

# List of Notation

$\mathbb{Z}$	the integers $\{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$ , 10
$b \mid a$	$b$ divides $a$ (integers), 10
$b \nmid a$	$b$ does not divide $a$ (integers), 10
gcd	greatest common divisor, 11
$a \equiv b \pmod{m}$	$a$ and $b$ are congruent modulo $m$ , 19
$\mathbb{Z}/m\mathbb{Z}$	the ring of integers modulo $m$ , 21
$(\mathbb{Z}/m\mathbb{Z})^*$	the group of units in $\mathbb{Z}/m\mathbb{Z}$ , 22
$\text{ord}_p(a)$	order (or exponent) of $p$ in $a$ , 28
$a^{-1} \pmod{p}$	the multiplicative inverse of $a$ modulo $p$ , 28
$\mathbb{R}$	the field of real numbers, 29
$\mathbb{Q}$	the field of rational numbers, 29
$\mathbb{C}$	the field of complex numbers, 29
$\mathbb{F}_p$	the finite field $\mathbb{Z}/p\mathbb{Z}$ , 29
$\mathcal{K}$	space of keys, 37
$\mathcal{M}$	space of messages (plaintexts), 37
$\mathcal{C}$	space of ciphertexts, 37
$e$ or $e_k$	encryption function, 37
$d$ or $d_k$	decryption function, 37
$\oplus$	exclusive or (XOR), 43
$\lceil x \rceil$	the greatest integer in $x$ , 53
$\log_g(h)$	the discrete logarithm of $h$ to the base $g$ , 65
$\star$	composition operation in a group, 74
$ G $	the order of the group $G$ , 74
$\#G$	the order of the group $G$ , 74
$\text{GL}_n$	the general linear group, 75
$g^x$	exponentiation of $g$ in a group $G$ , 75
$\mathcal{O}(g(x))$	big- $\mathcal{O}$ notation, 78
$\star$	multiplication in a ring, 95
$\mathbb{Z}[x]$	ring of polynomials with integer coefficients, 96
$b \mid a$	$b$ divides $a$ (in a ring), 96
$b \nmid a$	$b$ does not divide $a$ (in a ring), 96
$a \equiv b \pmod{m}$	$a$ and $b$ are congruent modulo $m$ (in a ring), 97
$R/mR$	quotient ring of $R$ by $m$ , 98
$R/(m)$	quotient ring of $R$ by $m$ , 98
$R[x]$	ring of polynomials with coefficients in $R$ , 98

$\deg$	degree of a polynomial, 98
$\mathbb{F}_{p^d}$	a finite field with $p^d$ elements, 106
$\text{GF}(p^d)$	a field with $p^d$ elements, 106
$\pi(X)$	number of primes between 2 and $X$ , 133
$\zeta(s)$	Riemann zeta function, 135
$\psi(X, B)$	Number of $B$ -smooth integers between 2 and $X$ , 150
$o(g(x))$	little- $o$ notation, 151
$L(X)$	the function $e^{\sqrt{(\ln X)(\ln \ln X)}}$ , 151
$\Omega(g(x))$	big- $\Omega$ notation, 152
$\Theta(g(x))$	big- $\Theta$ notation, 152
$f(X) \ll g(X)$	alternative for $f(X) = \mathcal{O}(g(X))$ , 152
$f(X) \gg g(X)$	alternative for $f(X) = \Omega(g(X))$ , 152
$f(X) \gg\ll g(X)$	alternative for $f(X) = \Theta(g(X))$ , 152
$\mathbb{Z}[\beta]$	the ring generated by the complex number $\beta$ , 162
$L_\epsilon(X)$	the function $e^{(\ln X)^\epsilon (\ln \ln X)^{1-\epsilon}}$ , 165
$\left(\frac{a}{p}\right)$	the Legendre symbol of $a$ modulo $p$ , 171
$\text{Li}(X)$	the logarithmic integral function, 186
$K^{\text{Pri}}$	private signing key, 194
$K^{\text{Pub}}$	public verification key, 194
<b>Sign</b>	signing algorithm, 194
<b>Verify</b>	verification algorithm, 194
$\binom{n}{r}$	combinatorial symbol $n$ choose $r$ , 212
$\text{IndCo}(\mathbf{s}, \mathbf{t})$	index of coincidence of $\mathbf{s}$ , 219
$\text{MutIndCo}(\mathbf{s}, \mathbf{t})$	mutual index of coincidence of $\mathbf{s}$ and $\mathbf{t}$ , 221
$\text{Pr}$	a probability function, 229
$\text{Pr}(F   E)$	conditional probability of $F$ on $E$ , 234
$f_X(x)$	probability density function of $X$ , 239
$F_X(x)$	probability distribution function of $X$ , 239
$f_{X,Y}(x, y)$	joint density function of $X$ and $Y$ , 241
$f_{X,Y}(x   y)$	conditional density function of $X$ and $Y$ , 241
$O_f^+(x)$	orbit of $x$ under iteration of $f$ , 254
$H(X)$	the entropy of the random variable $X$ , 270
$\oplus$	addition on an elliptic curve, 302
$\mathcal{O}$	point at infinity on elliptic curve, 305
$\Delta_E$	discriminant of the elliptic curve $E$ , 306
$E(\mathbb{F}_p)$	points of elliptic curve with coordinates in $\mathbb{F}_p$ , 308
$\log_P(Q)$	the elliptic discrete logarithm of $Q$ with respect to $P$ , 313
$\tau$	the $p$ -power Frobenius map $\mathbb{F}_{p^k} \rightarrow \mathbb{F}_{p^k}$ , 334
$\tau$	the $p$ -power Frobenius map on an elliptic curve $E(\mathbb{F}_{p^k})$ , 334
$E[m]$	points of order $m$ on an elliptic curve $E$ , 339
$\deg(D)$	degree of the divisor $D$ , 341
$\text{Sum}(D)$	sum of points in the divisor $D$ , 341
$e_m$	the Weil pairing on an elliptic curve, 342
$\tau(P, Q)$	Tate pairing on an elliptic curve, 348
$\hat{\tau}(P, Q)$	modified Tate pairing on an elliptic curve, 348
$\hat{e}_\ell$	modified Weil pairing on an elliptic curve, 354
$\mathbf{a} \cdot \mathbf{b}$	dot product of $\mathbf{a}$ and $\mathbf{b}$ , 385
$\ \mathbf{a}\ $	Euclidean norm of $\mathbf{a}$ , 385

$GL_n(\mathbb{Z})$	the special linear group (over $\mathbb{Z}$ ), 390
$\det(L)$	the determinant (covolume) of the lattice $L$ , 392
$\gamma_n$	Hermite constant, 397
$\mathcal{H}(\mathcal{B})$	the Hadamard ratio of the basis $\mathcal{B}$ , 397
$\mathbb{B}_R(\mathbf{a})$	closed ball of radius $R$ centered at $\mathbf{a}$ , 397
$\Gamma(s)$	the gamma function, 400
$\sigma(L)$	Gaussian expected shortest length of a vector in $L$ , 402
$R$	the convolution polynomial ring $\mathbb{Z}[x]/(x^N - 1)$ , 412
$R_q$	the convolution polynomial ring $(\mathbb{Z}/q\mathbb{Z})[x]/(x^N - 1)$ , 412
$\mathbf{a} \star \mathbf{b}$	multiplication in convolution polynomial ring, 413
$\star$	convolution product of vectors, 414
$\mathcal{T}(d_1, d_2)$	ternary polynomial, 417
$L_{\mathbf{h}}^{\text{NTRU}}$	the NTRU lattice associated to $\mathbf{h}(x)$ , 425
$M_{\mathbf{h}}^{\text{NTRU}}$	matrix for the NTRU lattice associated to $\mathbf{h}(x)$ , 425
$\ \mathbf{a}\ _{\infty}$	sup norm of $\mathbf{a}$ , 434
$\mathcal{B}^*$	Gram–Schmidt orthogonal basis associated to $\mathcal{B}$ , 439
$W^{\perp}$	the orthogonal complement of $W$ , 440
Hash	a hash function, 472
$\text{Div}(C)$	group of divisors on a curve, 495
$\text{Div}_0(C)$	group of divisors of degree 0 on a curve, 495
$\text{Jac}_0(C)$	the Jacobian variety of the curve $C$ , 495
$J(\mathbb{F}_p)$	the group of points modulo $p$ on the Jacobian $\text{Jac}_0(C)$ , 495
$ 0\rangle$	ket notation in quantum mechanics, 497

# References

- [1] M. Agrawal, N. Kayal, N. Saxena, PRIMES is in P. *Ann. Math. (2)* **160**(2), 781–793 (2004)
- [2] L.V. Ahlfors, *Complex Analysis: An Introduction to the Theory of Analytic Functions of One Complex Variable*. International Series in Pure and Applied Mathematics, 3rd edn. (McGraw-Hill, New York, 1978)
- [3] M. Ajtai, The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract), in *STOC '98: Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, Dallas (ACM, New York, 1998), pp. 10–19
- [4] M. Ajtai, C. Dwork, A public-key cryptosystem with worst-case/average-case equivalence, in *STOC '97*, El Paso (ACM, New York, 1999), pp. 284–293 (electronic)
- [5] W.R. Alford, A. Granville, C. Pomerance, There are infinitely many Carmichael numbers. *Ann. Math. (2)* **139**(3), 703–722 (1994)
- [6] ANSI-ECDSA, Public key cryptography for the financial services industry: the elliptic curve digital signature algorithm (ECDSA). ANSI Report X9.62, American National Standards Institute, 1998
- [7] T.M. Apostol, *Introduction to Analytic Number Theory*. Undergraduate Texts in Mathematics (Springer, New York, 1976)
- [8] L. Babai, On Lovász' lattice reduction and the nearest lattice point problem. *Combinatorica* **6**(1), 1–13 (1986)
- [9] E. Bach, Explicit bounds for primality testing and related problems. *Math. Comput.* **55**(191), 355–380 (1990)
- [10] E. Bach, J. Shallit, *Algorithmic Number Theory: Efficient Algorithms*. Foundations of Computing Series, vol. 1 (MIT, Cambridge, 1996).
- [11] M. Bellare, Practice oriented provable-security, in *Proceedings of the First International Workshop on Information Security—ISW '97*, Tatsunokuchi. Volume of 1396 Lecture Notes in Computer Science (Springer, Berlin, 1998)
- [12] M. Bellare, P. Rogaway, Random oracles are practical: a paradigm for designing efficient protocols, in *Proceedings of the First Annual Conference on Computer and Communications Security*, Fairfax, 1993, pp. 62–73

