theory of Secrecy** Systems (Shannon), 7
- Commutative** cryptosystems, 33
- Complexity-theoretic approach to stream cipher design, 115-23
 - generators, 118-23
 - notions/concepts, 115-18
- Complexity theory, as a game, 425-426
- Comprehensive Test Ban (CTB) Treaty, 618
- Computational complexity, 254
 - and cryptocomplexity, 236-39
- Computationally secure authentication schemes, 392, 395
- Computation**, classic theory, 252-54
 - computational complexity, 254
 - nondeterministic Turing machines, 254
 - Turing machines, 253-54
- Computing:
 - architectures, 25 1-52
 - quadratic sieve machine proposal, 251-52
 - relation to algorithms, 247-52
 - systolic arrays, 251
 - wavefront arrays, 251
 - modes, 248-49
 - probabilistic. theory, 255-56
- Concurrence schemes:
 - constructing, 459-69
 - definition, 460
- Conditional access system, 592-94
- Conditional entropy, II-12
- Confusion, 20-21
- Congruential generators:
 - cryptanalysis of, 523-26
 - definition, 523
 - linear-truncated congruential generators:
 - with known oarameters, 524-25*
 - with unknown parameters, 526
- Connection machine, 249
- Contact location, smart cards, 567-69
- Continued fractions, relation to linear complexity profile, 80-81
- Conventional cryptosystems, *see* Secret key cryptography
- Coppersmith algorithm, 296-303
 - and computation of discrete logarithms, 293-94
 - practical analysis, 299-303
- Coppersmith's attack on Rabin-type functions, 214-15
- Correlation attacks, 88-93
 - on combination generators, 88-92
 - on filter generators, 92-93
- Correlation-immune combiners, 46-47
- Credentials, *see* Certificates
- Cryptanalysis: A Survey Of Recent Results** (Brickell/Odlyzko), 148, 167
- Cryptanalysis, 4, 46, 115, 501-40
 - Cade cryptosystem, 517
 - complexity-theoretic approach, 68
 - congruential generators, 523-26
 - definition, 46
 - DES, 526-28
 - birthday attacks, 528
 - cryptanalytic attacks on weakened DES, 526-27
 - DES cycles, 527-28
 - structural properties, 528
 - discrete exponential cryptosystem, 521
 - fast data encipherment algorithm (FEAL), 529
 - generalized knapsack cryptosystems, 510-14
 - hardware/software support, 247-52
 - computing modes, 248-49
 - technology, 247-48
 - information-theoretic approach, 68
 - knapsack cryptosystems, 505-10
 - Luccio-Mazzone** cryptosystem, 518
 - McEliece** cryptosystem, 521-22
 - Matsumoto-Imai cryptosystem, 517
 - multiple-iterated knapsacks, 509-10
 - Okamoto-Shiraishi signature scheme, 516-17
 - Ong-Schnorr-Shamir signature schemes, 514-15
 - Rao-Nam cryptosystem, 522
 - research in, 503-4
 - RSA cryptosystem, 519-21
 - system-theoretic approach, 68
 - Tsujii-Matsumoto-Kurosama-Itoh-Fujioka** cryptosystem, 518
 - Yagisawa cryptosystem, 518
- Cryptanalyst, definition of, 181
- Cryptanalytic attack:
 - brute-force, 22
 - chosen-ciphertext, 4, 31
 - chosen-plaintext, 4
 - chosen text, 4
 - ciphertext-only, 4
 - known-plaintext, 4
 - meet-in-the-middle, 22
- Cryptanalytic principles, 75
- Cryptech (Waterloo University), 161-62
- CRYPTO conferences, 36
- Cryptogram, *see* Ciphertext
- Cryptographic checksum, 329
- Cryptography, 4, 42-322, 564-65
 - authenticity/integrity requirements, 182-83

