

Bibliography	413
Index.....	428

Bibliography

- [ACGS88] W. ALEXI, B. CHOR, O. GOLDREICH AND C. P. SCHNORR. RSA and Rabin functions: certain parts are as hard as the whole. *SIAM Journal on Computing*, **17** (1988), 194–209.
- [AN91] H. ANTON. *Elementary Linear Algebra* (Sixth Edition). John Wiley and Sons, 1991.
- [BHS93] D. BAYER, S. HABER AND W. S. STORNETTA. Improving the efficiency and reliability of digital time-stamping. In *Sequences II, Methods in Communication, Security, and Computer Science*, pages 329–334. Springer-Verlag, 1993.
- [BB88] P. BEAUCHEMIN AND G. BRASSARD. A generalization of Hellman's extension to Shannon's approach to cryptography. *Journal of Cryptology*, **1** (1988), 129–131.
- [BBCGP88] P. BEAUCHEMIN, G. BRASSARD, C. CRÉPEAU, C. GOUTIER AND C. POMERANCE. The generation of random numbers that are probably prime. *Journal of Cryptology*, **1** (1988), 53–64.
- [BC94] A. BEIMEL AND B. CHOR. Interaction in key distribution schemes. *Lecture Notes in Computer Science*, **773** (1994), 444–455. (Advances in Cryptology – CRYPTO '93.)
- [BP82] H. BEKER AND F. PIPER. *Cipher Systems, The Protection of Communications*. John Wiley and Sons, 1982.
- [BL90] J. BENALOH AND J. LEICHTER. Generalized secret sharing and monotone functions. *Lecture Notes in Computer Science*, **403** (1990), 27–35. (Advances in Cryptology – CRYPTO '88.)
- [BE83] T. BETH (ED.) *Cryptography Proceedings, 1982. Lecture Notes in Computer Science*, vol. 149, Springer-Verlag, 1983.
- [BCI85] T. BETH, N. COT AND I. INGEMARSSON (EDS.) *Advances in Cryptology: Proceedings of EUROCRYPT '84. Lecture Notes in Computer Science*, vol. 209, Springer-Verlag, 1985.
- [BJL85] T. BETH, D. JUNGnickel, AND H. LENZ. *Design Theory*. Bibliographisches Institut, Zurich, 1985.

- [BE94] A. BEUTELSPACHER. *Cryptology*. Mathematical Association of America, 1994.
- [BS91] E. BIHAM AND A. SHAMIR. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, **4** (1991), 3–72.
- [BS93] E. BIHAM AND A. SHAMIR. *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, 1993.
- [BS93A] E. BIHAM AND A. SHAMIR. Differential cryptanalysis of the full 16-round DES. *Lecture Notes in Computer Science*, **740** (1993), 494–502. (Advances in Cryptology – CRYPTO '92.)
- [BL79] G. R. BLAKLEY. Safeguarding cryptographic keys. *AFIPS Conference Proceedings*, **48** (1979), 313–317.
- [BC85] G. R. BLAKLEY AND D. CHAUM (EDS.) *Advances in Cryptology: Proceedings of CRYPTO '84. Lecture Notes in Computer Science*, vol. 196, Springer-Verlag, 1985.
- [BL85] R. BLOM. An optimal class of symmetric key generation schemes. *Lecture Notes in Computer Science*, **209** (1985), 335–338. (Advances in Cryptology – EUROCRYPT '84.)
- [BBS86] L. BLUM, M. BLUM AND M. SHUB. A simple unpredictable random number generator. *SIAM Journal on Computing*, **15** (1986), 364–383.
- [BL82] M. BLUM. Coin flipping by telephone: a protocol for solving impossible problems. In *24th IEEE Spring Computer Conference*, pages 133–137. IEEE Press, 1982.
- [BG85] M. BLUM AND S. GOLDWASSER. An efficient probabilistic public-key cryptosystem that hides all partial information. *Lecture Notes in Computer Science*, **196** (1985), 289–302. (Advances in Cryptology – CRYPTO '84.)
- [BM84] M. BLUM AND S. MICALI. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM Journal on Computing*, **13** (1984), 850–864.
- [Bo89] J. BOYAR. Inferring sequences produced by pseudo-random number generators. *Journal of Association for Computing Machinery*, **36** (1989), 129–141.
- [BDSV93] C. BLUNDO, A. DE SANTIS, D. R. STINSON, AND U. VACCARO. Graph decompositions and secret sharing schemes. *Lecture Notes in Computer Science*, **658** (1993), 1–24. (Advances in Cryptology – EUROCRYPT '92.)
- [BDSHKVY93] C. BLUNDO, A. DE SANTIS, A. HERZBERG, S. KUTTEN, U. VACCARO AND M. YUNG. Perfectly-secure key distribution for dynamic conferences. *Lecture Notes in Computer Science*, **740**

- (1993), 471–486. (Advances in Cryptology – CRYPTO '92.)
- [BC93] J. N. E. BOS AND D. CHAUM. Provably unforgeable signatures. *Lecture Notes in Computer Science*, **740** (1993), 1–14. (Advances in Cryptology – CRYPTO '92.)
- [BR88] G. BRASSARD. *Modern Cryptology – A Tutorial*. *Lecture Notes in Computer Science*, vol. 325, Springer-Verlag, 1988.
- [BR90] G. BRASSARD (ED.) *Advances in Cryptology – CRYPTO '89 Proceedings*. *Lecture Notes in Computer Science*, vol. 435, Springer-Verlag, 1990.
- [BB88A] G. BRASSARD AND P. BRATLEY. *Algorithmics, Theory and Practice*. Prentice Hall, 1988.
- [BCC88] G. BRASSARD, D. CHAUM AND C. CRÉPEAU. Minimum disclosure proofs of knowledge. *Journal of Computer and Systems Science*, **37** (1988), 156–189.
- [BC90] G. BRASSARD AND C. CRÉPEAU. Sorting out zero-knowledge. *Lecture Notes in Computer Science*, **434** (1990), 181–191. (Advances in Cryptology – EUROCRYPT '89.)
- [BR89] D. M. BRESSOUD. *Factorization and Primality Testing*. Springer-Verlag, 1989.
- [BR85] E. F. BRICKELL. Breaking iterated knapsacks. *Lecture Notes in Computer Science*, **218** (1986), 342–358. (Advances in Cryptology – CRYPTO '85.)
- [BR89A] E. F. BRICKELL. Some ideal secret sharing schemes. *Journal of Combinatorial Mathematics and Combinatorial Computing*, **9** (1989), 105–113.
- [BR93] E. F. BRICKELL (ED.) *Advances in Cryptology – CRYPTO '92 Proceedings*. *Lecture Notes in Computer Science*, vol. 740, Springer-Verlag, 1993.
- [BD91] E. F. BRICKELL AND D. M. DAVENPORT. On the classification of ideal secret sharing schemes. *Journal of Cryptology*, **4** (1991), 123–134.
- [BM92] E. F. BRICKELL AND K. S. MCCURLEY. An interactive identification scheme based on discrete logarithms and factoring. *Journal of Cryptology*, **5** (1992), 29–39.
- [BMP87] E. F. BRICKELL, J. H. MOORE AND M. R. PURTILL. Structure in the *S*-boxes of DES. *Lecture Notes in Computer Science*, **263** (1987), 3–8. (Advances in Cryptology – CRYPTO '86.)
- [BO92] E. F. BRICKELL AND A. M. ODLYZKO. Cryptanalysis, a survey of recent results. In *Contemporary Cryptology, The Science of Information Integrity*, pages 501–540. IEEE Press, 1992.