- [13] M. Bellare, P. Rogaway, Optimal asymmetric encryption, in *Advances in Cryptology—EUROCRYPT '94*, Perugia. Volume 950 of Lecture Notes in Computer Science (Springer, Berlin, 1995), pp. 92–111
- [14] I.F. Blake, G. Seroussi, N.P. Smart, Elliptic Curves in Cryptography. Volume 265 of London Mathematical Society Lecture Note Series (Cambridge University Press, Cambridge, 2000)
- [15] G. Blakley, Safeguarding cryptographic keys, in *Proceedings of AFIPS National Computer Conference*, Zurich, vol. 48, 1979, pp. 313–317
- [16] D. Bleichenbacher, Chosen ciphertext attacks against protocols based on RSA encryption standard PKCS #1, in *Advances in Cryptology—CRYPTO 1998*, Santa Barbara. Volume 1462 of Lecture Notes in Computer Science (Springer, Berlin, 1998), pp. 1–12
- [17] J. Blömer, A. May, Low secret exponent RSA revisited, in *Cryptography and Lattices*, Providence, 2001. Volume 2146 of Lecture Notes in Computer Science (Springer, Berlin, 2001), pp. 4–19
- [18] D. Boneh, G. Durfee, Cryptanalysis of RSA with private key  $d$  less than  $N^{0.292}$ , in *Advances in Cryptology—EUROCRYPT '99*, Prague. Volume 1592 of Lecture Notes in Computer Science (Springer, Berlin, 1999), pp. 1–11
- [19] D. Boneh, G. Durfee, Cryptanalysis of RSA with private key  $d$  less than  $N^{0.292}$ . *IEEE Trans. Inf. Theory* **46**(4), 1339–1349 (2000)
- [20] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, in *Advances in Cryptology—CRYPTO 2001*, Santa Barbara. Volume 2139 of Lecture Notes in Computer Science (Springer, Berlin, 2001), pp. 213–229
- [21] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing. *SIAM J. Comput.* **32**(3), 586–615 (electronic) (2003)
- [22] D. Boneh, R. Venkatesan, Breaking RSA may not be equivalent to factoring (extended abstract), in *Advances in Cryptology—EUROCRYPT '98*, Espoo. Volume 1403 of Lecture Notes in Computer Science (Springer, Berlin, 1998), pp. 59–71
- [23] R.P. Brent, An improved Monte Carlo factorization algorithm. *BIT* **20**(2), 176–184 (1980)
- [24] E.R. Canfield, P. Erdős, C. Pomerance, On a problem of Oppenheim concerning “factorisatio numerorum”. *J. Number Theory* **17**(1), 1–28 (1983)
- [25] J.W.S. Cassels, *Lectures on Elliptic Curves*. Volume 24 of London Mathematical Society Student Texts (Cambridge University Press, Cambridge, 1991)
- [26] D. Chaum, Blind signatures for untraceable payments, in *Advances in Cryptology—CRYPTO '82*, Santa Barbara. Lecture Notes in Computer Science (Plenum Press, New York/London, 1983), pp. 199–203
- [27] D. Chaum, A. Fiat, M. Naor, Untraceable electronic cash, in *Advances in Cryptology—CRYPTO 1988*, Santa Barbara. Volume 403 of Lecture Notes in Computer Science (Springer, 1988), pp. 319–327
- [28] H. Cohen, *A Course in Computational Algebraic Number Theory*. Volume 138 of Graduate Texts in Mathematics (Springer, Berlin, 1993)

- [29] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren (eds.), *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Discrete Mathematics and Its Applications (Boca Raton) (Chapman & Hall/CRC, Boca Raton, 2006)
- [30] S.A. Cook, The complexity of theorem-proving procedures, in *STOC '71: Proceedings of the Third Annual ACM Symposium on Theory of Computing*, Shaker Heights (ACM, New York, 1971), pp. 151–158
- [31] D. Coppersmith, Solving homogeneous linear equations over  $\text{GF}(2)$  via block Wiedemann algorithm. *Math. Comput.* **62**(205), 333–350 (1994)
- [32] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptol.* **10**(4), 233–260 (1997)
- [33] D. Coppersmith, Finding small solutions to small degree polynomials, in *Cryptography and Lattices*, Providence, 2001. Volume 2146 of Lecture Notes in Computer Science (Springer, Berlin, 2001), pp. 20–31
- [34] R. Crandall, C. Pomerance, *Prime Numbers* (Springer, New York, 2001)
- [35] H. Davenport, *The Higher Arithmetic* (Cambridge University Press, Cambridge, 1999)
- [36] M. Dietzfelbinger, *Primality Testing in Polynomial Time: From Randomized Algorithms to “PRIMES is in P”*. Volume 3000 of Lecture Notes in Computer Science (Springer, Berlin, 2004)
- [37] W. Diffie, The first ten years of public key cryptology, G.J. Simmons (ed.), in *Contemporary Cryptology* (IEEE, New York, 1992), pp. 135–175
- [38] W. Diffie, M.E. Hellman, New directions in cryptography. *IEEE Trans. Inf. Theory* **IT-22**(6), 644–654 (1976)
- [39] L. Ducas, P.Q. Nguyen, Learning a zonotope and more: cryptanalysis of NTRUSign countermeasures, in *Advances in Cryptology—ASIACRYPT 2012*, Beijing. Volume 7658 of Lecture Notes in Computer Science (Springer, Berlin, 2012), pp. 433–450
- [40] D.S. Dummit, R.M. Foote, *Abstract Algebra*, 3rd edn. (Wiley, Hoboken, 2004)
- [41] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* **31**(4), 469–472 (1985)
- [42] J. Ellis, The story of non-secret encryption, 1987 (released by CSEG in 1997). <https://cryptocellar.web.cern.ch/cryptocellar/cesg/ellis.pdf>
- [43] W. Fleming, *Functions of Several Variables*. Undergraduate Texts in Mathematics, 2nd edn. (Springer, New York, 1977)
- [44] M. Fouquet, P. Gaudry, R. Harley, An extension of Satoh’s algorithm and its implementation. *J. Ramanujan Math. Soc.* **15**(4), 281–318 (2000)
- [45] J. Fraleigh, *A First Course in Abstract Algebra*, 7th edn. (Addison Welsley, Boston/London, 2002)
- [46] M.R. Garey, D.S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*. A Series of Books in the Mathematical Sciences (W. H. Freeman, San Francisco, 1979)

- [47] C. Gentry, *A Fully Homomorphic Encryption Scheme*, PhD thesis, Stanford University, 2009. [crypto.stanford.edu/craig](http://crypto.stanford.edu/craig)
- [48] C. Gentry, Fully homomorphic encryption using ideal lattices, in *STOC'09—Proceedings of the 2009 ACM International Symposium on Theory of Computing*, Bethesda (ACM, New York, 2009), pp. 169–178
- [49] O. Goldreich, S. Goldwasser, S. Halevi, Public-key cryptosystems from lattice reduction problems, in *Advances in Cryptology—CRYPTO '97*, Santa Barbara, 1997. Volume 1294 of Lecture Notes in Computer Science (Springer, Berlin, 1997), pp. 112–131
- [50] O. Goldreich, D. Micciancio, S. Safra, J.-P. Seifert, Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. *Inf. Process. Lett.* **71**(2), 55–61 (1999)
- [51] G.R. Grimmett, D.R. Stirzaker, *Probability and Random Processes*, 3rd edn. (Oxford University Press, New York, 2001)
- [52] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, 5th edn. (The Clarendon Press/Oxford University Press, New York, 1979)
- [53] I.N. Herstein, *Topics in Algebra*, 2nd edn. (Xerox College Publishing, Lexington, 1975)
- [54] J. Hoffstein, J. Pipher, J.H. Silverman, NTRU: a ring-based public key cryptosystem, in *Algorithmic Number Theory*, Portland, 1998. Volume 1423 of Lecture Notes in Computer Science (Springer, Berlin, 1998), pp. 267–288
- [55] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J.H. Silverman, W. Whyte, NTRUSign: digital signatures using the NTRU lattice, in *Topics in Cryptology—CT-RSA 2003*. Volume 2612 of Lecture Notes in Computer Science (Springer, Berlin, 2003), pp. 122–140. <https://www.securityinnovation.com/uploads/Crypto/NTRUSign-preV2.pdf>
- [56] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J.H. Silverman, W. Whyte, Performance improvements and a baseline parameter generation algorithm for NTRUSign. Presented at Workshop on Mathematical Problems and Techniques in Cryptology, Barcelona, 2005. <https://www.securityinnovation.com/uploads/Crypto/NTRUSignParams-2005-08.pdf>
- [57] J. Hoffstein, J. Pipher, J. Schanck, J. Silverman, W. Whyte, Transcript secure signatures based on modular lattices. *Cryptology ePrint archive*, report 2014/457, 2014. <http://eprint.iacr.org/2014/457>
- [58] N. Howgrave-Graham, Approximate integer common divisors, in *Cryptography and Lattices*, Providence, 2001. Volume 2146 of Lecture Notes in Computer Science (Springer, Berlin, 2001), pp. 51–66
- [59] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*. Volume 84 of Graduate Texts in Mathematics (Springer, New York, 1990)
- [60] E.T. Jaynes, Information theory and statistical mechanics. *Phys. Rev.* (2) **106**, 620–630 (1957)
- [61] A. Joux, A one round protocol for tripartite Diffie-Hellman, in *Algorithmic Number Theory*, Leiden, 2000. Volume 1838 of Lecture Notes in Computer Science (Springer, Berlin, 2000), pp. 385–393

- [62] A. Joux, A one round protocol for tripartite Diffie-Hellman. *J. Cryptol.* **17**(4), 263–276 (2004)
- [63] D. Kahn, *The Codebreakers: The Story of Secret Writing* (Scribner Book, New York, 1996)
- [64] P. Kaye, R. Laflamme, M. Mosca, *An Introduction to Quantum Computing* (Oxford University Press, Oxford, 2007)
- [65] A.W. Knapp, *Elliptic Curves*. Volume 40 of Mathematical Notes (Princeton University Press, Princeton, 1992)
- [66] D. Knuth, *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, 2nd edn. (Addison-Wesley, Reading, 1981)
- [67] N. Koblitz, Elliptic curve cryptosystems. *Math. Comput.* **48**(177), 203–209 (1987)
- [68] N. Koblitz, *Algebraic Aspects of Cryptography*. Volume 3 of Algorithms and Computation in Mathematics (Springer, Berlin, 1998)
- [69] N. Koblitz, The uneasy relationship between mathematics and cryptography. *Not. Am. Math. Soc.* **54**, 972–979 (2007)
- [70] N. Koblitz, A.J. Menezes, Another look at “provable security”. *J. Cryptol.* **20**(1), 3–37 (2007)
- [71] J.C. Lagarias, H.W. Lenstra Jr., C.-P. Schnorr, Korkin–Zolotarev bases and successive minima of a lattice and its reciprocal lattice. *Combinatorica* **10**(4), 333–348 (1990)
- [72] B.A. LaMacchia, A.M. Odlyzko, Solving large sparse linear systems over finite fields, in *Advances in Cryptology—CRYPTO ’90*, Santa Barbara, 1990. Lecture Notes in Computer Science (Springer, Berlin, 1990)
- [73] S. Lang, *Elliptic Curves: Diophantine Analysis*. Volume 231 of Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Sciences) (Springer, Berlin, 1978)
- [74] S. Lang, *Elliptic Functions*. Volume 112 of Graduate Texts in Mathematics, 2nd edn. (Springer, New York, 1987). With an appendix by J. Tate
- [75] H.W. Lenstra Jr., Factoring integers with elliptic curves. *Ann. Math.* (2) **126**(3), 649–673 (1987)
- [76] H.W. Lenstra jr., C. Pomerance, Primality testing with Gaussian periods (2011). <https://www.math.dartmouth.edu/~carlp/PDF/complexity12.pdf>
- [77] A.K. Lenstra, H.W. Lenstra Jr., L. Lovász, Factoring polynomials with rational coefficients. *Math. Ann.* **261**(4), 515–534 (1982)
- [78] V. Lyubashevsky, Lattice-based identification schemes secure under active attacks, in *Public Key Cryptography—PKC 2008*, Barcelona. Volume 4939 of Lecture Notes in Computer Science (Springer, Berlin, 2008), pp. 162–179
- [79] V. Lyubashevsky, Fiat-Shamir with aborts: applications to lattice and factoring-based signatures, in *Advances in Cryptology—ASIACRYPT 2009*, Tokyo. Volume 5912 of Lecture Notes in Computer Science (Springer, Berlin, 2009), pp. 598–616