- classical, see Cryptography, *single key*
- Data Encryption Standard (DES), 21–22, 43–64, 183
- exponentiation, 184, 216
- information-theoretic approach, 24–25
- protocols, 32–36, 543–548
- public key cryptography, x, 7, 25–32, 135–75, 185–87
- public perception of, 46–47
- secrecy requirements, 181–82
- secret key, see Cryptography, *single key*
- single key (also Secret key, classical), ix, 8–25, 183
- trends, 181
- Cryptology:
 - assumptions about, 4–5
 - history, 6–7
 - need for, 5
 - nomenclature, vii, 4–5
 - subdivisions, 4
- Cryptosystems, 181, 183
 - design criteria, 232–33
 - numeric criteria, 233
 - patent restrictions/license fees, 233, 608–9
 - security, 232–33
 - versatility, 233
 - export controls, 5, 564–65
 - protocol failures, 541–58
 - analysis, 554–57
 - classes of, 554–55
 - common modulus, 546–49
 - low-entropy, 550–51
 - notary, 544–46
 - single-key protocol failure, 552–54
 - small exponent RSA, 549–50
 - public key, 185–87
 - secret key, (also Single key, one-key, symmetric), 8
 - services provided, 180
- Cryptowriting, (also Secure writing), 591
- Cylink CIDECS-HS, 160–61
- DARPA-Internet, 224–29**
 - authentication and key exchange, 228–29
 - authentication framework, 227
 - certificates:
 - obtaining, 227–28
 - revocation of, 228
 - use of, 226–27
 - encapsulation/encoding, 225–26
 - key management, 225
 - services, 225
- Data compression, 13
- Datacryptor II, 157–58
- Data encryption:
 - and authentication, 57
 - and DES, 54–56
- Data Encryption Standard (DES), 21–22, 43–64, 149–50, 181, 183, 350, 385, 573–74
 - algorithm, 22, 50
 - authentication, using, 57
 - acceptance of, 49–54
 - applications, 54–58
 - commercial, 61–62
 - general, 54–57
 - governmental, 61–62
 - specific, 57–58
 - characteristics, 183
 - cipher-block chaining (CBC) mode, 23
 - cipher feedback (CFB) mode, 56
 - controversy over, 22, 48–49
 - cryptanalysis, 526–28
 - cryptography:
 - public perception of, 46–47
 - public's interest in, vii, 3, 54
 - cycles, 527–28
 - development, 45–48
 - electronic code book (ECB) mode, 21
 - future, 60–62
 - government use, 61
 - key length, 48
 - modes of operation:
 - cipher-block chaining, 55
 - electronic codebook, 55
 - k-bit cipher feedback, 56
 - k-bit output feedback, 56
 - new algorithms, 59–60
 - Commercial COMSEC Endorsement Program (CCEP), 59–60
 - forces for, 59
 - output feedback mode (OFB), 56
 - publication of standard, 49
 - reaffirmation, 60–61
 - S-boxes, 48–49
 - security, 183
 - standards, making organizations, 50–53
 - structural properties, 528
 - trapdoors, 48–49
 - validation and certification, 50, 53–54
- Data storage and mail systems, and DES, 57–58
- Decapitation attacks, 483–85
- Deception, and perfect authenticity, 15–16
- Deception attack, 15
- Defense Advanced Research Projects Agency (DARPA)-Internet, see DARPA-Internet
- Denelco HEP, 248
- Department of Treasury authentication of EFTs, 53
- DES, see Data Encryption Standard (DES)
- Desensitized authentication, 387
- Difference decimation sequence, 103
- Diffie-Hellman exponential key exchange, 26–27, 142–44, 188–89, 217–18
- Diffie-Hellman one-way function, 27, 31
- Diffie's randomized stream cipher, 125
- Diffusion, 20–21
 - product cipher, 21
- Digital signatures, 27–29, 138–39, 155, 166, 187, 195–99, 325–78
 - applications, 368–73
 - authentication and verification, 369–70, 373
 - computer networks, 373
 - dispute resolution, 371–72
 - distribution/validation of software, 373
 - electronic mail security, 370–71
 - public key certification, 368–69
 - secure telephone system, 372
 - and authentication, 196, 369–70, 373
 - and certificate-based systems, 202
 - commitments, 340–41
 - common features, 195
 - compared to handwritten signatures, 195–96
 - compared to zero-knowledge proofs, 166
 - disputes, 341–44
 - resolution, 341–44, 371–72
 - witnessed digital signatures, 344
 - El Carnal's signature scheme, 351–52
 - Fiat-Shamir signature scheme, 352–53
 - fundamental concepts, 328–48
 - Goldwasser-Micali-Rivest signature scheme, 353–54
 - and hash functions, 195–96, 344–48
 - initial agreement, 332–33
 - legal status, 332–33
 - Merkle's tree signature scheme, 355–56
 - methods for, 333–35
 - arbitrated signatures, 333–34
 - true signatures, 334
 - properties, 330–31
 - public key implementation, 196–99, 336
 - nonrepudiation issue, 197–98
 - proof of delivery issue, 198–99
 - Rabin's cryptoscheme, 354–55
 - RSA public key scheme, 350–51
 - schemes proposed, 196
 - signature schemes, 196
 - implementation, 350–55
 - practical use, 344–48
 - signature scheme settings, 335–40
 - composition of trapdoor permutations, 338–39
 - public key cryptography, 336
 - schemes with implicit verification functions, 339
 - schemes with probabilistic verification, 339–40
 - secret key cryptography, 337
 - signatures by tamper-resistant modules, 338
 - trapdoor signature schemes, 336–37
 - signing process, 331–32
 - techniques, 348–57
 - one-way functions, 348–50
 - using Rabin's public key cryptosystem, 354–55
 - verifying transformations, 331–32
 - witnessed, 344
- Diophantine approximation (UGSDA), 507–9
- Discrete exponential function, 26