- [BS92] E. F. BRICKELL AND D. R. STINSON. Some improved bounds on the information rate of perfect secret sharing schemes. *Journal of Cryptology*, **5** (1992), 153–166.
- [BKPS90] L. BROWN, M. KWAN, J. PIEPRZYK AND J. SEBERRY. LOKI – A cryptographic primitive for authentication and secrecy applications. *Lecture Notes in Computer Science*, **453** (1990), 229–236. (Advances in Cryptology – AUSCRYPT '90.)
- [BDB92] M. BURMESTER, Y. DESMEDT AND T. BETH. Efficient zero-knowledge identification schemes for smart cards. *The Computer Journal*, **35** (1992), 21–29.
- [CDGV93] R. M. CAPOCELLI, A. DE SANTIS, L. GARGANO, AND U. VACCARO. On the size of shares for secret sharing schemes. *Journal of Cryptology*, **6** (1993), 157–167.
- [CH95] F. CHABAUD. On the security of some cryptosystems based on error-correcting codes. *Lecture Notes in Computer Science*, to appear. (Advances in Cryptology – EUROCRYPT '94.)
- [CH84] D. CHAUM (ED.) *Advances in Cryptology: Proceedings of CRYPTO '83*. Plenum Press, 1984.
- [CP88] D. CHAUM AND W. L. PRICE (EDS.) *Advances in Cryptology – EUROCRYPT '87 Proceedings. Lecture Notes in Computer Science*, vol. 304, Springer-Verlag, 1988.
- [CRS83] D. CHAUM, R. L. RIVEST AND A. T. SHERMAN (EDS.) *Advances in Cryptology: Proceedings of CRYPTO '82*. Plenum Press, 1983.
- [CvA90] D. CHAUM AND H. VAN ANTWERPEN. Undeniable signatures. *Lecture Notes in Computer Science*, **435** (1990), 212–216. (Advances in Cryptology – CRYPTO '89.)
- [CvHP92] D. CHAUM, E. VAN HEIJST AND B. PFITZMANN. Cryptographically strong undeniable signatures, unconditionally secure for the signer. *Lecture Notes in Computer Science*, **576** (1992), 470–484. (Advances in Cryptology – CRYPTO '91.)
- [CR88] B. CHOR AND R. L. RIVEST. A knapsack-type public key cryptosystem based on arithmetic in finite fields. *IEEE Transactions on Information Theory*, **45** (1988), 901–909.
- [CKM94] D. COPPERSMITH, H. KRAWCZYK AND Y. MANSOUR. The shrinking generator. *Lecture Notes in Computer Science*, **773** (1994), 22–39. (Advances in Cryptology – CRYPTO '93.)
- [CSV94] D. COPPERSMITH, J. STERN AND S. VAUDENAY. Attacks on the birational permutation signature schemes. *Lecture Notes in Computer Science*, **773** (1994), 435–443. (Advances in Cryptology – CRYPTO '93.)

- [CW91] T. W. CUSICK AND M. C. WOOD. The REDOC-II cryptosystem. *Lecture Notes in Computer Science*, **537** (1991), 545–563. (Advances in Cryptology – CRYPTO '90.)
- [DA90] I. B. DÅMGARD. A design principle for hash functions. *Lecture Notes in Computer Science*, **435** (1990), 416–427. (Advances in Cryptology – CRYPTO '89.)
- [DA91] I. B. DÅMGARD (ED.) *Advances in Cryptology – EUROCRYPT '90 Proceedings. Lecture Notes in Computer Science*, vol. 473, Springer-Verlag, 1991.
- [DLP93] I. DÅMGARD, P. LANDROCK AND C. POMERANCE. Average case error estimates for the strong probable prime test. *Mathematics of Computation*, **61** (1993), 177–194.
- [DA91A] D. W. DAVIES (ED.) *Advances in Cryptology – EUROCRYPT '91 Proceedings. Lecture Notes in Computer Science*, vol. 547, Springer-Verlag, 1991.
- [DE84] J. M. DELAURENTIS. A further weakness in the common modulus protocol for the RSA cryptosystem. *Cryptologia*, **8** (1984), 253–259.
- [DBB92] B. DEN BOER AND A. BOSSALAERS. An attack on the last two rounds of MD4. *Lecture Notes in Computer Science*, **576** (1992), 194–203. (Advances in Cryptology – CRYPTO '91.)
- [DE82] D. E. R. DENNING. *Cryptography and Data Security*. Addison-Wesley, 1982.
- [DE94] Y. G. DESMEDT (ED.) *Advances in Cryptology – CRYPTO '94 Proceedings. Lecture Notes in Computer Science*, vol. 839, Springer-Verlag, 1994.
- [DWQ93] D. DE WALEFFE AND J.-J. QUISQUATER. Better login protocols for computer networks. *Lecture Notes in Computer Science*, **741** (1993), 50–70. (Computer Security and Industrial Cryptography, State of the Art and Evolution, ESAT Course, May 1991.)
- [Di92] W. DIFFIE. The first ten years of public-key cryptography. In *Contemporary Cryptology, The Science of Information Integrity*, pages 135–175. IEEE Press, 1992.
- [DH76] W. DIFFIE AND M. E. HELLMAN. Multiuser cryptographic techniques. *AFIPS Conference Proceedings*, **45** (1976), 109–112.
- [DH76A] W. DIFFIE AND M. E. HELLMAN. New directions in cryptography. *IEEE Transactions on Information Theory*, **22** (1976), 644–654.
- [DVW92] W. DIFFIE, P. C. VAN OORSCHOT AND M. J. WIENER. Authen-