- [80] V. Lyubashevsky, Lattice signatures without trapdoors, in *Advances in Cryptology—EUROCRYPT 2012*, Cambridge. Volume 7237 of Lecture Notes in Computer Science (Springer, Heidelberg, 2012), pp. 738–755
- [81] A. Menezes, *Elliptic Curve Public Key Cryptosystems*. The Kluwer International Series in Engineering and Computer Science, 234 (Kluwer Academic, Boston, 1993)
- [82] A.J. Menezes, T. Okamoto, S.A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inf. Theory* **39**(5), 1639–1646 (1993)
- [83] R.C. Merkle, Secure communications over insecure channels, in *Secure Communications and Asymmetric Cryptosystems*, ed. by G.J. Simmons. Volume 69 of AAAS Selected Symposium Series (Westview, Boulder, 1982), pp. 181–196
- [84] R.C. Merkle, M.E. Hellman, Hiding information and signatures in trapdoor knapsacks, in *Secure Communications and Asymmetric Cryptosystems*, ed. by G.J. Simmons. Volume 69 of AAAS Selected Symposium Series (Westview, Boulder, 1982), pp. 197–215
- [85] D. Micciancio, Improving lattice based cryptosystems using the Hermite normal form, in *Cryptography and Lattices*, Providence, 2001. Volume 2146 of Lecture Notes in Computer Science (Springer, Berlin, 2001), pp. 126–145
- [86] D. Micciancio, S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*. The Kluwer International Series in Engineering and Computer Science, 671 (Kluwer Academic, Boston, 2002)
- [87] G.L. Miller, Riemann’s hypothesis and tests for primality. *J. Comput. Syst. Sci.* **13**(3), 300–317 (1976). Working papers presented at the ACM-SIGACT Symposium on the Theory of Computing, Albuquerque, 1975
- [88] V.S. Miller, Use of elliptic curves in cryptography, in *Advances in Cryptology—CRYPTO ’85*, Santa Barbara, 1985. Volume 218 of Lecture Notes in Computer Science (Springer, Berlin, 1986), pp. 417–426
- [89] V.S. Miller, The Weil pairing, and its efficient calculation. *J. Cryptol.* **17**(4), 235–261 (2004). Updated and expanded version of unpublished manuscript *Short programs for functions on curves*, 1986
- [90] P.L. Montgomery, Speeding the Pollard and elliptic curve methods of factorization. *Math. Comput.* **48**(177), 243–264 (1987)
- [91] S.p. Nakamoto, Bitcoin: a peer-to-peer electronic cash system (2009). <https://bitcoin.org/bitcoin.pdf>
- [92] P. Nguyen, Cryptanalysis of the Goldreich–Goldwasser–Halevi cryptosystem from crypto’97, in *Advances in Cryptology—CRYPTO ’99*, Santa Barbara, 1999. Volume 1666 of Lecture Notes in Computer Science (Springer, Berlin, 1999), pp. 288–304
- [93] P. Nguyen, O. Regev, Learning a parallelepiped: cryptanalysis of GGH and NTRU signatures, in *Advances in Cryptology—EUROCRYPT ’06*, St. Petersburg. Volume 4004 of Lecture Notes in Computer Science (Springer, Berlin, 2006)
- [94] P.Q. Nguyen, O. Regev, Learning a parallelepiped: cryptanalysis of GGH and NTRU signatures. *J. Cryptol.* **22**(2), 139–160 (2009)

- [95] P. Nguyen, J. Stern, Cryptanalysis of the Ajtai-Dwork cryptosystem, in *Advances in Cryptology—CRYPTO '98*, Santa Barbara, 1998. Volume 1462 of Lecture Notes in Computer Science (Springer, Berlin, 1998), pp. 223–242
- [96] NIST–AES, Advanced Encryption Standard (AES). FIPS Publication 197, National Institute of Standards and Technology, 2001. <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- [97] NIST–DES, Data Encryption Standard (DES). FIPS Publication 46-3, National Institute of Standards and Technology, 1999. <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>
- [98] NIST–DSS, Digital Signature Standard (DSS). FIPS Publication 186-2, National Institute of Standards and Technology, 2004. <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf>
- [99] NIST–SHS, Secure Hash Standard (SHS). FIPS Publication 180-2, National Institute of Standards and Technology, 2003. <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>
- [100] I. Niven, H.S. Zuckerman, H.L. Montgomery, *An Introduction to the Theory of Numbers* (Wiley, New York, 1991)
- [101] NTRU Cryptosystems, A meet-in-the-middle attack on an NTRU private key. Technical report, 1997, updated 2003. Tech. Note 004, <https://www.securityinnovation.com/uploads/Crypto/NTRUTech004v2.pdf>
- [102] NTRU Cryptosystems, Estimated breaking times for NTRU lattices. Technical report, 1999, updated 2003. Tech. Note 012, <https://www.securityinnovation.com/uploads/Crypto/NTRUTech012v2.pdf>
- [103] A.M. Odlyzko, The rise and fall of knapsack cryptosystems, in *Cryptology and Computational Number Theory*, Boulder, 1989. Volume 42 of Proceedings of Symposia in Applied Mathematics (American Mathematical Society, Providence, 1990), pp. 75–88
- [104] J.M. Pollard, Monte Carlo methods for index computation (mod  $p$ ). *Math. Comput.* **32**(143), 918–924 (1978)
- [105] C. Pomerance, A tale of two sieves. *Not. Am. Math. Soc.* **43**(12), 1473–1485 (1996)
- [106] E.L. Post, A variant of a recursively unsolvable problem. *Bull. Am. Math. Soc.* **52**, 264–268 (1946)
- [107] J. Proos, C. Zalka, Shor’s discrete logarithm quantum algorithm for elliptic curves. *Quantum Inf. Comput.* **3**(4), 317–344 (2003)
- [108] M.O. Rabin, Digitized signatures and public-key functions as intractible as factorization. Technical report, MIT Laboratory for Computer Science, 1979. Technical Report LCS/TR-212
- [109] H. Riesel, *Prime Numbers and Computer Methods for Factorization*. Volume 126 of Progress in Mathematics (Birkhäuser, Boston, 1994)
- [110] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**(2), 120–126 (1978)
- [111] K.H. Rosen, *Elementary Number Theory and Its Applications*, 4th edn. (Addison-Wesley, Reading, 2000)

- [112] S. Ross, *A First Course in Probability*, 9th edn. (Pearson, England, 2001)
- [113] T. Satoh, The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.* **15**(4), 247–270 (2000)
- [114] T. Satoh, K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Comment. Math. Univ. St. Paul.* **47**(1), 81–92 (1998)
- [115] C.-P. Schnorr, A hierarchy of polynomial time lattice basis reduction algorithms. *Theor. Comput. Sci.* **53**(2–3), 201–224 (1987)
- [116] C.P. Schnorr, Fast LLL-type lattice reduction. *Inf. Comput.* **204**(1), 1–25 (2006)
- [117] C.-P. Schnorr, M. Euchner, Lattice basis reduction: improved practical algorithms and solving subset sum problems, in *Fundamentals of Computation Theory*, Gosen, 1991. Volume 529 of Lecture Notes in Computer Science (Springer, Berlin, 1991), pp. 68–85
- [118] C.-P. Schnorr, M. Euchner, Lattice basis reduction: improved practical algorithms and solving subset sum problems. *Math. Program.* **66**(2, Ser. A), 181–199 (1994)
- [119] C.P. Schnorr, H.H. Hörner, Attacking the Chor–Rivest cryptosystem by improved lattice reduction, in *Advances in Cryptology—EUROCRYPT '95*, Saint-Malo, 1995. Volume 921 of Lecture Notes in Computer Science (Springer, Berlin, 1995), pp. 1–12
- [120] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod  $p$ . *Math. Comput.* **44**(170), 483–494 (1985)
- [121] R. Schoof, Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordx.* **7**(1), 219–254 (1995). Les Dix-huitièmes Journées Arithmétiques, Bordeaux, 1993
- [122] I.A. Semaev, Evaluation of discrete logarithms in a group of  $p$ -torsion points of an elliptic curve in characteristic  $p$ . *Math. Comput.* **67**(221), 353–356 (1998)
- [123] A. Shamir, How to share a secret. *Commun. ACM* **22**(11), 612–613 (1979)
- [124] A. Shamir, A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem. *IEEE Trans. Inf. Theory* **30**(5), 699–704 (1984)
- [125] A. Shamir, Identity-based cryptosystems and signature schemes, in *Advances in Cryptology*, Santa Barbara, 1984. Volume 196 of Lecture Notes in Computer Science (Springer, Berlin, 1985), pp. 47–53
- [126] C.E. Shannon, A mathematical theory of communication. *Bell Syst. Tech. J.* **27**, 379–423, 623–656 (1948)
- [127] C.E. Shannon, Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**, 656–715 (1949)
- [128] P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in *35th Annual Symposium on Foundations of Computer Science*, Santa Fe, 1994 (IEEE Computer Society, Los Alamitos, 1994), pp. 124–134
- [129] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**(5), 1484–1509 (1997)