Discrete exponentiation **cryptosystems**, 521
 Discrete Fourier transform, and linear complexity, 76-78
 Discrete logarithms, 266-68
 in fields of characteristic 2, 295-303, 311-13
 Dispute resolution, digital signatures, **341-44**
 Dissymmetrization, **591**
 Distributed computing, 248-49
 Double-iterated knapsack, 506
 Draft international standard, smart cards, 567

EEPROM technology, and smart cards, 580-81

Electronic business data interchange, and DES, 58
 Electronic **codebook (ECB)** mode, and DES, 21, 54
 Electronic funds transfer (**EFT**) and DES, 53, 58, 384-85
 Electronic mail security, based on digital signatures, 370-71
 El Gamal cryptosystem:
 compared to RSA cryptosystem, **310-16**
 arithmetic systems (choice), **315-16**
 message expansion, 315
 security comparison, 311-13
 throughput, **314-15**
 description of, 310
 in fields of characteristic 2:
 basic algorithm, 295-96
 compared to RSA, 310, 313-16
 Coppersmith algorithm, 296-97
 faster generation of Coppersmith equations, 297-98
 practical analysis of Coppersmith algorithm, 299-303
 smoothness testing of polynomials, 298-99
 solution of linear system, 299
 integer factorization, 303-10
 security, 291-92
 signature scheme, **211-12**, **351-52**, 397

Elliptic curve cryptosystems, recent work regarding, 316-18

Elliptic **curve factoring algorithm**, **309**

Encryption, **232**

Encryption Algorithm for Computer Data Protection. Federal Register, 47-48

Entitlement:
 control message (ECM), 593
 management message (**EMM**), 592

Entropy $H(X)$, definition, **11-12**

Equivocation, see Entropy $H(X)$, definition

ETA-10, 248

Euclid's algorithm, 261-62

Euler totient function, 28, 259

EUROCRYPT conferences, 36

European Open Shop Information System (**OSIS-TeleTrust**) project, 365-67

Exhaustive Cryptanalysis, see Brute-force attack

Exponential key exchange, **142-44**
 Exponential systems, mathematics of, 271-72

Exponentiation, **184**, 216, 251
 discrete exponentiation **cryptosystems**, 184, 521
 in finite fields, 349-50
 Extrinsic identifiers, **410**, 411

Factoring, see Integer factorization

Fast data encipherment algorithm (FEAL), 529

Federal Reserve System, 53, 58, **384-85**

Feedback clock-controlled shift registers, **105-6**

Feige-Fiat-Shamir Proof of Identity, 429-30

Fermat's theorem, 30, 259-60

Fiat-Shamir signature scheme, 352-53

Fiat-Shamir identification scheme, 599

Filter generators, 83-86
 correlation attacks, 92-93

Finite **fields** (Galois fields), **143**, **260-61**

 computations in, 250-51
 exponentiation in, 349-50

Finite-state machine theory, 69-70
 Forward clock control (shift register sequence generators), 101-5

Future Directions in Cryptography (Workshop, **1989**), **126**

Gallium arsenide (GaAs) technology, and cryptanalysis, 247-48

Geffe's generator, 107

General Services Administration (GSA), standards, 52

Generator (bit):

 Blum-Micah, 117, 119-20
 quadratic residue, 117, 122-23
 RSA, 118, 120-22
 Shamir, 118-19

Generator (pseudorandom number):
 Luby-Rackoff, 74
 Schnorr, 74-75
 Shamir, 118-19

Generators (keystream):

 combination, 86-88
 filter, 83-86
 system-theoretic approach, **106-15**

 Geffe's, 107
 inner product, 110-11
 knapsack, **114-15**
 multiplexer, **108-9**
 1/p, **112-13**
 Pless, 107-8
 summation, **113-14**
 threshold, **109-10**

 Wolfram's cellular automata, 111-12

Gilbert-McWilliams-Sloan authentication channel bound, 401

Goldwasser-Micali-Rivest signature scheme, **196**, 353-54

Goodman-McAuley knapsack **cryptosystem**, **512-13**

Goppa codes, 147-48

Graham-Shamir knapsack, 275

Guillou-Quisquater scheme, smart cards, 599, 605

Handwritten signatures, compared to digital signatures, 195-96

Hardware support, key management, **191-92**

Hash functions, 235, 356-68

 block cipher-based, 357-65
 bidirectional message authentication code, **358-60**

 cipher block chaining-message authentication code, 357-58

 Coppersmith's attack on Rabin-type functions, **214-15**

 Davies-Meyer (DM) scheme, 360-61

 and digital signatures, **195-99**
 examples, **213-16**

 insecure schemes, 361-63

 keyed hash functions, 347-48

 MD2 and MD4, 267-68

 Merkle's block cipher-based hash functions, 363-64

 and message digests, 199-202
 minimal requirement, 200

 and modification of message, detection of, 200

 modular-arithmetic-based hash functions, 365-67

 Jueneman's methods, 365

TeleTrust/Open shop information system method, 365-67

 relation to one-way functions, 200-201

 strong hash functions, 201-2
 uses, **196**, 200

 weak hash functions, 201-2

Homophonic:

 ciphers, 9
 substitution, **14**

How to Insure That Data Acquired to Verify Treaty Compliance Are Trustworthy (Simmons), 1.55, 387, 409, **615-30**