- tication and authenticated key exchanges. *Designs, Codes and Cryptography*, **2** (1992), 107–125.
- [EB93] H. EBERLE. A high-speed DES implementation for network applications. *Lecture Notes in Computer Science*, **740** (1993), 527–545. (Advances in Cryptology – CRYPTO '92.)
- [EL85] T. ELGAMAL. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, **31** (1985), 469–472.
- [EAKMM86] D. ESTES, L. M. ADLEMAN, K. KOMPPELLA, K. S. MCCURLEY AND G. L. MILLER. Breaking the Ong-Schnorr-Shamir signature schemes for quadratic number fields. *Lecture Notes in Computer Science*, **218** (1986), 3–13. (Advances in Cryptology – CRYPTO '85.)
- [FFS88] U. FEIGE, A. FIAT AND A. SHAMIR. Zero-knowledge proofs of identity. *Journal of Cryptology*, **1** (1988), 66–94.
- [Fe92] J. FEIGENBAUM (ED.) *Advances in Cryptology – CRYPTO '91 Proceedings. Lecture Notes in Computer Science*, vol. 576, Springer-Verlag, 1992.
- [Fe73] H. FEISTEL. Cryptography and computer privacy. *Scientific American*, **228**(5) (1973), 15–23.
- [FN91] A. FIAT AND M. NAOR. Rigorous time/space trade-offs for inverting functions. In *Proceedings of the 23rd Symposium on the Theory of Computing*, pages 534–541. ACM Press, 1991.
- [FS87] A. FIAT AND A. SHAMIR. How to prove yourself: practical solutions to identification and signature problems. *Lecture Notes in Computer Science*, **263** (1987), 186–194. (Advances in Cryptology – CRYPTO '86.)
- [FOM91] A. FUJIOKA, T. OKAMOTO AND S. MIYAGUCHI. ESIGN: an efficient digital signature implementation for smart cards. *Lecture Notes in Computer Science*, **547** (1991), 446–457. (Advances in Cryptology – EUROCRYPT '91.)
- [GIB91] J. K. GIBSON. Discrete logarithm hash function that is collision free and one way. *IEE Proceedings-E*, **138** (1991), 407–410.
- [GMS74] E. N. GILBERT, F. J. MACWILLIAMS AND N. J. A. SLOANE. Codes which detect deception. *Bell Systems Technical Journal*, **53** (1974), 405–424.
- [GIR91] M. GIRAULT. Self-certified public keys. *Lecture Notes in Computer Science*, **547** (1991), 490–497. (Advances in Cryptology – EUROCRYPT '91.)
- [GP91] C. M. GOLDIE AND R. G. E. PINCH. *Communication Theory*.

- Cambridge University Press, 1991.
- [GMW91] O. GOLDREICH, A. MICALI AND A. WIGDERSON. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, **38** (1991), 691–729.
- [Go90] S. GOLDWASSER (ED.) *Advances in Cryptology – CRYPTO '88 Proceedings. Lecture Notes in Computer Science*, vol. 403, Springer-Verlag, 1990.
- [GM84] S. GOLDWASSER AND A. MICALI. Probabilistic encryption. *Journal of Computer and Systems Science*, **28** (1984), 270–299.
- [GMR89] S. GOLDWASSER, S. MICALI AND C. RACKOFF. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, **18** (1989), 186–208.
- [GMT82] S. GOLDWASSER, S. MICALI AND P. TONG. Why and how to establish a common code on a public network. In *23rd Annual Symposium on the Foundations of Computer Science*, pages 134–144. IEEE Press, 1982.
- [GM93] D. M. GORDON AND K. S. MCCURLEY. Massively parallel computation of discrete logarithms. *Lecture Notes in Computer Science*, **740** (1993), 312–323. (Advances in Cryptology – CRYPTO '92.)
- [GQ88] L. C. GUILLOU AND J.-J. QUISQUATER. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. *Lecture Notes in Computer Science*, **330** (1988), 123–128. (Advances in Cryptology – EUROCRYPT '88.)
- [Gu88] C. G. GUNTHER Alternating step generators controlled by de Bruijn sequences. *Lecture Notes in Computer Science*, **304** (1988), 88–92. (Advances in Cryptology – EUROCRYPT '87.)
- [Gu88A] C. G. GUNTHER (ED.) *Advances in Cryptology – EUROCRYPT '88 Proceedings. Lecture Notes in Computer Science*, vol. 330, Springer-Verlag, 1988.
- [HS91] S. HABER AND W. S. STORNETTA. How to timestamp a digital document. *Journal of Cryptology*, **3** (1991), 99–111.
- [HSS93] J. HÅSTAD, A. W. SCHRIFT AND A. SHAMIR. The discrete logarithm modulo a composite hides $O(n)$ bits. *Journal of Computer and Systems Science*, **47** (1993), 376–404.
- [He80] M. E. HELLMAN. A cryptanalytic time-memory trade-off. *IEEE Transactions on Information Theory*, **26** (1980), 401–

- 406.
- [Hi29] L. S. HILL. Cryptography in an algebraic alphabet. *American Mathematical Monthly*, **36** (1929), 306–312.
- [He94] T. HELLESETH (ED.) *Advances in Cryptology – EUROCRYPT '93 Proceedings. Lecture Notes in Computer Science*, vol. 765, Springer-Verlag, 1994.
- [HLLPRW91] D. G. HOFFMAN, D. A. LEONARD, C. C. LINDNER, K. T. PHELPS, C. A. RODGER AND J. R. WALL. *Coding Theory, The Essentials*. Marcel Dekker, 1991.
- [IRM93] H. IMAI, R. L. RIVEST AND T. MATSUMOTO (EDS.) *Advances in Cryptology – ASIACRYPT '91 Proceedings. Lecture Notes in Computer Science*, vol. 739, Springer-Verlag, 1993.
- [ISN87] M. ITO, A. SAITO, AND T. NISHIZEKI. Secret sharing scheme realizing general access structure. *Proceedings IEEE Globecom '87*, pages 99–102, 1987.
- [Jo88] D. S. JOHNSON. The NP-completeness column: an ongoing guide. *Journal of Algorithms*, **9** (1988), 426–444.
- [KA67] D. KAHN. *The Codebreakers. The Story of Secret Writing*. Macmillan, 1967.
- [Ko87] N. KOBLITZ. *A Course in Number Theory and Cryptography*. Springer-Verlag, 1987.
- [Ko87A] N. KOBLITZ. Elliptic curve cryptosystems. *Mathematics of Computation*, **48** (1987), 203–209.
- [Ko87A] N. KOBLITZ. Elliptic curve cryptosystems. *Mathematics of Computation*, **48** (1987), 203–209.
- [KN93] J. KOHL AND C. NEUMAN. *The Kerberos Network Authentication Service*. Network Working Group Request for Comments: 1510, September 1993.
- [Ko81] A. G. KONHEIM. *Cryptography, A Primer*. John Wiley and Sons, 1981.
- [KR86] E. KRANAKIS. *Primality and Cryptography*. John Wiley and Sons, 1986.
- [LA90] J. C. LAGARIAS Pseudo-random number generators in cryptography and number theory. In *Cryptology and Computational Number Theory*, pages 115–143. American Mathematical Society, 1990.
- [LO91] B. A. LAMACCHIA AND A. M. ODLYZKO. Computation of discrete logarithms in finite fields. *Designs, Codes and Cryptography*, **1** (1991), 47–62.
- [LL93] A. K. LENSTRA AND H. W. LENSTRA, JR. (EDS.) *The Develop-*