- [130] V. Shoup, Lower bounds for discrete logarithms and related problems, in *Advances in Cryptology—EUROCRYPT '97*, Konstanz. Volume 1233 of Lecture Notes in Computer Science (Springer, Berlin, 1997), pp. 256–266
- [131] V. Shoup, OAEP reconsidered, in *Advances in Cryptology—CRYPTO 2001*, Santa Barbara. Volume 2139 of Lecture Notes in Computer Science (Springer, Berlin, 2001), pp. 239–259
- [132] V. Shoup, *A Computational Introduction to Number Theory and Algebra* (Cambridge University Press, 2005). <http://shoup.net/ntb/ntb-b5.pdf>
- [133] C.L. Siegel, A mean value theorem in geometry of numbers. *Ann. Math. (2)* **46**, 340–347 (1945)
- [134] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. Volume 151 of Graduate Texts in Mathematics (Springer, New York, 1994)
- [135] J.H. Silverman, Elliptic curves and cryptography, in *Public-Key Cryptography*, Les Diablerets. Volume 62 of Proceedings of Symposia in Applied Mathematics (American Mathematical Society, Providence, 2005), pp. 91–112
- [136] J.H. Silverman, *The Arithmetic of Elliptic Curves*. Volume 106 of Graduate Texts in Mathematics, 2nd edn. (Springer, Dordrecht, 2009)
- [137] J.H. Silverman, *A Friendly Introduction to Number Theory*, 4th edn. (Pearson, Upper Saddle River, 2013)
- [138] J.H. Silverman, J. Tate, *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics (Springer, New York, 1992)
- [139] S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* Reprint edn. (Anchor, New York, 2000)
- [140] B. Skjernaas, Satoh’s algorithm in characteristic 2. *Math. Comput.* **72**(241), 477–487 (electronic) (2003)
- [141] N.P. Smart, The discrete logarithm problem on elliptic curves of trace one. *J. Cryptol.* **12**(3), 193–196 (1999)
- [142] Standards for Efficient Cryptography, SEC 2: recommended elliptic curve domain parameters (Version 1), 20 Sept 2000. [http://www.secg.org/collateral/sec2\\_final.pdf](http://www.secg.org/collateral/sec2_final.pdf)
- [143] J. Talbot, D. Welsh, *Complexity and Cryptography: An Introduction* (Cambridge University Press, Cambridge, 2006)
- [144] E. Teske, Speeding up Pollard’s rho method for computing discrete logarithms, in *Algorithmic Number Theory*, Portland, 1998. Volume 1423 of Lecture Notes in Computer Science (Springer, Berlin, 1998), pp. 541–554
- [145] E. Teske, Square-root algorithms for the discrete logarithm problem (a survey), in *Public-Key Cryptography and Computational Number Theory*, Warsaw, 2000 (de Gruyter, Berlin, 2001), pp. 283–301
- [146] J. Von Neumann, Various techniques used in connection with random digits. *Natl. Bur. Stand. Appl. Math. Ser.* **12**(36–38), 1 (1951). Reprinted in von Neumann’s *Collected Works*, 5 (1963), Pergamon Press, pp. 768–770. <https://dornsifecms.usc.edu/assets/sites/520/docs/VonNeumann-ams12p36-38.pdf>

- [147] L.C. Washington, *Elliptic Curves: Number Theory and Cryptography*. Discrete Mathematics and Its Applications (Chapman & Hall/CRC, Boca Raton, 2003)
- [148] A.E. Western, J.C.P. Miller, *Tables of Indices and Primitive Roots*. Royal Society Mathematical Tables, vol. 9 (Published for the Royal Society at the Cambridge University Press, London, 1968)
- [149] M.J. Wiener, Cryptanalysis of short RSA secret exponents. *IEEE Trans. Inf. Theory* **36**(3), 553–558 (1990)
- [150] S.Y. Yan, *Primality Testing and Integer Factorization in Public-Key Cryptography*. Volume 11 of Advances in Information Security (Kluwer Academic, Boston, 2004)

# Index

- abelian group, 74, 304
- addition law on elliptic curve, 300, 303
  - adding point to self, 301
  - formulas for, 305, 325
  - properties of, 304
  - works over finite field, 307
- addition law on hyperelliptic curve, 495
- additive subgroup, 390, 455
- adjoint matrix, 388, 455
- Adleman, Leonard, 61, 123, 496
- Advanced Encryption Standard, *see* AES
- AES, 45, 58, 278, 499
  - competition to choose, 501
  - S-box, 501
  - used to build PRNG, 476
- affine cipher, 43, 57
- Agrawal, M., 136, 281
- Ajtai–Dwork cryptosystem, 407, 408
- Ajtai, Miklós, 282, 407
- Ajtai, Miklós, 408
- AKS primality test, 137, 279, 281
- Alberti, Leon Batista, 2
- Alford, W.R., 130
- algebraic geometry, 307
- algorithm
  - BKZ–LLL, 427
  - collision, 81, 208, 246, 250, 315
  - decryption, 63
  - double-and-add, 312, 313
  - encryption, 63
  - exponential time, 80, 136
  - export of cryptographic, 62, 107
  - fast powering, 24, 25, 32, 53, 54, 251, 281
  - Frobenius-and-add, 335, 367
  - lattice reduction, 384
  - linear time, 80
  - LLL, 384, 427, 443, 444
  - Monte Carlo, 236, 290, 291, 432
  - MOV, 348, 370, 496
  - Pohlig–Hellman, 89
  - polynomial-time, 80, 137, 279, 281, 310, 335
  - probabilistic, 236
  - signing, 194
  - subexponential-time, 80, 154, 161, 165, 169, 329
  - verification, 194
- Alice, 2
- alternating pairing, 336, 341, 368
- angle between vectors, 386
- anomalous elliptic curve, 349
- ANSI, 487
- apprCVP, *see* approximate closest vector problem
- approximate closest vector problem,
  - 396, 429
  - LLL solves, 448, 468
- approximate shortest vector problem,
  - 396
  - LLL solves, 443, 450
- apprSVP, *see* approximate shortest vector problem
- arithmetic progression, 241
- arithmetic, fundamental theorem of, 27
- ASCII, 39, 57, 275
- associative law, 74, 95, 304
- asymmetric cipher, 46
  - bank vault analogy, 193
  - key, 46, 63
- Atkin, A.O.L., 310
- attack, 38, 41
  - brute-force, 41
  - chosen plaintext, 38

- collision, 41
- exhaustive search, 41
- known plaintext, 38, 59, 288
- man-in-the-middle, 126, 183
- meet-in-the-middle, 41
- autokey cipher, 287
- average case versus hardest case
  - equivalence, 282, 408
- axiomatic theory, 229
  
- Babai closest plane algorithm, 448, 468
- Babai closest vertex algorithm, 403, 405, 410, 429, 448, 453, 468
- Babai, L., 403
- babystep-giantstep algorithm, 82
- bad basis, 405
- ball, 397
  - volume, 400
- basis, 385
  - bad, 405
  - good, 405
  - Gram matrix, 456
  - Gram-Schmidt algorithm, 387, 439
  - Hadamard ratio, 397, 407
  - LLL reduced, 440
  - of a lattice, 388
  - orthogonal, 386
  - orthonormal, 386
  - quasi-orthogonal, 448, 452, 453, 467, 468
- basis problem, 362
- Bayes's formula, 234, 237, 243, 264, 432
  - general version, 289
- Bellare, Mihir, 484, 485
- Bertoni, G., 474
- Bertrand's box paradox, 290
- big-endian, 486
- big- $\mathcal{O}$ , *see* order notation
- big- $\Omega$  notation, 152
- bigram, 7, 275
  - entropy, 276, 298
  - index of coincidence, 286
- big- $\Theta$  notation, 152
- bijjective function, 210
- bilinear pairing
  - alternating, 336, 341, 368
  - dot product, 336
  - elliptic curve, 336
  - nondegenerate, 352
  - Tate, 346
  - Weil, 340
- binary digit, 39, 497
- binary expansion, 25, 312, 363
- binary polynomial, 417
- binomial distribution, 239, 292
  - expected value, 292
- binomial symbol, 212
  - identity, 284
- binomial theorem, 213, 284, 292, 332, 366
- birthday paradox, 223, 246, 247, 293
- birthday paradox algorithm, *see* collision algorithm
- bit, 39, 497
  - eight in a byte, 40
- bit security, 176, 190
- bit string, 40
  - concatenation, 191, 279, 472
  - exclusive or, 44, 473
- Bitcoin, 487, 488
- BKZ-LLL algorithm, 427, 449, 450
- black box discrete logarithm problem, 253
- Blakley, George, 480
- Bleichenbacher, D., 484
- blind digital signature, 196, 487
- block, 40
- block Korkin-Zolotarev algorithm, 427, 449, 450
- blocksize, 40, 219
- Bob, 2
- Boneh, Dan, 359
- bounded Post correspondence problem, 279
  - is  $\mathcal{NP}$ , 279
- bounded set, 398
- box method to solve  $au + bv = 1$ , 18, 416
- brute-force attack, 41
  - DLP, 81
  - NTRU, 423
- $B$ -smooth number, *see* smooth number
- byte, 40
  
- Caesar cipher, 1, 2, 23, 34, 48
- Caesar, Julius, 1, 2, 34
- calculus, multivariable, 393
- Canfield, E.R., 151

- Canfield–Erdős–Pomerance theorem,  
151, 154
- card problem, 231, 249, 293
- Carmichael number, 130, 183  
infinitely many, 130  
is product of distinct odd primes,  
183  
Korselt criterion, 184
- Carmichael, R.D., 130
- Carroll, Lewis, 298
- Cauchy–Schwarz inequality, 386
- center-lift, 414
- Certicom, 323  
patents, 324
- Chaldean poetry, 323
- challenge-and-response, 481
- change-of-basis formula, 385, 388
- change-of-basis matrix, 388
- change-of-variable formula, 393
- characteristic, 115
- Chaum, D., 487
- Chinese remainder theorem, 83–86, 89,  
167, 176, 183, 416  
as a state of mind, 88  
ring theory proof, 111
- chosen ciphertext attack, 483
- chosen plaintext attack, 38
- Church, Alonzo, 278
- cipher  
affine, 43, 57  
asymmetric, 46  
autokey, 287  
blocksize, 40  
Caesar, 1, 2, 23, 34, 48  
combinatorially secure, 208  
examples of symmetric, 41  
Hill, 43, 57  
homophonic, 34, 56  
monoalphabetic, 214  
one-time pad, 44, 269, 476  
polyalphabetic, 35, 214  
shift, 2, 23, 34, 265, 296  
simple substitution, 2, 34, 48, 211,  
263, 285  
symmetric, 37–39, 263, 499  
transposition, 34, 56  
Vigenère, 35, 214–227, 263,  
284–287
- cipher machine, 36
- ciphertext, 1  
blocksize, 41  
entropy, 274  
random variable, 264  
space of, 37
- cipherwheel, 2, 47, 285
- clock arithmetic, 19
- closed ball, 397  
volume, 400
- closed set, 398
- closest plane algorithm, 448, 468
- closest vector problem, 395, 483  
approximate, 396, 429  
at least as hard as SVP, 395  
average case versus hardest case,  
282, 408  
Babai algorithm, 403  
cryptosystems based on, 407  
is  $\mathcal{NP}$ -hard, 395  
LLL solves approximate, 448, 468  
no quantum algorithm known, 498  
NTRU plaintext recovery, 463
- closest vertex algorithm, *see* Babai  
closest vertex algorithm
- Cocks, Clifford, 61
- code, 35, 39  
ASCII, 39, 57  
*Codebreakers, The*, 36
- coding scheme, 39
- Cohen, Henri, 466
- coin toss experiment, 233, 240, 288, 289
- collision algorithm, 208, 246, 250, 315,  
496  
discrete logarithm problem, 81,  
251, 293  
NTRU, 424  
requiring little storage, 256  
subset-sum problem, 377
- collision attack, 41
- collision resistance, 472
- collision theorem, 247
- combination, 211–213  
number of, 212
- combinatorial security, 208
- combinatorial symbol, 212
- common divisor, 11, 100
- commutative group, 74, 304
- commutative law, 74, 95, 304
- commutative ring, 95