IBM (International Business Machines Corp.):

 cryptography program, 22, 47
 LUCIFER, 47

Ideal ciphers, 20

Ideally secure cipher system, 68

Identification Friend or Foe (IFF) systems, **138**

Identity-based schemes, 245-46
 security, 246

Impersonation attack, 14, 389-91

Implementation standards, 46

Implicit verification function schemes, and digital signatures, 339

Information authentication, 379-419

 authentication channel based on RSA cryptosystem, **411-12**

 extrinsic identifiers, **410**, **411**

 identity verification schemes, 410-14

 intrinsic identifiers, 410

 issuing authority:

 role of, 413

- Message authentication codes (*cont.*)
 smart cards, 566
- Message digest. 154. 199. 234
 discovery, 154
 and hash functions. 199-202
- Message source, 8, 386
- Method for Obtaining Digital Signatures and Public-Key Cryptosystems, A (Rivest-Shamir-Adleman).** 27
- Military authentication protocol, 86, 383-84
- Miller-Rabin primality test, 270
- Minimal polynomial, 81-82
- Minitel, 597
- MITRENET. MEMO system, 217-18
- MIT RSA board. 157
- Modes of operation (DES):
 cipher-block chaining (CBC), 55
 electronic codebook (ECB), 55
 k-bit cipher feedback (CFB), 56
 k-bit output feedback (OFB), 56
- Modular arithmetic, 256-60
 Euler-Fermat theorem, 259-60
 Euler totient function, 259
- Modular-arithmetic-based hash functions, 365-67
- Multioracle version, instance-hiding schemes, 434
- Multiple-iterated knapsacks. 509
- Multiplexer generator, 108-9
- Multiprover interactive protocols, 428-29
- Multisignature schemes. smart cards, 605-7
- National Bureau of Standards (NBS), also National Institute of Standards and Technology (NIST), 22, 45-50, 52-53, 373, 574**
 Data Encryption Standard. 53
 DES validations, 50
 Institute for Computer Sciences and Technology (ICST), 45
 standard for computer data authentication, 57
 standard for password usage, 57
 National Communications System (NCS), standards, 52
 National institute of Standards and Technology (NIST), see National Bureau of Standards (NBS)
 National Security Agency (NSA), 6, 22, 49, 53, 59, 149, 383, 574
 Secure Telephone Unit (STU-II and STU-III). 158-60
 NBS, see National Bureau of Standards (NBS)
- New Directions in Cryptography (Diffie-Hellman), 7, 25, 142, 146, 330**
- Niederreiter cryptosystem, 51 1-12
- Nomenclature, cryptology, 4-5
- Nondeterministic (NP) completeness. 31-32, 425
- Nondeterministic Turing machines, 254
- Nonlinearity criteria of Boolean functions. 93-101
- Meier-Staffelbach framework for. 97-99
 and memory. 96
 perfect nonlinear (bent) functions, 100-101
- Nonrepudiation of origination, 180, 197-98
- Nonvolatile programmable memory (NVM), in smart cards. 577-80
- Notary protocol failure, 544-46
- NP-hard problem, 32
- NSA. see National Security Agency (NSA)
- Nuclear Regulatory Commission (NRC), 618
- Number field sieve, 308-10, 520
- Okamoto-Shiraishi signature scheme, 516-17**
- 1/p generator, 112-13
- One-key cryptosystems, see Secret key cryptography
- One-person interactive protocol, 426-27