- ment of the Number Field Sieve. Lecture Notes in Mathematics*, vol. 1554. Springer-Verlag, 1993.
- [LL90] A. K. LENSTRA AND H. W. LENSTRA, JR. Algorithms in number theory. In *Handbook of Theoretical Computer Science, Volume A: Algorithms and Complexity*, pages 673–715. Elsevier Science Publishers, 1990.
- [LN83] R. LIDL AND H. NIEDERREITER. *Finite Fields*. Addison-Wesley, 1983.
- [LW88] D. L. LONG AND A. WIGDERSON. The discrete log hides $O(\log n)$ bits. *SIAM Journal on Computing*, **17** (1988), 363–372.
- [MS77] F. J. MACWILLIAMS AND N. J. A. SLOANE. *The Theory of Error-Correcting Codes*. North-Holland, 1977.
- [MA86] J. L. MASSEY. Cryptography – a selective survey. In *Digital Communications*, pages 3–21. North-Holland, 1986.
- [MA94] M. MATSUI. Linear cryptanalysis method for DES cipher. *Lecture Notes in Computer Science*, **765** (1994), 386–397. (Advances in Cryptology – EUROCRYPT '93.)
- [MA94A] M. MATSUI. The first experimental cryptanalysis of the data encryption standard. *Lecture Notes in Computer Science*, **839** (1994), 1–11. (Advances in Cryptology – CRYPTO '94.)
- [MTI86] T. MATSUMOTO, Y. TAKASHIMA AND H. IMAI. On seeking smart public-key distribution systems. *Transactions of the IECE (Japan)*, **69** (1986), 99–106.
- [Mc90] K. MCCURLEY. The discrete logarithm problem. In *Cryptology and Computational Number Theory*, pages 49–74. American Mathematical Society, 1990.
- [Mc78] R. McELIECE. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report*, **42–44** (1978), 114–116.
- [Mc87] R. McELIECE. *Finite Fields for Computer Scientists and Engineers*. Kluwer Academic Publishers, 1987.
- [ME93] A. J. MENEZES. *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Publishers, 1993.
- [MBGMVY93] A. J. MENEZES, I. F. BLAKE, X. GAO, R. C. MULLIN, S. A. VANSTONE AND T. YAGHOUBIAN. *Applications of Finite Fields*. Kluwer Academic Publishers, 1993.
- [MOV94] A. J. MENEZES, T. OKAMOTO AND S. A. VANSTONE. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, **39** (1993), 1639–1646.
- [MV91] A. J. MENEZES AND S. A. VANSTONE (EDS.) *Advances in Cryptology*

- tology* – CRYPTO '90 Proceedings. *Lecture Notes in Computer Science*, vol. 537, Springer-Verlag, 1991.
- [MV93] A. J. MENEZES AND S. A. VANSTONE. Elliptic curve cryptosystems and their implementation. *Journal of Cryptology*, **6** (1993), 209–224.
- [ME78] R. C. MERKLE. Secure communications over insecure channels. *Communications of the ACM*, **21** (1978), 294–299.
- [ME90] R. C. MERKLE. One way hash functions and DES. *Lecture Notes in Computer Science*, **435** (1990), 428–446. (Advances in Cryptology – CRYPTO '89.)
- [ME90A] R. C. MERKLE. A fast software one-way hash function. *Journal of Cryptology*, **3** (1990), 43–58.
- [MH78] R. C. MERKLE AND M. E. HELLMAN. Hiding information and signatures in trapdoor knapsacks. *IEEE Transactions on Information Theory*, **24** (1978), 525–530.
- [MM82] C. MEYER AND S. MATYAS. *Cryptography: A New Dimension in Computer Security*. John Wiley and Sons, 1982.
- [Mi76] G. L. MILLER. Riemann's hypothesis and tests for primality. *Journal of Computer and Systems Science*, **13** (1976), 300–317.
- [Mi86] V. MILLER. Uses of elliptic curves in cryptography. *Lecture Notes in Computer Science*, **218** (1986), 417–426. (Advances in Cryptology – CRYPTO '85.)
- [MPW92] C. J. MITCHELL, F. PIPER AND P. WILD. Digital signatures. In *Contemporary Cryptology, The Science of Information Integrity*, pages 325–378. IEEE Press, 1992.
- [Mi91] S. MIYAGUCHI. The FEAL cipher family. *Lecture Notes in Computer Science*, **537** (1991), 627–638. (Advances in Cryptology – CRYPTO '90.)
- [MOI90] S. MIYAGUCHI, K. OHTA AND M. IWATA. 128-bit hash function (N -hash). *Proceedings of SECURICOM 1990*, 127–137.
- [Mo92] J. H. MOORE. Protocol failures in cryptosystems. In *Contemporary Cryptology, The Science of Information Integrity*, pages 541–558. IEEE Press, 1992.
- [NBS77] *Data Encryption Standard (DES)*. National Bureau of Standards FIPS Publication 46, 1977.
- [NBS80] *DES modes of operation*. National Bureau of Standards FIPS Publication 81, 1980.
- [NBS81] *Guidelines for implementing and using the NBS data encryption standard*. National Bureau of Standards FIPS Publication

- 74, 1981.
- [NBS85] *Computer data authentication*. National Bureau of Standards FIPS Publication 113, 1985.
- [NBS93] *Secure hash standard*. National Bureau of Standards FIPS Publication 180, 1993.
- [NBS94] *Digital signature standard*. National Bureau of Standards FIPS Publication 186, 1994.
- [Od87] A. M. ODLYZKO (ED.) *Advances in Cryptology – CRYPTO '86 Proceedings. Lecture Notes in Computer Science*, vol. 263, Springer-Verlag, 1987.
- [Ok93] T. OKAMOTO. Provably secure and practical identification schemes and corresponding signature schemes. *Lecture Notes in Computer Science*, **740** (1993), 31–53. (Advances in Cryptology – CRYPTO '92.)
- [OSS85] H. ONG, C. P. SCHNORR AND A. SHAMIR. Efficient signature schemes based on polynomial equations. *Lecture Notes in Computer Science*, **196** (1985), 37–46. (Advances in Cryptology – CRYPTO '84.)
- [PA87] W. PATTERSON. *Mathematical Cryptology for Computer Scientists and Mathematicians*. Rowman and Littlefield, 1987.
- [PE86] R. PERALTA. Simultaneous security of bits in the discrete log. *Lecture Notes in Computer Science*, **219** (1986), 62–72. (Advances in Cryptology – EUROCRYPT '85.)
- [Pi86] F. PICHLER (ED.) *Advances in Cryptology – EUROCRYPT '85 Proceedings. Lecture Notes in Computer Science*, vol. 219, Springer-Verlag, 1986.
- [PB45] R. L. PLACKETT AND J. P. BURMAN. The design of optimum multi-factorial experiments. *Biometrika*, **33** (1945), 305–325.
- [PH78] S. C. POHLIG AND M. E. HELLMAN. An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. *IEEE Transactions on Information Theory*, **24** (1978), 106–110.
- [Po88] C. POMERANCE (ED.) *Advances in Cryptology – CRYPTO '87 Proceedings. Lecture Notes in Computer Science*, vol. 293, Springer-Verlag, 1988.
- [Po90] C. POMERANCE. Factoring. In *Cryptology and Computational Number Theory*, pages 27–47. American Mathematical Society, 1990.
- [Po90A] C. POMERANCE (ED.) *Cryptology and Computational Number Theory*, American Mathematical Society, 1990.