- complement, probability of, 230, 288
- completeness, 477
- complex numbers, 29, 103
- complexity theory, 278
  - average case versus hardest case, 282, 408
- composite number
  - Miller–Rabin test, 131, 135, 184, 291
  - small witness for, 136
  - test for, 32, 129
  - witness for, 130, 131, 291
- compound event, 229
- zero-knowledge proof, 479
- concatenation, 191, 279, 472
- concave function, 272
  - geometric interpretation, 272
  - second derivative test, 272, 297
- conditional density function, 241
  - for key, plaintext, and ciphertext, 264
- conditional entropy, 274, 298
- conditional probability, 234
  - Monty Hall problem, 290
- congruence, 19, 97
  - behaves like equality, 20, 51, 97
  - Chinese remainder theorem, 85
  - Euler formula, 118, 181
  - fraction modulo  $m$ , 21
  - group of units, 22, 52
  - multiplicative inverse, 20, 28, 29, 32, 54
  - ring modulo  $m$ , 21, 98
  - root modulo  $N$ , 181
  - root modulo  $p$ , 119
  - root modulo  $pq$ , 120, 180
  - simultaneous, 85
  - square root modulo  $m$ , 87
  - square root modulo  $p$ , 86, 108, 190
  - square root modulo  $p^n$ , 112
- congruence class, 98, 102
- congruential cryptosystem, 373
  - lattice attack, 376, 451
  - random element, 374
- $\text{co-}\mathcal{NP}$ , 281
- continued fraction, 156, 499
- convex set, 398
- convolution polynomial ring, 412
  - center-lift, 414
  - formula for product, 413
  - inverses in, 415, 460
    - looks random, 420
    - modulo  $p^k$ , 416, 460
  - modulo  $q$ , 412
  - norm of product, 461
  - reduction modulo  $q$  map, 414
  - rotation, 422
  - speed of multiplication, 421
  - vector of coefficients, 413
- convolution product, 414
  - expected value of norm, 461
  - norm of, 461
- Cook, Stephen, 280
- counting principle, 208, 209
- cryptanalysis, 5, 34
  - Arabic, 34
  - differential, 500
  - substitution cipher, 4–10
  - Vigenère cipher, 218
- cryptogram, 2
- cryptographic protocol, 486
- cryptographically secure PRNG, 476
- cryptography, 2
  - asymmetric, 46
  - export of, 62, 107
  - ID-based, 358
  - implementation issues, 126
  - Kerckhoff’s principle, 38
  - practical lesson, 5
  - public key, 46
  - the role of patents in, 323, 324
- cryptology, 2
- cryptosystem
  - Ajtai–Dwork, 407, 408
  - autokey, 287
  - Caesar, 2
  - combinatorially secure, 208
  - congruential, 373
  - Elgamal, 70, 496
  - elliptic Elgamal, 319
  - GGH, 407, 409, 410
  - Goldwasser–Micali, 178
  - hyperelliptic, 494
  - knapsack, 282, 380, 381
  - lattice-based, 407
  - MV-Elgamal, 364, 365
  - NTRU, 323, 407, 416, 417, 419
  - one-time pad, 44, 269, 476

- perfect secrecy, 264
- probabilistic, 177, 412
  - conversion to, 191, 475, 484
- product, 277
- RSA, 124
- subset-sum, 282, 380, 381
- substitution, 2, 211, 263, 285
- summation of, 277
- transposition, 56
  - Vigenère, 214, 263, 284
- cube root of unity, 370
- cubic polynomial, 301, 303, 361
- cubic residue, 190
- CVP, *see* closest vector problem
  
- Daemen, J., 474, 501
- Data Encryption Standard, *see* DES
- decision problem, 278
  - Diffie–Hellman, 108, 278
  - elliptic Diffie–Hellman, 369
  - $\mathcal{NP}$ -complete, 280
  - $\mathcal{NP}$ -hard, 280
  - $\mathcal{P}$ , 279
  - polynomial-time, 279
  - polynomial-time reduction, 280
  - primality, 278
  - satisfiability, 280
  - undecidable, 278
- decryption
  - is a function, 37
- decryption exponent, 125, 182
- decryption failure, 420
- decryption function, 3, 46, 63, 211
  - ECC, 319
  - Elgamal, 70
  - GGH, 410
  - knapsack, 380
  - NTRU, 418
  - RSA, 124
- decryption table, 4
- deep insertion method, 449
- degree
  - of a polynomial, 98
  - of divisor, 339, 495
  - of product is sum of degrees, 113
- Deligne, Pierre, 309
- DeMarais, J., 496
- density
  - binomial, 240
  - geometric, 241
  - hypergeometric, 240
  - uniform, 239
- density function, 239
  - conditional, 241
  - for key, plaintext, and ciphertext, 264
  - joint, 241
- dependent vectors, 384
- derangement, 284
- DES, 45, 58, 278, 499
  - DES-X, 501
  - S-box, 500
  - triple, 500
  - used to build PRNG, 476
- determinant, 336
  - of Gram–Schmidt basis, 439
  - of lattice, 392
  - of lattice for  $m \neq n$ , 457
  - of NTRU lattice, 427
  - Weil pairing, 341
  - Weil pairing is, 369
- DHP, *see* Diffie–Hellman problem
- difference of squares, 141, 143
- differential cryptanalysis, 500
- differentiation trick, 245, 292
- Diffie–Hellman decision problem, 108, 278, 369
- Diffie–Hellman key exchange, 67–69, 483
  - elliptic, 316, 363
  - hyperelliptic, 496
  - man-in-the-middle attack, 126
  - tripartite, 356, 370, 371
- Diffie–Hellman problem, 69, 108, 109, 371
  - Elgamal oracle solves, 73
  - elliptic, 318
- Diffie, Whitfield, 45, 61
- digital cash, 487
- digital signature, 193, 482
  - blind, 196, 487
  - Elgamal, 198
  - elliptic curve, 321, 322
  - forgery on random document, 205
  - GGH, 428, 429
  - hash function used in, 196, 429
  - lattice-based, 428
  - NTRUMLS, 434
  - real-world applications, 195

- rejection sampling, 431
- RSA, 196, 197
- signet ring analogy, 193
- signing algorithm, 194
- transcript attack, 195, 430, 431
- verification algorithm, 194
- Digital Signature Algorithm (DSA), 199, 201, 202
- Digital Signature Standard (DSS), 199
- dimension, 385
  - of a lattice, 388
- direct sum, 465
- discrete additive subgroup, 390, 455
- discrete dynamical system, 254
- discrete logarithm, 65
  - coverts product to sum, 65, 108, 311
  - defined modulo order of base, 65, 107
  - irregular behavior, 66
  - is even if and only if has square root, 108
  - is homomorphism, 110
  - of a power, 108
- discrete logarithm problem (DLP), 64–67, 357
  - babystep–giantstep algorithm, 82
  - base not a primitive root, 66
  - base of prime power order, 91
  - bit security, 176, 190
  - black box, 253
  - brute-force algorithm, 81
  - collision algorithm, 81, 251, 293
  - Elgamal digital signature, 199
  - elliptic curve, *see* elliptic curve
    - discrete logarithm problem
  - finite field, 65
  - for addition modulo  $p$ , 81
  - group, 67
  - how hard is the . . . , 77
  - hyperelliptic curve, 349, 495
  - index calculus, 166, 316, 348
  - is  $\mathcal{NP}$ , 281
  - parity computed using quadratic reciprocity, 176
  - Pohlig–Hellman algorithm, 89
  - Pollard  $\rho$  algorithm, 259
  - quantum algorithm, 498
  - time to solve, 80
- discriminant, 494
  - cubic polynomial, 303, 361
  - elliptic curve, 303, 330
  - equal to zero, 361
- disjoint events, 230, 289
- distortion map, 350, 356, 359, 369
  - for  $y^2 = x^3 + x$ , 352, 354, 370
  - for  $y^2 = x^3 + 1$ , 370
- distribution
  - binomial, 239, 292
  - function, 239, 431
  - geometric, 240
  - hypergeometric, 240
  - uniform, 239
- distributive law, 95
- divisibility, 10, 96
  - properties of, 11, 49
- division with remainder, 12, 49–51, 99
  - computing on a calculator, 15
- divisor, 338, 495
  - common, 11, 100
  - degree of, 339, 495
  - group of, 495
  - is divisor of rational function if . . . , 339
  - linearly equivalent, 495
  - of degree zero, 495
  - of product is sum of, 368
  - on elliptic curve, 339
  - on hyperelliptic curve, 495
  - sum of, 339
- DLP, *see* discrete logarithm problem
- dot product, 336, 385
- double-and-add algorithm, 312, 313
  - ternary method, 314
- Doyle, Sir Arthur Conan , 10
- DSA, *see* Digital Signature Algorithm
- DSS, *see* Digital Signature Standard
- Dwork, Cynthia, 282, 407, 408
- dynamical system, 254
- ECC, 316–321
  - Chaldean poetry, 323
  - Diffie–Hellman key exchange, 316, 363
  - Elgamal, 319
  - invention of, 322
  - message expansion, 320
  - point compression, 321, 363

- send only  $x$  coordinate, 318, 321, 363
  - versus RSA, 323
- ECDHP, *see* elliptic curve
  - Diffie–Hellman problem
- ECDLP, *see* elliptic curve discrete logarithm problem
- ECDSA, *see* elliptic curve digital signature algorithm
- efficiency versus security, 218
- Einstein, Albert, 298
- Elements*, of Euclid, 26, 54
- Elgamal, 70–73, 483
  - Diffie–Hellman oracle decrypts, 109
  - digital signature, 198
    - discrete logarithm problem, 199
    - forged on random document, 205
    - random element, 199
    - repeated use of random element, 205
    - signature length, 201
  - elliptic, 319
  - hyperelliptic, 496
  - is probabilistic, 180
  - man-in-the-middle attack, 183
  - Menezes–Vanstone variant, 364, 365
  - message expansion, 72, 320
  - oracle solves Diffie–Hellman problem, 73
  - public parameters, 70
  - random element, 475
  - send only  $x$  coordinate, 321, 363
- Elgamal, Taher, 70
- elimination step in linear algebra, 146
- Elkies, Noam, 310
- elliptic curve, 299, 303
  - adding point to reflection, 303
  - adding point to self, 301
  - addition law, 300, 303, 304
    - formulas, 305, 325
    - works over finite field, 307
  - anomalous, 349
  - basis problem, 362
  - bilinear pairing, 336
  - cryptography, *see* ECC
  - degree of divisor, 339
  - Diffie–Hellman problem, 318
  - discriminant, 303, 330
  - distortion map, 350, 356, 359, 369
    - for  $y^2 = x^3 + x$ , 352, 354, 370
    - for  $y^2 = x^3 + 1$ , 370
  - divisor, 339
    - is divisor of rational function if . . . , 339
    - of rational function, 338
  - double-and-add algorithm, 312, 313
  - embedding degree, 347
  - example over  $\mathbb{F}_8$ , 331
  - factorization algorithm, 321, 324–329
    - running time, 329
  - Frobenius-and-add algorithm, 335, 367
  - Frobenius map, 332
  - Frobenius used to count points, 333
  - generalized Weierstrass equation, 330, 365
  - genus one, 494
  - Hasse theorem, 309, 330
  - homomorphism, 353
  - is not an ellipse, 299
  - isogeny, 353
  - Koblitz, 334, 366
  - Miller algorithm, 343, 355
  - modified Weil pairing, 352, 356, 359
  - number of points in finite field, 309, 330
  - order of point, 311
  - over field with  $p^k$  elements, 330
  - over finite field, 306
  - point at infinity, 303
  - point counting, 310, 335
  - point of finite order, 337
  - point operation, 313
  - rational function, 338
    - with no zeros or poles, 339
  - Satoh algorithm, 335
  - SEA algorithm, 310, 335
  - singular point, 361
  - sum of divisor, 339
  - supersingular, 323, 349
  - Tate pairing, 346
  - torsion point, 337
  - torsion subgroup structure, 337
  - Weierstrass equation, 299, 330