- One-time pad, 10, 34, 73
- One-way functions, 25-28, 31-32, 138-39, 201, 348-50, 439
 DES. 350
 exponential modulo $n = pq$, 349
 exponentiation in finite field, 349-50
 knapsack function, 350
 multiplication of two large primes. 348-49
 relation to hash functions, 200-201
 squaring modulo n , 350
- Ong-Schnorr-Shamir (OSS) signature scheme, 514-15
 quadratic, cryptanalysis of, 515
- Open cryptologic research, 5-6
- Oracle, instance-hiding, 434
- Output feedback (OFB) mode, 54, 56
- Parallel computing, 248-49**
 Parameterized hash functions, 347-48
 Parity check code, 328-29
 Percentage redundancy, 13
 Perfect authenticity, 15-16, 18
 Perfect keystream generator, 68, 115
 Perfectly secure cipher system, 68
 Perfect secrecy. IO- 12
 key requirements for, I I- 12
 with probability I, 25
 Periodic sequences, 81-83
 functions of, 83-88
 products of, 82-83
 PERM function, 430-431
 Personal identification number (PIN), smart cards, 191, 410, 444, 566, 587, 589
 Personnel identity verification. 154-57, 409-13
 PIN, see Personal identification number
- Pieprzyk knapsack cryptosystem, 5 13
- Plaintext, 4, 46, 180, 213
- Pless generator, 107-8
- Point of sale records, 413-16
- Practical security, 10, 24
- Prescientific cryptology, era of, 6
- Primality testing, 163, 268-70
- Cohen-Lenstra, 268
 Lehman's test, 270
 Miller-Rabin test, 270
 Solovay-Strassen test, 269
 strong pseudoprime, 163
- Primitive element, 26
- Primitive roots, 266-68
- Private randomization, 8-9
- Probabilistic algorithms, 238
- Probabilistic computing, theory of, 255-56
- Probabilistic encryption, 244-45
- Probabilistic verification schemes, and digital signatures, 339-40
- Probability of successful:
 deception, 15
 impersonation, 14-15
 substitution, 15
- Processor/memory pairs, connecting, 249
- Product cipher, 21
- Program checkability, 426, 434
- Programmable active memory (PAM), 314
- Proofs of identity, 4 14- 16, 429-3 1
- Protocol:
 Arthur-Merlin, 428-429
 cryptographic, 32-36, 543-544
 definition, 3, 543-44
 interactive proof systems/zero-knowledge, 423-40
 key distribution, 33
 Ingemarsson-Simmons, 479-483
 mental poker, 35
 notary, 544-546
 Shamir's three-pass, 33-35
 shared secret/shared control schemes, 44 I-97
 strict avalanche criterion, 100-1
 U. S. Military authentication, 383-84
- Protocol failures, 543-58
 analysis, 554-57
 classes of, 554-55
common modulus (RSA), 546-49
 low-entropy, 550-5 I
 notary, 54446
 single key. 552-54
 small exponent (RSA), 549-50
- Provably secure authentication schemes, 392
- Provably secure cryptographic schemes, 24, 392, 395
 based on public key cryptographic algorithms, 397
- Pseudorandom number generator, see Generator (pseudorandom number)
- Public components distribution scheme (public key), 189-92
 certificates, use of, 190
 component pairs, generation/storage of, 191
 hardware support for key management, 191-92
- Public key cryptography and cryptosystems, 7, 25-32, 135-75, 185-87, 203-12, 291-318, 336
 algorithms/architectures, 247-52