- [PGV93] B. PRENEEL, R. GOVAERTS AND J. VANDEWALLE. Information authentication: hash functions and digital signatures. *Lecture Notes in Computer Science*, **741** (1993), 87–131. (Computer Security and Industrial Cryptography, State of the Art and Evolution, ESAT Course, May 1991.)
- [PGV94] B. PRENEEL, R. GOVAERTS AND J. VANDEWALLE. Hash functions based on block ciphers: a synthetic approach. *Lecture Notes in Computer Science*, **773** (1994), 368–378. (Advances in Cryptology – CRYPTO '93.)
- [QG90] J.-J. QUISQUATER AND L. GUILLOU. How to explain zero-knowledge protocols to your children. *Lecture Notes in Computer Science*, **435** (1990), 628–631. (Advances in Cryptology – CRYPTO '89.)
- [QV90] J.-J. QUISQUATER AND J. VANDEWALLE (EDS.) *Advances in Cryptology – EUROCRYPT '89 Proceedings. Lecture Notes in Computer Science*, vol. 434, Springer-Verlag, 1990.
- [RA79] M. O. RABIN. Digitized signatures and public-key functions as intractible as factorization. *MIT Laboratory for Computer Science Technical Report*, LCS/TR-212, 1979.
- [RA80] M. O. RABIN. Probabilistic algorithms for testing primality. *Journal of Number Theory*, **12** (1980), 128–138.
- [Ri91] R. L. RIVEST. The MD4 message digest algorithm. *Lecture Notes in Computer Science*, **537** (1991), 303–311. (Advances in Cryptology – CRYPTO '90.)
- [RSA78] R. L. RIVEST, A. SHAMIR, AND L. ADLEMAN. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, **21** (1978), 120–126.
- [Ro93] K. H. ROSEN. *Elementary Number Theory and its Applications* (Third Edition). Addison Wesley, 1993.
- [RU86] R. A. RUEPPEL. *Analysis and Design of Stream Ciphers*. Springer-Verlag, 1986.
- [RU93] R. A. RUEPPEL (ED.) *Advances in Cryptology – EUROCRYPT '92 Proceedings. Lecture Notes in Computer Science*, vol. 658, Springer-Verlag, 1993.
- [RV94] R. A. RUEPPEL AND P. C. VAN OORSCHOT. Modern key agreement techniques. To appear in *Computer Communications*, 1994.
- [SA90] A. SALOMAA. *Public-Key Cryptography*. Springer-Verlag, 1990.
- [Sc94] J. I. SCHILLER. Secure distributed computing. *Scientific Amer-*

- ican, **271**(5) (1994), 72–76.
- [Sc93] B. SCHNEIER. *Applied Cryptography, Protocols, Algorithms and Source Code in C*. John Wiley and Sons, 1993.
- [Sc91] C. P. SCHNORR. Efficient signature generation by smart cards. *Journal of Cryptology*, **4** (1991), 161–174.
- [SP89] J. SEBERRY AND J. PIEPRZYK. *Cryptography: An Introduction to Computer Security*. Prentice-Hall, 1989.
- [SP90] J. SEBERRY AND J. PIEPRZYK (EDS.) *Advances in Cryptology – AUSCRYPT '90 Proceedings. Lecture Notes in Computer Science*, vol. 453, Springer-Verlag, 1990.
- [SZ92] J. SEBERRY AND Y. ZHENG (EDS.) *Advances in Cryptology – AUSCRYPT '92 Proceedings. Lecture Notes in Computer Science*, vol. 718, Springer-Verlag, 1993.
- [SH79] A. SHAMIR. How to share a secret. *Communications of the ACM*, **22** (1979), 612–613.
- [SH84] A. SHAMIR. A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem. *IEEE Transactions on Information Theory*, **30** (1984), 699–704.
- [SH90] A. SHAMIR. An efficient identification scheme based on permuted kernels. *Lecture Notes in Computer Science*, **435** (1990), 606–609. (Advances in Cryptology – CRYPTO '89.)
- [SH94] A. SHAMIR. Efficient signature schemes based on birational permutations. *Lecture Notes in Computer Science*, **773** (1994), 1–12. (Advances in Cryptology – CRYPTO '93.)
- [SH48] C. E. SHANNON. A mathematical theory of communication. *Bell Systems Technical Journal*, **27** (1948), 379–423, 623–656.
- [SH49] C. E. SHANNON. Communication theory of secrecy systems. *Bell Systems Technical Journal*, **28** (1949), 656–715.
- [ST92] J. H. SILVERMAN AND J. TATE. *Rational Points on Elliptic Curves*. Springer-Verlag, 1992.
- [Si85] G. J. SIMMONS. Authentication theory / coding theory. *Lecture Notes in Computer Science*, **196** (1985), 411–432. (Advances in Cryptology – CRYPTO '84.)
- [Si88] G. J. SIMMONS. A natural taxonomy for digital information authentication schemes. *Lecture Notes in Computer Science*, **293** (1988), 269–288. (Advances in Cryptology – CRYPTO '87.)
- [Si92] G. J. SIMMONS. A survey of information authentication. In *Contemporary Cryptology, The Science of Information In-*