- Weil pairing, 340
  - zero discriminant, 361
- elliptic curve cryptography, *see* ECC
- Elliptic Curve Digital Signature
  - Algorithm (ECDSA), 203, 321, 322, 488
- elliptic curve discrete logarithm, 311
  - defined modulo order of  $P$ , 311
  - takes sum to sum, 311
- elliptic curve discrete logarithm
  - problem, 81, 310, 311, 357
  - how hard is the... , 315
  - is homomorphism, 311
  - MOV algorithm, 323, 348, 370
  - on anomalous curve, 349
  - Pollard  $\rho$  algorithm, 363
  - quantum algorithm, 498
  - Weil descent, 349
- elliptic Diffie–Hellman decision
  - problem, 369
- elliptic Diffie–Hellman problem, 318
- Ellis, James, 61
- embedding degree, 347
  - prime, 347
  - small, 349
- encoding scheme, 39–40
- encryption exponent, 125, 182
- encryption function, 3, 46, 63, 211
  - ECC, 319
  - Elgamal, 70
  - GGH, 410
  - is a function, 37
  - knapsack, 380
  - NTRU, 418
  - RSA, 124
- encryption table, 3
- English frequency table, 6, 219
- Enigma machine, 36
- entropy, 263, 269, 270, 297
  - bigram, 276, 298
  - conditional, 274
  - equivocation, 274, 298
  - for key, plaintext, and ciphertext, 274
  - is at most  $\log_2 n$ , 273
  - is sum of  $p \log p$ , 271
  - measures uncertainty, 272
  - of a language, 276
  - of a single letter, 275
  - properties of, 270
  - trigram, 276, 298
- equivocation, 274, 298
  - key, 274, 298
- Eratosthenes, sieve of, 156
- Erdős, Paul, 151
- escrow, key, 107
- Euclid, 26, 54
- Euclidean algorithm, 13, 50, 145, 279
  - extended, 16, 27, 29, 50, 81, 100, 102, 120, 260, 325, 351, 415
  - running time, 13, 15
- Euclidean norm, 386
- Euclidean ring, 99
- Euler formula, 118, 121, 181, 197
- Euler  $\phi$  function, 22, 34, 52, 181
  - product formula for, 181
  - value at prime, 181
- Eve, 2
- even integer, 11
- event, 228, 229
  - compound, 229
  - disjoint, 230, 289
  - independent, 229, 232, 241, 244
  - pairwise disjoint, 289
- exclusive or, 44, 58, 59, 359, 473
- exhaustive search attack, 41
- expected value, 244
  - alternative formula, 292
  - binomial distribution, 292
  - of geometric distribution, 245
  - of uniform distribution, 245, 292
- experiment, 209
- exponent of a prime dividing a number, 28
- exponential growth, 153
- exponential time algorithm, 80, 136
- exponentiation to a negative power, 76
- export of cryptographic algorithms, 62, 107
- extended Euclidean algorithm, 16, 27, 50, 81, 90, 120, 260, 325, 351
  - box method, 18, 416
  - computes inverses modulo  $p$ , 29, 54
  - for polynomial ring, 100, 102, 415
- factor base, 157, 169
- factorial, 31
  - gamma function interpolates, 400

- number of permutations, 210
- Stirling's formula, 139, 400, 424
- factorization
  - elimination step, 145
  - gcd step, 145
  - harder than roots mod  $N$ ?, 126
  - Lenstra elliptic curve algorithm, 321, 324–329
    - running time, 329
  - linear algebra elimination step, 146
  - number field sieve, 162
  - number of relations needed, 154
  - Pollard  $p - 1$  algorithm, 137, 139, 322, 324
  - Pollard  $\rho$  algorithm, 295
  - probability of success, 144
  - quadratic sieve, 155
  - running time, 154, 155
  - subexponential algorithm, 154
  - three step procedure, 143
  - unique, 27
  - via difference of squares, 141, 143
- fast Fourier transform, 498
- fast powering algorithm, 24, 25, 53, 251, 281
  - computes inverses modulo  $p$ , 32, 54
  - double-and-add, 312
- Fermat little theorem, 30, 33, 117–119, 129, 170, 284, 324
  - Euler formula generalizes, 118, 181
  - generalization to finite field, 107
- FHE scheme, 490
- field, 29, 96
  - characteristic, 115
  - examples of, 29, 96
  - finite, 29
  - Galois, 106
  - quotient polynomial ring, 104
    - with  $2^d$  elements, 106
    - with  $p^2$  elements, 105, 330, 336, 354
    - with  $p^d$  elements, 104, 106, 329
- finite field, 29
  - characteristic, 115
  - discrete logarithm problem, 65–66
  - elliptic curve over, 306
  - exponentiation, 74
  - Frobenius map, 332
  - Galois group, 332
  - generalization of Fermat little theorem, 107
  - generator of  $\mathbb{F}_p^*$ , 33, 54, 55
  - has element of order  $N$  for  $N \mid p - 1$ , 112
  - has prime power number of elements, 115
  - isomorphic, 106
  - linear algebra over, 146
  - multiplicative inverse, 29, 32, 54
  - number of primitive roots, 34
  - order of an element, 32, 54
  - powers in, 29–34
  - primitive root, 33, 54, 55, 107, 114, 170, 354
  - quadratic residue, 169, 309
  - square root, 55, 86, 108, 158, 161, 169, 190, 309, 363
  - two with same number of elements, 106
    - used in AES, 501
    - with  $2^d$  elements, 106
    - with 49 elements, 114
    - with 8 elements, 114
    - with  $p^2$  elements, 105, 330, 336, 354
    - with  $p^d$  elements, 104, 106, 329
- finite group, 74
- finite order, 76
  - point on elliptic curve, 337
- forgery on random document, 205
- formal language, 280
- fraction modulo  $m$ , 21
- Franklin, Matthew, 359
- frequency analysis, 6, 215
- frequency table, 6, 48, 219
- Frey, Gerhard, 349
- Friedman, William, 36
- Frobenius-and-add algorithm, 335, 367
- Frobenius map, 113, 332
  - elliptic curve, 332
  - is field automorphism, 332, 366
  - is homomorphism, 333
  - respects elliptic curve addition, 333, 366
  - trace of, 309, 362
  - used to count points, 333
- fully homomorphic encryption, 490
- function

- bijjective, 210
- concave, 272
- encryption/decryption, 3, 46, 63, 211
- exponential growth, 153
- iteration of, 254
- one-to-one, 3, 210, 265
- one-way, 63
- onto, 210
- polynomial growth, 153
- rational, 338, 368, 495
- subexponential growth, 153
- trapdoor, 63
- fundamental domain, 390, 431
  - all have same volume, 394
  - determinant formula for volume, 393
  - translates cover  $\mathbb{R}^n$ , 390, 398, 404, 457
  - volume, 392, 457
- fundamental parallelepiped, 390
- fundamental theorem of arithmetic, 27
- Galois, Évariste, 29, 106
- Galois field, 29, 106
- Galois group, 332
  - Weil pairing invariant for, 342
- gamma function, 400
  - interpolates factorial, 400
  - Stirling's formula, 400
- Gaudry, P., 496
- Gaussian elimination, 146, 481
  - modulo composite number, 167
- Gaussian heuristic, 400, 402, 447
  - exact value, 402
  - for CVP, 403
  - NTRU lattice, 427
  - subset sum lattice, 403, 451
- Gaussian lattice reduction, 436, 437
  - solves SVP, 437
- gcd, *see* greatest common divisor
- general linear group, 75, 110, 390, 456
- generalized Weierstrass equation, 330, 365
- Gentry, C., 491
- genus, 494
- geometric distribution, 240
  - expected value, 245
- geometric progression, 241
- geometric series, 292
- GGH, 407, 409, 410
  - digital signature, 428, 429
  - transcript attack, 430
- is probabilistic, 412
- lattice reduction attack, 452
- public key size, 408
- random element, 409
- repeated plaintext, 458
- repeated random element, 412, 458
- Gilbert, W.S., 213
- GIMPS, 186
- $GL_n$ , *see* general linear group
- $GL_n(\mathbb{Z})$ , 390, 456
- Gödel incompleteness, 278
- Goldreich, Oded, 407
- Goldwasser–Micali public key cryptosystem, 88, 178
  - message expansion, 180
- Goldwasser, Shafi, 407
- good basis, 405
- Gram matrix, 456
- Gram–Schmidt algorithm, 387, 439
  - determinant of basis, 439
- Granville, Andrew, 130
- great Internet Mersenne prime search, 186
- greatest common divisor, 11, 100
  - equals  $au + bv$ , 16, 27, 29, 50, 54, 100
  - Euclidean algorithm, 13, 50, 145
  - of relatively prime integers, 17
  - polynomial ring, 103
  - solve  $au + bv$  efficiently, 50
- greatest integer function, 53, 59, 157
- group, 74–77
  - abelian, 74, 304
  - commutative, 74, 304
  - discrete logarithm problem, 67
  - elements of order dividing  $d$ , 109
  - examples of, 75
  - finite, 74
  - general linear, 390, 456
  - homomorphism, 110, 311
  - Lagrange theorem, 76
  - noncommutative, 75
  - of divisors, 495
  - of points on elliptic curve, 304

- of tuples on hyperelliptic curve, 495
- order of, 74
- order of element, 76
- order of element divides order of group, 76
- Pohlig–Hellman algorithm, 89
- group exponentiation, 75
- group of units, 22, 52
- Gulliver’s Travels*, 486
  