- application/implementation, 154–62, 186–87, 217–29
 - AT&T link encryptors, 157
 - Cryptech (Waterloo Univ.), 161–62
 - Cylink CIDECS-HS, 160–61
 - DARPA-Internet, 224–29
 - Integrated Services Digital Network (ISDN), 218–19
 - ISO authentication framework, 2 19–24
 - LAN implementation, proposal for, 229–35
 - MITRENET, 217–18
 - MIT RSA board, 156–57
 - Racal-Milgo Datacryptor II, 157–58
 - Sandia 336-bit RSA board, 154–56**
 - Secure Telephone Unit (STU-II, STU-III), 158–60
- benefits, 387
- categories, 203
- certificate-based key management protocols, 193–95
- digital signatures, 27–29, 138–39, 155, 166, 187, 195–99, 336
- early responses to, 149–54
 - key management, 151–54
- El Gamal signature scheme, 211–12
- exponential key exchange, 142–44
- first application, 154–55, 412–13
- future, 166–68
- initial discoveries, 137–42
 - Merkle's puzzles, 140–42, 143
- key distribution, 137
- key distribution center (KDC), 138, 151–52
- key management, 187–95
 - hardware support, 191–92
 - public component distributions scheme, 189–92
 - public distribution of secret keys, 188–89
 - secret key management, 188
- knapsacks, fall of, 148–49
- knapsack systems, 209–11
- limitations, 187
- McEliece coding scheme, 147–48, 166**
- mathematical/computational aspects, 235–39
- modifications of Diffie-Hellman model, 243–46
 - identity-based systems, 245–56
- probabilistic encryption, 244–45**
- one-way function, 25–26, 138–39
- primality testing, 163, 268–70
- proof of security, 504
- research directions, 164–66
- Rivest-Shamir-Adleman public key cryptosystem, 27–31, 145–47, 204–9
 - secrecy and authenticity, 185–86
 - secret key distribution, 192–93
 - trapdoor knapsacks, 144–45
 - trapdoor one-way function, 25–26, 28, 139
- Public randomizer, 8
- Quadratic congruential hash functions, 215–16**
- Quadratic OSS signature scheme, cryptanalysis of, 5 15
- Quadratic residue generator, 122–23
- Quadratic residues modulo a prime, 264–65
- Quadratic residuosity modulo a composite, 245, 272–77
 - Jacobi symbol, 273–74
 - quadratic residues, characterizing, 272–73
 - quadratic residuosity and Blum integers, 275–77
- Quadratic residuosity modulo a prime, 266
- Quadratic sieve factoring algorithm, 207, 250
 - outline, 303–4
 - practical analysis, 304–8
- Quadratic sieve machine, proposal for, 25 1–52
- Quantitative criteria for cryptosystems, 233**
- Querier, and instance-hiding, 434
- Rabin's public key cryptosystem, digital signatures using, 354–55**
- Rabin-type functions.
 - Coppersmith's attack on, 214–15
- Rabin-Williams' variant of the RSA system, 3 1, 394–95
- Racal-Milgo Datacryptor II, 157–58**
- "Random cipher," 12–13
- Randomization, cryptographic, 9
- Randomized stream ciphers, 24, 68–69, 123–36
 - Diffie's randomized stream cipher, 125
 - Maurer's randomized stream cipher, 125–26
- Rao-Nam cryptosystem, 522
- Random sequences, 80–8 1
- Receipts, verifiable, 414–16
- RECOVER, 618
- Redundancy, and authentication schemes, 397–98
- Replay attack, 230
- Repudiation, 23 1
- Rip van Winkle cipher, 124–25
- Resolution of Disputes, 341–44
- Rivest-Shamir-Adleman (RSA)
 - public key cryptosystem, 27–31, 49, 115, 145–47, 204–9, 519–21, 393–94
 - compared to El Carnal cryptosystem, 291–322
 - factoring as the basis of security, 207–8
 - implementation, 205–6, 2 16–17
 - low-exponent versions, 208–9
 - mathematics, 27 1–72
 - RSA chips:
 - design considerations, 2 16–17
 - proposed design, 217
 - RSA generators, 120–22
 - RSA public key scheme, 204–9, 350–5 1
 - RSA **trapdoor** one-way function, 28–31
 - security, 206–8, 291–92, 625
 - timings, 246
 - variations, 52 1
- RSA cryptosystem, see **Rivest-Shamir-Adleman (RSA)**
- public key cryptosystem
- Running-key generator (RKG), 23–24
- Sandia National Laboratories, 154–56, 412–13, 617–30**
 - authentication channel, availability of, 623
 - authentication with arbitration, 562–69
 - first application of public key cryptography, 154–55, 412–13
 - message authentication without **secrecv**, 622
 - personnel identity verification, 154–55, 412–13
 - public key devices:
 - low-speed chip**, 156
 - technology development for, 154–56
 - 336-bit RSA board, 154–56
 - unmanned seismic monitoring system, 619–22
- S-boxes, 48–49
- Scramblers, 71–72
- Secrecy:
 - definition, 180
 - and infeasibility of message decryption, 182
 - requirements, 181–82
- Secret cryptologic research, 5–6
- Secret key cryptography, 8–25, 337–38
 - authenticity and deception, 14–20
 - commutative property, system with, 33–34
 - Data Encryption Standard (DES), 21–22, 183
 - diffusion/confusion, 20–21
 - and digital signatures, 337–38
 - imperfect cipher, breaking, 12–14
 - model/notation, 8–9
 - perfect secrecy, 10–12
 - practical security, 20
 - secure channel, 8
 - security, 9–10
 - stream ciphers, 22–24
 - subdivisions, 67
- Secret key distribution:
 - key exchange protocol, 192–93
- Secret key generation, LAN, 234
- Secret keys, 4, 139, 181, 192
- Secret sharing, see **Shared secret schemes**
- Secure telephone system, and digital signatures, 372
- Secure Telephone Unit (STU-II and STU-III), 158–60, 371–72
- Secure writing, see **Cryptowriting**
- Security, 232–33
 - future, 62
 - identity-based systems, 246
 - mechanisms, 231–32
 - perfect, 68, 72
 - practical, 10
 - theoretical, 9
 - threats, 230–3 1
- Security standards development, 45–46
- NBS-NSA-IBM roles, 47–48