- egrity, pages 379–419. IEEE Press, 1992.
- [SI92A] G. J. SIMMONS. An introduction to shared secret and/or shared control schemes and their application. In *Contemporary Cryptology, The Science of Information Integrity*, pages 441–497. IEEE Press, 1992.
- [SI92B] G. J. SIMMONS (ED.) *Contemporary Cryptology, The Science of Information Integrity*. IEEE Press, 1992.
- [SB92] M. E. SMID AND D. K. BRANSTAD. The data encryption standard: past and future. In *Contemporary Cryptology, The Science of Information Integrity*, pages 43–64. IEEE Press, 1992.
- [SB93] M. E. SMID AND D. K. BRANSTAD. Response to comments on the NIST proposed digital signature standard. *Lecture Notes in Computer Science*, **740** (1993), 76–88. (Advances in Cryptology – CRYPTO '92.)
- [SS77] R. SOLOVAY AND V. STRASSEN. A fast Monte Carlo test for primality. *SIAM Journal on Computing*, **6** (1977), 84–85.
- [ST88] D. R. STINSON. Some constructions and bounds for authentication codes. *Journal of Cryptology*, **1** (1988), 37–51.
- [ST90] D. R. STINSON. The combinatorics of authentication and secrecy codes. *Journal of Cryptology*, **2** (1990), 23–49.
- [ST92] D. R. STINSON. Combinatorial characterizations of authentication codes. *Designs, Codes and Cryptography*, **2** (1992), 175–187.
- [ST92A] D. R. STINSON. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, **2** (1992), 357–390.
- [ST94] D. R. STINSON (ED.) *Advances in Cryptology – CRYPTO '93 Proceedings. Lecture Notes in Computer Science*, vol. 773, Springer-Verlag, 1994.
- [vHP93] E. VAN HEYST AND T. P. PEDERSEN. How to make efficient fail-stop signatures. *Lecture Notes in Computer Science*, **658** (1993), 366–377. (Advances in Cryptology – EUROCRYPT '92.)
- [VV89] S. A. VANSTONE AND P. C. VAN OORSCHOT. *An Introduction to Error Correcting Codes with Applications*. Kluwer Academic Publishers, 1989.
- [VT88] H. C. A. VAN TILBURG. *An Introduction to Cryptology*. Kluwer Academic Publishers, 1988.
- [VT93] J. VAN TILBURG. Secret-key exchange with authentication. *Lecture Notes in Computer Science*, **741** (1993), 71–86. (Computer Security and Industrial Cryptography, State of the Art

- and Evolution, ESAT Course, May 1991.)
- [VV84] U. VAZIRANI AND V. VAZIRANI. Efficient and secure pseudo-random number generation. In *Proceedings of the 25th Annual Symposium on the Foundations of Computer Science*, pages 458–463. IEEE Press, 1984.
- [WA90] M. WALKER. Information-theoretic bounds for authentication systems. *Journal of Cryptology*, **2** (1990), 131–143.
- [WE88] D. WELSH. *Codes and Cryptography*. Oxford Science Publications, 1988.
- [Wi94] M. J. WIENER. Efficient DES key search. Technical report TR-244, School of Computer Science, Carleton University, Ottawa, Canada, May 1994 (also presented at CRYPTO '93 Rump Session).
- [Wi80] H. C. WILLIAMS. A modification of the RSA public-key encryption procedure. *IEEE Transactions on Information Theory*, **26** (1980), 726–729.
- [Wi86] H. C. WILLIAMS (ED.) *Advances in Cryptology – CRYPTO '85 Proceedings. Lecture Notes in Computer Science*, vol. 218, Springer-Verlag, 1986.
- [YA82] A. YAO. Theory and applications of trapdoor functions. In *Proceedings of the 23rd Annual Symposium on the Foundations of Computer Science*, pages 80–91. IEEE Press, 1982.

Index

- abelian group, **4**, 116, 184
- accept, **387**
- access structure, **333**
 - threshold, **333**, 334
- active adversary, **259**
- additive identity, **3**
- additive inverse, **3**
- adjoint matrix, **17**
- adversary
 - active, **259**
 - passive, **259**
- Affine Cipher, **8**, 8–12
 - cryptanalysis of, 26–28
- affine function, **8**
- Affine-Hill Cipher, **41**
- algorithm
 - deterministic, **129**
 - Las Vegas, **139**, 171, 235
 - Monte Carlo, 129, **129**
 - probabilistic, **129**
- associative property, **3**
 - of cryptosystems, **66**
- authentication code, **305**, 305–324
 - combinatorial bounds, 312–315
 - deception probability, **306**, 307–315, 320–324
 - entropy bounds, 322–324
 - impersonation attack, **306**, 307–309
 - orthogonal array characterization, 320–322
 - substitution attack, **306**, 308–310
- authentication matrix, **307**
- authentication rule, **306**
- authentication tag, **306**
- authorized subset, **333**
 - minimal, **333**
- Autokey Cipher, **23**, **24**
- basis, **334**
- Bayes' Theorem, **45**, 60, 135, 341, 342
- binding, **401**
- binomial coefficient, **32**
- birthday paradox, **237**
- bit commitment scheme, **401**, 400–403, 407–409
- blob, **401**
- block cipher, **20**
- Blom Key Predistribution Scheme, **262**, 261–264
- Blum-Blum-Shub Generator, **374**, 372–379, 381
- Blum-Goldwasser Cryptosystem, **382**, 381–384
- boolean circuit, 334
 - fan-in, **334**
 - fan-out, **334**
 - monotone, **334**
- boolean formula, **335**
 - conjunctive normal form, **338**
 - disjunctive normal form, **335**
- Bos-Chaum Signature Scheme, **217**, 216–218
- Brickell Secret Sharing Scheme, **346**, 345–350

- Caesar Cipher, **4**
- certificate, **265**
- challenge, **387**
- challenge-and-response protocol, **218**,
284, 387
- Chaum-van Antwerpen Signature Scheme,
219, 219–225
- Chaum-van Heijst-Pfitzmann hash func-
tion, **239**, 239–242
- Chinese remainder theorem, **122**, 119–
122, 142, 166, 382
- Chor-Rivest Cryptosystem, **115**
- chosen ciphertext cryptanalysis, **25**
- chosen plaintext cryptanalysis, **25**
- cipher
 - block, **20**
 - stream, **21**, 20–24, 362
- cipher block chaining mode, **83**, 84,
268
- cipher feedback mode, **83**, 85
- ciphertext, **1**, **21**, **380**
- ciphertext-only cryptanalysis, **25**
- closure, **334**
- closure property, **3**
- code, **194**
 - distance of, **195**
 - dual code, **195**
 - generating matrix, **194**
 - Goppa code, **196**
 - Hamming code, **197**
 - nearest neighbor decoding, **195**
 - parity-check matrix, **195**
 - syndrome, **195**
 - syndrome decoding, **196**
- coin-flipping by telephone, **402**
- commutative cryptosystems, **66**
- commutative property, **3**
- complete graph, **347**
- complete multipartite graph, **347**, 354,
355
- completeness, **287**, **388**
- Composites, **129**, **130**
- computational security, **44**
- concave function, **56**
 - strictly, **56**
- concealing, **401**
- conditional entropy, **59**
- conditional probability, **45**
- congruence, **3**
- conjunctive normal form boolean for-
mula, **338**
- cryptanalysis, **6**
 - chosen ciphertext, **25**
 - chosen plaintext, **25**
 - ciphertext-only, **25**
 - known-plaintext, **25**
- cryptogram, **7**
- cryptosystem, **1**
 - endomorphic, **64**
 - idempotent, **66**
 - iterated, **66**
 - monoalphabetic, **12**
 - polyalphabetic, **14**
 - private-key, **114**
 - probabilistic public-key, **380**
 - product, **64**, 64–67
 - public-key, **114**
- cyclic group, **123**, 184
- Data Encryption Standard, **51**, **70**
 - description of, 70–79
 - differential cryptanalysis of, **89**,
89–104
 - dual keys, **110**
 - exhaustive key search, **83**
 - expansion function, **71**, 73
 - initial permutation, **70**, 73
 - key schedule, **71**, 75–79
 - modes of operation, **83**, 83–86
 - S-boxes, **72**, 73–75, 82
 - time-memory tradeoff, **86**, 86–
89
- dealer, **327**
- deception probability, **306**
- decision problem, **129**, 191
- decomposition construction, **356**, **357**,
355–359
- decryption rule, **1**, **21**, **380**