- $H$  (entropy), 270
- Hadamard inequality, 393, 397, 439
- Hadamard ratio, 397, 407, 409, 447, 453
  - reciprocal of orthogonality defect, 397
- Halevi, Shai, 407
- halting problem, 278
  - is  $\mathcal{NP}$ -hard, 280
- hardest case versus average case
  - equivalence, 282, 408
- hash function, 196, 359, 429, 472
  - collision resistant, 196, 472
  - difficult to invert, 472
  - rounds, 474
  - used to build PRNG, 476
- Hasse, Helmut, 309
- Hasse theorem, 309, 330, 333
- HCC, *see* hyperelliptic curve cryptography
- HCDLP, *see* hyperelliptic curve discrete logarithm problem
- Heisenberg uncertainty principle, 499
- Hellman, Martin, 45, 61, 282, 377, 380
- Hermite constant, 397
- Hermite theorem, 396, 397, 399
- hexadecimal, 40
- Hilbert question, 278
- Hilbert space, 497
- Hill cipher, 43, 57
- Hoffstein, Jeffrey, 407
- homomorphic encryption, 490
- homomorphism, 110, 113, 311, 353, 490
  - Frobenius, 113
  - Frobenius map is, 333
  - group, 110
  - ring, 111, 414
- homophonic substitution cipher, 34, 56
- Huang, M., 496
  
- hyperelliptic curve, 349, 494
  - addition law, 495
  - divisor, 495
  - divisor group, 495
  - Jacobian variety, 495
  - number of points in finite field, 496
- hyperelliptic curve cryptography, 494
  - has shorter signatures, 496
- hyperelliptic curve discrete logarithm problem, 349, 495
  - index calculus, 496
  - MOV algorithm, 496
  - solution for big  $p$ , 496
- hyperelliptic Diffie–Hellman key exchange, 496
- hyperelliptic Elgamal public key cryptosystem, 496
- hypergeometric distribution, 240
  
- IATR, 107
- IBM, 499
- ID-based cryptography, 358
  - hash function, 359, 360
  - random element, 359
- ideal, 98
- identification scheme, 481
- identity law, 74, 95, 304
- IEEE, 487
- IETF, 487
- IFP, *see* integer factorization problem
- implementation, 126
- inclusion–exclusion principle, 288
- independent events, 229, 232, 241, 244
- independent vectors, 384
- index, 65, 167
- index calculus, 80, 166–169, 201, 348
  - factor base, 169
  - none known for ECDLP, 316
  - running time, 169
  - subexponential algorithm, 169
- index of coincidence, 219, 285, 287
  - for bigrams, 286
  - formula for, 220
  - mutual, 221, 285–287
- infinite order, 76
- infinite series
  - differentiation trick, 245, 292
  - geometric, 292
- infinity, point at, 303



- information theory, 263
- injective function, 3, 210, 265
- integer, 10
  - divisibility, 10
  - division with remainder, 12, 49–51
  - even/odd, 11
  - greatest common divisor, 11
  - modulo  $m$ , 21
  - order of  $p$  in, 28
  - relatively prime, 17
  - unique factorization of, 27
- integer factorization problem, 79
  - is  $\mathcal{NP}$ , 281
  - quantum algorithm, 498
  - subexponential algorithm, 154
- integral lattice, 389
- international traffic in arms regulations (IATR), 107
- interpolation polynomial, 481
- intersection, 231
  - probability of, 231–233
- inverse
  - in convolution polynomial ring, 415, 460
    - looks random, 420
  - in polynomial ring, 101, 113
  - of a matrix, 456
- inverse law, 74, 95, 304
- inverse modulo  $m$ , 20
- inverse modulo  $p$ , 28, 29, 32, 54
- irreducible element, 97
- irreducible polynomial, 102
  - depends on coefficient ring, 101
  - of every degree exists, 106
  - quotient ring is field, 104
- isogeny, 353
- isomorphism, 106
- iteration, 254
- Jacobi symbol, 174, 179
  - multiplication formula, 175
  - quadratic reciprocity, 175
- Jacobian variety, 495
  - group of points with coordinates in  $\mathbb{F}_p$ , 495
- Jaynes, E.T., 263
- Jensen inequality, 272, 297
- joint density function, 241
  - for key, plaintext, and ciphertext, 264
- Joux, Antoine, 356
- Kasiski, Friedrich, 219
- Kasiski method, 219, 286
- Kayal, N., 136, 281
- Kerckhoff's principle, 38, 41
- ket notation, 497
- key, 5, 44
  - asymmetric cipher, 46, 63
  - blocksize, 41
  - creation uses random number, 475
  - ECC, 319
  - Elgamal, 70
  - entropy, 274
  - equivocation, 274, 298
  - GGH, 409
  - knapsack, 380
  - NTRU, 417
  - private/public, 46, 63
  - random variable, 264
  - RSA, 124
  - space of, 37
  - substitution cipher, 5
  - used once, 269
- key escrow, 107
- key exchange
  - Diffie–Hellman, 67, 496
  - elliptic Diffie–Hellman, 316, 363
  - tripartite Diffie–Hellman, 356, 370, 371
- key recovery problem for NTRU, 422
- knapsack cryptosystem, 64, 282, 380, 381
  - faster than RSA, 382
  - lattice reduction attack, 451
  - message expansion, 382
- knapsack problem, 377
  - Pollard  $\rho$  algorithm, 455
- known plaintext attack, 38, 59, 288
- Koblitz curve, 334, 366
  - Frobenius-and-add algorithm, 335, 367
- Koblitz, Neal, 322, 332, 485
- Korkin–Zolotarev reduced basis, 449
- Korselt criterion, 184
- kryptos, 2
- KZ reduced basis, 449

- $L(X)$ , 151
  - is subexponential, 153, 188
- $L_\epsilon(X)$ , 165
- Lagarias, Jeffrey, 383
- Lagrange interpolation polynomial, 481
- Lagrange theorem, 30, 76, 107
- lambda calculus, 278
- language, 280
  - entropy of, 276
- lattice, 373, 388
  - all fundamental domains have same volume, 394
  - approximate closest vector problem, 396
  - approximate shortest vector problem, 396
  - associated to subset-sum problem, 383, 403, 451
  - Babai algorithm, 403
  - basis, 388
  - change-of-basis formula, 388
  - change-of-basis matrix, 388
  - closest vector problem, 395
  - covolume, 392
  - determinant, 392
    - for  $m \neq n$ , 457
  - digital signature, 428
  - dimension, 388
  - fundamental domain, 390, 431
  - Gaussian heuristic, 400, 402, 447
    - for CVP, 403
  - Gram matrix of basis, 456
  - Gram–Schmidt basis has same determinant, 439
  - Hadamard inequality, 393, 439
  - Hadamard ratio, 397, 407, 409, 447, 453
  - Hermite theorem, 396, 397, 399
  - integral, 389
  - is discrete additive subgroup, 390, 455
  - Korkin–Zolotarev reduced basis, 449
  - large symmetric convex set
    - contains lattice point, 398
  - Minkowski theorem, 396, 398, 401
  - NTRU, 409, 425
    - orthogonality defect, 397
    - quasi-orthogonal basis, 448, 452, 453, 467, 468
    - reduction, *see* lattice reduction
    - shortest basis problem, 396
    - shortest vector problem, 395
    - translates of  $\mathcal{F}$  cover  $\mathbb{R}^n$ , 390, 398, 404, 457
    - volume, 392
- lattice-based cryptosystems, 407
  - faster than RSA and ECC, 408
- lattice problem
  - CVP average case versus hardest case, 408
- lattice reduction, 384, 436
  - attack on congruential cryptosystem, 376, 451
  - attack on GGH, 452
  - attack on knapsack cryptosystem, 451
  - attack on NTRU, 453
  - attack on RSA, 450
  - BKZ-LLL, 449, 450
  - CVP average case versus hardest case, 282
  - efficient implementation of LLL, 466
  - finding very short vectors, 428
  - Gaussian, 436, 437
  - LLL, 439
    - matrix scaling, 452
  - leading coefficient, 98
  - learning with errors, 434
  - least common multiple, 188
- Legendre symbol, 171
  - computes parity of discrete logarithm, 176
  - Jacobi symbol, 174
  - multiplication formula, 172
- length, 386
- Lenstra factorization algorithm, 321, 324–329
  - running time, 329
- Lenstra, Arjen, 383
- Lenstra, Hendrik, 321, 325, 383
- L'Hôpital's rule, 79
- $\text{Li}(X)$ , 185
- Lichtenbaum pairing, 346
- linear algebra, 146, 384–387, 481

- modulo composite number, 167
  - sparse system of equations, 150
- linear combination, 384
- linear equivalence, 495
- linear time algorithm, 80
- little-endian, 486
- little theorem (of Fermat), *see* Fermat
  - little theorem
- little- $o$  notation, 151
- LLL algorithm, 384, 427, 443, 444
  - attack on congruential cryptosystem, 451
  - attack on GHG, 452
  - attack on knapsack cryptosystem, 451
  - attack on NTRU, 453
  - attack on RSA, 450
  - deep insertion method, 449
  - efficient implementation, 443, 466
  - finding very short vectors, 428
  - is polynomial-time, 443
  - Lovász condition, 440, 467
  - matrix scaling, 452
  - running time, 443, 446
  - size condition, 440
  - subset-sum problem solution, 451
  - swap step, 443
- LLL reduced basis, 440
  - properties of, 441
- logarithm
  - complex, 65, 311
  - discrete, *see* discrete logarithm
  - is concave, 273, 297
- logarithmic integral, 135, 185
- Lovász condition, 440
  - relaxed, 467
- Lovász, L., 383
- LWE, 434
- machine cipher, 36
- Major General Stanley, 213
- man-in-the-middle attack, 126, 183
- master key, 358
- matrix, 43, 57
  - adjoint, 388, 455
  - formula for inverse, 456
- mean, 244
- meet-in-the-middle algorithm, *see* collision algorithm
  - meet-in-the-middle attack, *see* collision algorithm
- Menezes, Alfred, 348, 485
- Menezes–Vanstone Elgamal cryptosystem, 364, 365
- Merkle–Hellman cryptosystem, 380, 381
- Merkle, Ralph, 61, 282, 377, 380
- Mersenne prime, 186
- message expansion, 72
  - Elgamal, 72
  - elliptic Elgamal, 320
  - Goldwasser–Micali, 180
  - MV-Elgamal, 364
  - NTRU, 462
  - subset-sum cryptosystem, 382
- Micciancio, Daniele, 408
- Millennium Prize, 64, 135, 280
- Miller algorithm, 343, 355
  - computes Tate pairing, 346
- Miller, J.C.P., 167
- Miller–Rabin test, 131, 135, 184, 236, 291
  - probability of success, 131, 291
- Miller–Rabin witness, 131
  - smaller than  $2(\ln n)^2$ , 136
- Miller, Victor, 322, 343
- Minkowski theorem, 396, 398, 401
- modified Tate pairing, 346
  - is symmetric, 369
- modified Weil pairing, 352, 356, 359
  - is nondegenerate, 352
- modular arithmetic, 19–22
- modulus, 19
  - RSA, 125
- monic polynomial, 98, 162
- monoalphabetic cipher, 214
- Monte Carlo algorithm, 236, 290, 291, 432
  - Bayes’s formula, 237
- Monty Hall problem, 236, 290
- Moriarty, 213
- MOV algorithm, 323, 348, 370, 496
- Mullin, Ron, 323
- multiplicative inverse
  - exist in field, 96
  - in polynomial ring, 101, 113
  - modulo  $m$ , 20
  - modulo  $p$ , 28, 29, 32, 54
- multiplicity of zero or pole, 338, 495