- Security threats:
 - interception of data, 230
 - manipulation, 230-3 I
 - masquerade, 230
 - replay, 230
 - repudiation, 23 I
 - Self-programmable one-chip micro-computer (SPOM), and smart cards, 582-85
 - Self-synchronous stream ciphers:
 - and cipher feedback mode, 71
 - and scramblers, 7 I-72
 - Semi-invertible secret key algorithm, smart cards, 590
 - Sequences, 80-83
 - periodic sequences, 8 I-83
 - Shamir's pseudorandom number generator, 118-19
 - Shamir's three-pass protocol, 33-35
 - Shannon's secrecy bound, 12
 - Shared secret schemes, 165, 441-97
 - autocratic schemes, 479
 - Blakley's scheme, 445, 447-53, 464
 - concurrency schemes:
 - characterization of classes of, 461-63
 - constructing, 459-69
 - definition, 460
 - multilevel and multipart schemes, 464-66, 483-88
 - unanimous consent schemes, 460-66
 - decapitation attacks, 483-85
 - democratic schemes, 479-83
 - and encryption/decryption, 443-44
 - general models, 450-59
 - geometry of, 469-77
 - ideal (definition), 447
 - indicators/domains, 456
 - key distribution via, 483-88
 - monotone schemes, 460
 - mutually distrustful participants,
 - general protocol for, 479-80
 - perfect (definition), 446
 - setting up, 478-83
 - shares (also shadows) definition, 445
 - Shamir's scheme, 445-47, 450-5 I
 - Simmons' scheme, 455-59
 - threshold schemes, 445-50
 - Shift registers:
 - alternating step generator, 103-4
 - cascade, 104-6
 - clock controlled, 101-6
 - forward clock control, 101-3
 - Signature, 232
 - Signatures using tamper-resistant modules (TRMs), 238
 - Simmons' authentication channel capacity, 406-7
 - Simmons' model for shared secret schemes, 455-59
 - Simmons' theory of authentication, 14-20, 381-419
 - Single-chip microcomputer, in smart cards, 565
 - Single key protocol failure, 552-54
 - Small exponent protocol failure, 549-50
 - Smart Card: A Standardized Security Device Dedicated to Public Cryptology** (Guillou-Quisquater-Ugon), 409
 - Smart cards, 234, 561-613
 - card authentication, 597-608
 - multisignature schemes, 605-7
 - new signatures, 603-5
 - public key algorithms, 598-99
 - zero-knowledge techniques, 599-603
 - definition, 563, 565
 - future evolution, 607-8
 - general** devices, initialization of automatic processes in, 572
 - history of, 563-65
 - MCU in, 565
 - message authentication codes (MACs), 566, 594
 - operations of, 565-66
 - personal identification numbers (PINs), 566, 587, 589
 - physical/logical security, 565
 - pseudosignature, 589
 - secret key algorithms, 590-91
 - security, 585-97
 - cardholder identification, 587-88, 599-603
 - chip security features/card life cycle, 585-87
 - conditional access to audio-visual services, 592-94
 - by control of algorithm execution in mask KC2, 594
 - cryptowriting/dissymmetrization**, 591
 - dynamic authentication by security modules, 588-89
 - invertible secret key algorithms, 590-91
 - logical architecture, 97
 - mechanisms/techniques, 566
 - secret key one-way function, 588
 - semi-invertible secret key algorithm, 590
- standardization, 566-75
 - of contact location, 567-69
 - at European level, 573
 - of file architecture/related security, 572
 - in ISO outside WG4, 572-73
 - of physical characteristics, 567
 - of security techniques in ISO, 573-75
 - of signals/protocols, 570-7 I
 - of smart card interpretive language (SCIL), 572
- technology, 575-85
 - integrated circuit card family, 581-82
 - nonvolatile programmable memory (NVM), 577-80
 - self-programmable one-chip microcomputer (SPOM), 582-85
 - transaction process, 564, 570
 - and VLSI chip technology, 563-64
- Snefru algorithm, 368
- Solovay-Strassen primality test, 30, 269
- Source encoding, 386
- Square roots modulo a prime, 265-66
- Squaring modulo n , 350
- Standardization, smart cards, 566-75
- Standards, functional classification, 46
- Strategic Arms Limitation Treaty (SALT), 619
- Statistical zero-knowledge, 428
- Stop-and-go generator, 102-3
- Stream ciphers, 22-24, 67-134
 - binary additive stream ciphers, 23
 - compared to block ciphers, 23-24
 - complexity-theoretic approach, 68
 - generators, 118-23
 - notions/concepts, 115-18
 - definition, 67
 - design approaches, 67-69
 - goal, 67
 - information-theoretic approach, 68, 72-75
 - local randomization, 73-75
 - randomized stream ciphers, 68-69, 123-26
 - system-theoretic** approach, 68, 75-I 15
 - clock-controlled shift registers, 101-6
 - correlation attacks, 88-93
 - generators, 106-15
 - nonlinearity criteria, 93-101
 - period and linear complexity of sequences, 80-83
 - period sequence functions, 83-88
 - transform techniques, 76-80
 - terminology/modes of operations, 69-72
 - self-synchronous stream ciphers and scramblers, 71-72
 - synchronous stream ciphers and pseudorandom generators, 70-71
- String, classic theory of computation, 252
- Strong hash functions, 201-2
- Strong pseudoprime tests, 163
- STU-II and STU-III, 158-60
- Substitution attack, 15, 389-91
- Substitution cipher, definition, 21
- Summation generator, 113-14
- Super increasing sequences, 144-45
- Symmetric cryptosystems, see Secret key cryptography
- Synchronous stream ciphers:
 - error propagation, 7 I
 - keystream generation, 70
 - and pseudorandom generators, 70-7 I
 - self-synchronizing feature, 72
- System-theoretic approach to stream cipher design, 68, 75-I 15
- Systolic arrays, 25 I