- determinant, **16**
- deterministic algorithm, **129**
- differential cryptanalysis, **89**
 - characteristic, **98**
 - filtering operation, **101**
 - input x-or, **89**
 - output x-or, **89**
 - right pair, **100**
 - wrong pair, **100**
- Diffie-Hellman Key Exchange, **271**,
271–272
- Diffie-Hellman Key Predistribution
Scheme, **266**, 264–268
- Diffie-Hellman problem, **267**, 266–
268, 277
- Digital Signature Standard, 206, **212**,
210–214
- digram, **26**
- disavowal protocol, **219**
- Discrete Logarithm Generator, **385**
- Discrete Logarithm problem, 162,
163, 164–177, 207, 208,
211, 239, 264, 267, 277,
288, 291, 364, 399, 402,
408
 - bit security of, 173–177, 402
 - elliptic curve, 187–188
 - generalized, **178**, 177–180
 - in Galois fields, 183–184
 - index calculus method, 171–172
 - i th Bit problem, **173**
 - Pohlig-Hellman algorithm, **169**,
166–170
 - Shanks' algorithm, **165**, 165–
166
- disjunctive normal form boolean for-
mula, **335**
- distinguishable probability distribu-
tions, **366**
- distinguisher, **366**
- distribution rule, **339**
- distributive property, **4**
- electronic codebook mode, **83**, 84
- ElGamal Cryptosystem, 115, **163**,
162–164, 267–268
 - elliptic curve, 188–190
 - generalized, 177–178, **179**
- ElGamal Signature Scheme, **206**, 206–
210
- elliptic curve, **184**, 184–187
 - point at infinity, **184**
- Elliptic Curve Cryptosystem, 115,
188–190
- encryption matrix, **47**
- encryption rule, **1**, **21**, **380**
- endomorphlic cryptosystem, **64**
- entropy, **52**, 51–52
 - conditional, **59**
 - of a natural language, **61**
 - of a secret sharing scheme, 350–
354
 - of authentication code, 322–324
 - properties of, 56–59, 351
- Euclidean algorithm, 116–120, 140,
178, 181
 - extended, 117, **119**
 - running time of, 128
- Euler phi-function, **9**
- Euler pseudo-prime, **132**
- Euler's criterion, 130, **131**, 173
- exclusive-or, **22**
- exhaustive key search, **6**, 13
 - of DES, **83**
- factor base, 171
- factoring, 150–156
 - factor base, **153**
 - number field sieve, 155
 - $p - 1$ algorithm, **151**, 151–153
 - quadratic sieve, 154
 - trial division, **151**
- fan-in, **334**
- fan-out, **334**
- Fermat's theorem, **122**, 137
- Fibonacci number, **128**
- field, **10**, 181
- forging algorithm, **392**

- for Graph 3-colorability, **407**
 - for Graph Isomorphism, **393**, **396**
- Galois field, 180–184
- Girault Key Agreement Scheme, **279**, 277–280
- Goldwasser-Micali Cryptosystem, **381**, 381, 401
- graph, 347
 - complete, **347**
 - complete multipartite, **347**, 354, 355
 - induced subgraph, **354**
 - isomorphic, **388**
 - proper 3-coloring, **403**
- Graph 3-colorability, **403**
- Graph 3-colorability Interactive Proof System, **404**, 402–407, 409
- Graph Isomorphism, **388**
- Graph Isomorphism Interactive Proof System, **391**, 390–397
- Graph Non-isomorphism, 388
- Graph Non-isomorphism Interactive Proof System, **389**, 388–390, 397–398
- group, **4**
 - abelian, **4**, 116, 184
 - cyclic, **123**, 183, 184, 187
 - order of element in, **122**
- Guillou-Quisquater Identification Scheme, **298**, 296–300
 - identity-based, **301**
- Hamming distance, **194**
- hash function, 204, **233**, 233–255
 - birthday attack, 237–238
 - collision-free, 234–236
 - constructed from a cryptosystem, 247–248
 - extending, 242–247
 - one-way, **235**
 - strongly collision-free, **234**
 - weakly collision-free, **234**
- Hill Cipher, 14–17, **18**
 - cryptanalysis of, 37
- Huffman encoding, 53–56
- Huffman's algorithm, **55**
- ideal decomposition, **355**
- ideal secret sharing scheme, 345, **345**, 347–350
- idempotent cryptosystem, **66**
- identification scheme, 283–302
 - converted to signature scheme, 302
 - identity-based, **300**, 300–302
- identity matrix, **15**
- impersonation, **306**
- implicit key authentication, **277**, 279
- independent random variables, **45**
- index of coincidence, **32**
 - mutual, **33**
- indistinguishable probability distributions, 365–372, 380, 406
- induced subgraph, **354**
- information rate, **343**
 - monotone circuit construction, **344**
- injective function, **2**
- interactive argument
 - perfect zero-knowledge, **409**
 - zero-knowledge, **408**, 407–409
- interactive proof, **387**, 387–399
 - computational zero-knowledge, 400, **406**, 402–407
 - perfect zero-knowledge, **395**, 390–399
 - perfect zero-knowledge for Vic, **393**
 - zero-knowledge, 387
- intruder-in-the-middle attack, **272**, 306
- inverse matrix, **15**
- inverse permutation, **7**
- isomorphic graphs, **388**
- iterated cryptosystem, **66**
- Jacobi symbol, **132**, 132–134, 372, 383