Tamper-resistant modules, and digital signature& 338

Téléétel, 397

Test Ban Treaty Verification, 155–56

Theoretical security, 9–10, 18

Threshold generator, 109–10

Threshold shared secret schemes, 445–50

Timestamps, 198, 235

Totient (function), see Euler totient function

Transform techniques, 76–80

algebraic normal form transform, 79–80

Blahut's theorem, 77

discrete Fourier transform and linear complexity, 76–78

Walsh transform and Boolean functions, 78–79

Transposition cipher, definition, 2 I

Trapdoor-knapsack public key cryptosystem, 5, 32, 144–45, 209–10

Trapdoor one-way function, 25–26, 28, 139

Trapdoor permutations, composition of, 338–39

Trapdoors, 48–49

Trapdoor signature schemes, 236–37

Treaty verification, 617–630
in the presence of deceit, 627–629

with arbitration, 625–627

without secrecy, 622–625

True signatures, 195–96, 334

Trust as a parameter, 443–445

Trusted key distribution center (TKDC), 33

Tsujii–Matsumoto–Kurosama–Itoh–Fujioka cryptosystem, 518

Turing machines, 253–54, 255
nondeterministic, 254

Uncertainty:

definition, I I

Unconditionally secure authentication schemes, 397–98, 403–8

Unconditionally secure cryptosystems, 73

Unicity distance, 12, 20, 73

U. S. digital standard (DSS), proposed (1991), 373

U. S. export/import controls, cryptographic devices, 5

U. S. National Bureau of Standards (NBS), see National Bureau of Standards (NBS)

Unusually good simultaneous diophantine approximation (UGSDA), 507–9

Vernam's cipher, 7

Vernam's system, modulo L , IO

Von Neumann model, computing, 248

Walsh transform, 78–79

Wavefront arrays, 25 I

Weakened DES-like cryptosystems, cryptanalytic-attacks on, 526–27

Weak hash functions, 201–2

Witnessed digital signatures, 344

Wolfram's cellular automata generator, I I I–12

Work characteristic of ciphers, 20

X.509 hash function, 347

Yagisawa cryptosystem, 518

Zero j-invariant, 317

Zero-knowledge, definition of, 425

Zero-knowledge proofs, 166, 239–43, 423–40

arguments, 426, 434

Arthur-Merlin protocol, 428

complexity classes, 438–39

definition, 239, 426–29

examples, 429–3 I

proofs for the PERM function, 430–3 I

proofs of identity, 429–30

instance-hiding schemes, 426, 234–35

interactive proof systems, 426–29

language-recognition power, 431–33

multi-prover interactive protocols, 428–29

one-prover interactive proof system, 427–28

open problems, 435–36

program checkability, 426, 434

simulator, 428

Zero knowledge techniques applied to smart cards, 599–603

Zero Power Plutonium Reactor, identity verification scheme, 412–14



Editor's Biography

Gustavus J. Simmons received the Ph.D. degree in mathematics from the University of New Mexico, Albuquerque. He is Senior Fellow for National Security Studies at the Sandia National Laboratories, Albuquerque, NM. Earlier he was Manager of the Applied Mathematics Department and Supervisor of one of two divisions at Sandia devoted to the command and control of nuclear weapons. In all these positions he has been primarily concerned with questions of information integrity arising in national security: command and control of nuclear weapons, verification of compliance with various arms control treaties, individual

identity verification at sensitive facilities, etc. His research has been primarily in combinatorics and graph theory and in the applied topics of information theory and cryptography, especially as applied to message authentication and systems design to achieve this function. His current research is aimed at devising information dependent protocols whose function can be trusted even though no specific inputs or participants can be. The need for such protocols arises frequently in questions of national security ranging from simple two-man control schemes for nuclear weapons to arbitrarily complex concurrence schemes for the initiation of various treaty controlled actions. Within the defense community he has pioneered in applying these techniques to the command and control of nuclear weapons.

Dr. Simmons was the recipient of the U.S. Government's E. O. Lawrence Award in 1986. The accompanying citation reads in part: "In the political climate that has emerged in the nuclear era, increasing importance in the design of nuclear weapons must be placed on control features including verification, authentication, and positive use control. This is the first time that achievements in this field, of vital importance to national security, have been recognized by a Lawrence Award. . . ." In that same year, he also received the Department of Energy Weapons Recognition of Excellence Award for "Contributions to the Command and Control of Nuclear Weapons."

Dr. Simmons was awarded an honorary Doctorate of Technology in May 1991 by the University of Lund (Sweden) in recognition of his contributions to communications science and to the field of information integrity. The diploma cites him as "The Father of Authentication Theory."

Dr. Simmons has published more than 120 papers and books, many of which are devoted to the analysis and application of asymmetric encryption techniques or to message authentication, and has been granted several patents for inventions in this area. At the invitation of the editors, he wrote the section on cryptology that appears in the 16th edition of the Encyclopaedia Britannica. He is an editor for *Journal of Cryptology*, *Ars Combinatoria*, and *Codes, Designs and Cryptography*.