- Jensen's Inequality, **56**, 63, 318
- joint probability, **45**
- Kasiski test, **31**
- Kerberos, **269**, 268–271
 - key lifetime, **269**
 - session key, 268
 - timestamp, **269**
- Kerckhoff's principle, **25**
- key, **1**, **21**, **204**, **306**, **327**, **380**
- key agreement, **259**
 - authenticated, **272**
- key confirmation, **270**
- key distribution, **259**
 - on-line, **260**
- key equivocation, **59**
- key freshness, **268**
- key predistribution, **260**, 261–268
- key server, **260**
- keystream, **20**
- keystream alphabet, **21**
- keystream generator, **21**
- keyword, **13**
- known-plaintext cryptanalysis, **25**
- Lagrange interpolation formula, **331**, 330–331
- Lagrange's theorem, **122**
- Lamport Signature Scheme, **215**, 214–216
- Lamé's theorem, **128**
- Las Vegas algorithm, **139**, 171, 235
- Legendre symbol, **131**, 131–132
- Linear Congruential Generator, **362**, 362
- linear feedback shift register, **23**, 362, 364
- linear recurrence, **22**
- linear transformation, **14**
- m*-gram Substitution Cipher, **68**
- matrix product, **14**
- McEliece Cryptosystem, 115, **197**, 194–199
- MD4 Hash Function, **250**, 248–251
- MD5 Hash Function, 248, 251
- memoryless source, **53**
- Menezes-Vanstone Cryptosystem, **189**, 189–190
- Merkle-Hellman Cryptosystem, 115, **193**, 191–194
- message, **204**, **306**
- message authentication code, **86**, 305
- message digest, **233**
- Miller-Rabin algorithm, 129, 130, **137**, 136–138
 - error probability of, 138
- mod operator, **3**
- modular exponentiation, **127**
 - square-and-multiply algorithm, 127, **127**, 131
- modular multiplication, **127**
- modular reduction, **3**
- modulus, **3**
- monoalphabetic cryptosystem, **12**
- monotone circuit, **334**
- monotone circuit construction, 334, **336**
 - information rate, **344**
- monotone property, **333**
- Monte Carlo algorithm, 129, **129**, 376
 - error probability of, **129**
 - no-biased, **129**
 - unbiased, **376**, 376–379
 - yes-biased, **129**
- MTI Key Agreement Protocol, **275**, 274–277
- Multiplicative Cipher, 65, **65**
- multiplicative identity, **4**
- multiplicative inverse, **10**
- mutual index of coincidence, **33**
- next bit predictor, 367–372
- NP-complete problem, 44, 191, 194, 402, 407
- Okamoto Identification Scheme, **293**, 291–296

- One-time Pad, 50, 50
- one-way function, 116, 214, 235
 - trapdoor, 116
- oracle, 139
- orthogonal array, 315, 315–322
 - bounds, 316–319
 - constructions, 319–320
- output feedback mode, 84, 85, 364
- passive adversary, 259
- perfect secrecy, 48, 44–51
- perfect secret sharing scheme, 333, 341, 351
- periodic stream cipher, 21
- permutation, 2
- Permutation Cipher, 18, 18, 18–20
- permutation matrix, 20
- plaintext, 1, 21, 380
- polyalphabetic cryptosystem, 14
- polynomial
 - congruence of, 181
 - degree of, 180
 - division, 180
 - irreducible, 181
 - modular reduction of, 181
- polynomial equivalence, 126
- prefix-free encoding, 54
- previous bit predictor, 375
- primality testing, 129–138
- prime, 9
- Prime number theorem, 129, 135
- primitive element, 123
- principal square root, 375, 381
- private-key cryptosystem, 114
- probabilistic algorithm, 129
- probabilistic encryption, 380–384
- probabilistic public-key cryptosystem, 380
- probability, 45
 - conditional, 45
 - joint, 45
- product cryptosystem, 64, 64–67
- proof of forgery algorithm, 225
- proof of knowledge, 286
- proper 3-coloring, 403
- protocol failure, 156, 158, 209
- prover, 387
- pseudo-random bit generator, 361, 361–379
- pseudo-square, 372
- public-key cryptosystem, 114
 - probabilistic, 380
- quadratic non-residue, 130
- Quadratic Non-residues Interactive Proof System, 410
- quadratic reciprocity, 133
- quadratic residue, 130
- Quadratic Residues, 130, 130, 373, 372–373, 376, 377, 379, 398, 401, 408
- Quadratic Residues Interactive Proof System, 398, 398–399
- Rabin Cryptosystem, 146, 145–150
 - security of, 149–150
- rank, 227
- redundancy of a natural language, 61
- reject, 387
- relative shift, 34
- relatively prime, 9
- replay attack, 270
- response, 387
- ring, 4, 180
- round, 387
- RSA Cryptosystem, 114, 124, 124–125
 - attacks on, 138–145
 - bit security of, 144–145
 - implementation of, 125–128
- RSA Generator, 364, 364–365
- RSA Signature Scheme, 204, 205
- Schnorr Identification Scheme, 287, 285–291, 296
- Schnorr Signature Scheme, 303
- search problem, 191
- secret sharing scheme, 327–359

- decomposition construction, 355–359
- ideal, 345, **345**, 347–350
- information rate, **343**, 343–345, 350–357
- monotone circuit construction, 334–339
- threshold scheme, 327–332
- Secure Hash Standard, 248, 251–253
- security parameter, **285**, **380**
- seed, **361**
- self-certifying public key, **277**
- session key, **260**
- Shamir Threshold Scheme, **328**, 328–332, 344, 347
- share, **327**
- Shift Cipher, **4**, 3–7
- Shrinking Generator, 364
- signature, **204**
- signature scheme, **204**, 203–230
 - constructed from identification scheme, 302
 - fail-stop, 225–230
 - one-time, 214–218, 229
 - undeniable, 218–225
- signing algorithm, **204**
- simulator, **392**
- Solovay-Strassen algorithm, **133**, 129–136
 - error probability, **136**, 134–136
- soundness, **289**
- source state, **305**
- Sperner property, **216**
- spurious keys, **60**, 59–64
 - expected number of, 63
- square-and-multiply algorithm, 127, **127**, 131
- Station-to-station Protocol, **273**, 272–274
- Stirling's formula, **68**, 218
- stream cipher, **21**, 20–24, 362
 - cryptanalysis of, 37
 - synchronous, **21**, 85
- Subgroup Membership, **399**
- Subgroup Membership Interactive Proof System, **400**
- Subset Sum problem, **191**, 191
 - modular transformation, **192**
 - superincreasing, **191**
- substitution, **306**
- Substitution Cipher, **7**, 7–8
 - cryptanalysis of, 28–31
 - m*-gram, **68**
- synchronous stream cipher, **21**, 85
- threshold scheme, **327**, 327–332
- timestamping, 254–255
- transcript, **392**
- Transposition Cipher, 18
- trapdoor, **116**
- trigram, **26**
- trusted authority, **259**
- unconditional security, **45**
- unicity distance, **63**, 59–64
- van Heyst-Pedersen Signature Scheme, **226**, 225–230
- Vandermonde matrix, 330
 - determinant of, 330
- verification algorithm, **204**
- verifier, **387**
- Vernam One-time Pad, 50, **50**
- Vigenère Cipher, **12**, 12–14, 40
 - cryptanalysis of, 31–36
- zero-knowledge interactive argument, **408**, 407–409
 - perfect, **409**
- zero-knowledge interactive proof, 387
 - computational, 400, **406**, 402–407
 - perfect, **395**, 390–399
 - perfect, for Vic, **393**