- munition, cryptographic algorithm is, 62
- mutual index of coincidence, 221, 285–287
- MV-Elgamal cryptosystem, 364, 365
  - message expansion, 364
- National Institute of Standards, 499, 501
- National Security Agency, 62, 499
- natural language, 275
- Nguyen, Phong, 408, 431
- NIST, 499, 501
- noncommutative group, 75
- nondegenerate pairing, 352
- nonresidue, 169, 309
  - is odd power of primitive root, 171
  - Legendre symbol, 171
  - product of two, 170
- norm, 386
  - expected value, 461
  - of product is product of norms, 461
  - sup, 434
- $\mathcal{NP}$ , 278, 279
  - co- $\mathcal{NP}$ , 281
- $\mathcal{NP}$ -complete, 280, 377
  - trapdoor, 281
- $\mathcal{NP}$ -hard, 280, 395
  - randomized reduction hypothesis, 395
  - trapdoor, 281
- NSA, *see* National Security Agency
- NTRU, 323, 407, 416, 417, 483
  - brute-force attack, 423
  - closest vector problem attack on plaintext, 463
  - collision algorithm, 424
  - CVP attack on plaintext, 463
  - decryption failure, 420
  - digital signature
    - transcript attack, 431
  - expected number of decryption keys, 424
  - $\gcd(p, q) = 1$ , 462
  - key recovery problem, 422
  - lattice, *see* NTRU lattice
  - lattice reduction attack, 453
  - matrix, 425
    - abbreviated form, 426
  - modular lattice signature scheme, 434
  - $N$  is prime, 463
  - public key size, 409
  - public parameters, 417, 462, 463
  - random element, 418, 475
    - repeated, 420, 462
  - repeated plaintext, 462
  - rotation of key, 422
  - security determined
    - experimentally, 428
  - speed, 421
    - SVP attack on key, 427
- NTRU lattice, 409, 425
  - abbreviated form, 426
  - contains private key vector, 426
  - contains short vector, 426
  - determinant, 427
  - Gaussian heuristic, 427
  - SVP, 427
- NTRUEncrypt, 416, 417, 419
- NTRUMLS, 434
- number field sieve, 162–165, 169
  - running time, 165
- number theory, 10
- OAEP, 484
- odd integer, 11
- Odlyzko, Andrew, 383, 424
- Okamoto, Tatsuaki, 348
- one-time pad, 44, 45, 269, 476
  - has perfect secrecy, 269
  - VENONA project, 269
- one-to-one function, 3, 210, 265
- one-way function, 45, 63
  - solves  $\mathcal{P} = \mathcal{NP}$  problem, 63
- onto function, 210
- optimal asymmetric encryption
  - padding, 484
- oracle, 73, 127, 482
- orbit, 254
- order
  - infinite, 76
  - notation (big- $\mathcal{O}$ ), *see* order notation
  - of a group, 74
  - of a number modulo a prime, 32, 54

- of a prime dividing a number, 28, 54
- of element divides order of group, 33, 76
- of element of group, 76
- of point on elliptic curve, 311
- $\text{ord}_p$  is valuation, 54
- point of finite, 337
- order notation, 78, 151, 152
  - alternative, 153
  - verify using limit, 78
- orthogonal basis, 386
  - Gram–Schmidt algorithm, 387, 439
  - solves SVP and CVP, 403
- orthogonal complement, 440, 465
- orthogonal projection, 440
- orthogonal vectors, 385
- orthogonality defect, 397
- orthonormal basis, 386
- outcome of an experiment, 209
- $\mathcal{P}$ , 278, 279
- P1363 project, 487
- padding scheme, 482
- pairwise disjoint events, 289
- parallelepiped, 390
- patents in cryptography, 323, 324
- Peeters, M., 474
- perfect secrecy, 264
  - conditions for, 267, 297
  - number of keys  $\geq$  number of plaintexts, 266
  - one-time pad has, 269
  - shift cipher, 265, 296
- zero-knowledge proof, 479
- period of Vigenère cipher, 219
- permutation, 210–211, 283
  - leaving elements fixed, 284
  - of  $n$ , 210
  - there are  $n!$  of  $n$ , 210
  - with some indistinguishable objects, 211, 283
- $\phi$  function, *see* Euler  $\phi$  function
- $\pi(X)$ , 133, 184
- Pipher, Jill, 407
- Pirates of Penzance*, 213
- PKC, *see* public key cryptosystem
- plaintext, 1
  - blocksize, 40
  - entropy, 274
  - random variable, 264
  - space of, 37
- plaintext attack, 38, 59, 288
- $\mathcal{P} = \mathcal{NP}$  problem, 63, 280
- $\mathcal{P} \neq \mathcal{NP}$  problem, 278
- Pohlig–Hellman algorithm, 80, 88, 89, 140, 167, 261
- point at infinity, 303
- point compression, 321, 324, 363
- point of finite order, 337
- polar coordinates, 295
- pole, 338
  - multiplicity, 338, 495
- Pollard  $p - 1$  algorithm, 137, 139, 322, 324
- Pollard  $\rho$  algorithm, 253, 294, 348, 496
  - abstract version, 254, 256
  - discrete logarithm problem, 259
  - expected running time, 256
  - factorization, 295
  - for elliptic curve, 315, 363
  - for subset-sum problem, 455
  - sufficiently random function, 259
- polyalphabetic cipher, 35, 214
- polynomial
  - binary, 417
  - degree, 98
  - discriminant, 494
  - interpolation, 481
  - irreducible, 102
  - leading coefficient, 98
  - monic, 98, 162
  - ternary, 417
  - unique factorization of, 102
  - vector of coefficients, 413
- polynomial growth, 153
- polynomial ring, 96, 98
  - convolution, 412
  - greatest common divisor, 100, 103
  - irreducible polynomial of every degree exists, 106
  - is Euclidean, 99
  - norm of convolution product, 461
  - number of elements in quotient, 103
  - quotient, 102, 162
  - quotient by irreducible is field, 104

- unit, 101, 113
- units in quotient, 103
- polynomial-time algorithm, 80, 137, 279, 281
  - count points on elliptic curve, 310
  - count points on  $j$  elliptic curve, 335
  - LLL, 443
  - to solve decision problem, 279
- polynomial-time reduction, 280
- Pomerance, Carl, 130, 151, 156
- Post correspondence problem, 278
  - bounded, 279
  - is  $\mathcal{NP}$ , 279
- power-smooth number, 187
- primality testing, 128–137, 278
  - AKS test, 137, 279, 281
  - exponential time algorithm, 136
  - polynomial-time algorithm, 137, 279, 281
  - witness for compositeness, 130, 131, 136, 291
- prime, 26
  - congruent to 1 modulo 4, 184
  - congruent to 3 modulo 4, 184
  - counting function, 133, 184
  - dividing a product, 27
  - infinitely many, 26, 54
  - largest known, 186
  - Mersenne, 186
  - Miller–Rabin test, 131, 135, 184, 291
  - order of dividing a number, 28
  - probability of being, 134, 184, 185, 291
  - Riemann hypothesis, 135
  - searching for large, 134
  - tests for, *see* primality testing
  - unique factorization into product of, 27
- prime number theorem, 133, 154, 184
  - implied by Riemann hypothesis, 135
  - logarithmic integral, 186
- primitive cube root of unity, 370
- primitive root, 33, 54, 55, 107, 114, 170, 354
  - even powers are squares, 171
  - number of, 34
- primitive root of unity, 346, 350
- principal ideal, 98
- prisoners problem, 235
- private key, 46, 63
  - ECC, 319
  - Elgamal, 70
  - GGH, 409
  - is trapdoor information, 63
  - knapsack, 380
  - master, 358
  - NTRU, 417
  - RSA, 124
- PRNG, 475
  - based on hard math problem, 477
  - built from hash function, 476
  - built from symmetric cipher, 476
  - cryptographically secure, 476
  - output is not random, 475
  - properties of, 476
  - used to build symmetric cipher, 476
- probabilistic algorithm, *see* Monte Carlo algorithm
- probabilistic encryption, 177, 412, 475
  - changing cryptosystem into, 191, 475, 484
  - Elgamal, 180
- probability
  - conditional, 234
  - of collision, 247
  - of complement, 230, 288
  - of intersection, 231–233
  - of union of disjoint events, 234
  - of union of events, 230, 288
- union of disjoint subevents, 265, 289
- probability density function, 239
- probability distribution
  - binomial, 239, 292
  - function, 239, 431
  - geometric, 240
  - hypergeometric, 240
  - uniform, 239
- probability function, 228, 229
- probability space, 228, 229
- probability theory, 228
  - Bayes’s formula, 234, 243, 264
  - card problem, 231, 249, 293
  - coin toss experiment, 233, 240, 288, 289
  - conditional density function, 241

- entropy, 270
- expected value, 244
- is axiomatic theory, 229
- joint density function, 241
- random variable, 238
- urn problem, 228, 235, 240, 242, 247, 289
- projection map, 449
- protocol, 486
- provable security, 482, 485
- pseudorandom number, 70
- pseudorandom number generator, *see* PRNG
- pseudorandom sequence, 45
- public key, 46, 63
  - ECC, 319
  - Elgamal, 70
  - GGH, 408, 409
  - knapsack, 380
  - master, 358
  - NTRU, 409, 418
  - RSA, 124
- public key cryptosystem, 46, 63
  - bank vault analogy, 193
  - congruential, 373
  - Elgamal, 70, 496
  - elliptic Elgamal, 319
  - GGH, 407, 409, 410
  - Goldwasser–Micali, 178
  - hyperelliptic, 494
  - ID-based, 358
  - key exchange, 67, 316, 356, 363, 370, 371, 496
  - knapsack, 282, 380, 381
  - multistep, 109, 363
  - MV-Elgamal, 364, 365
  - NTRU, 323, 407, 416, 417, 419
  - probabilistic, 177, 412
  - RSA, 124
- purple cipher machine, 36
- quadratic nonresidue, 169
- quadratic reciprocity, 172, 190, 354
  - computes parity of discrete logarithm, 176
  - Jacobi symbol version, 175
- quadratic residue, 169, 309
  - is even power of primitive root, 171
  - Legendre symbol, 171
  - modulo  $pq$ , 176, 177
  - product of two, 170
  - zero-knowledge proof, 477
- quadratic sieve, 155–162
  - factor base, 157
  - implementation tricks, 161
  - running time, 161, 329
- quadratic-time algorithm, 80
- quantum bit, 497
- quantum computing, 373, 497
- quantum cryptography, 499
- quantum entanglement, 499
- quantum state, 498
- quantum theory generates random bits, 475
- quasi-orthogonal basis, 448, 452, 453, 467, 468
- qubit, 497
- quotient polynomial ring, 102, 162
  - by irreducible is field, 104
  - number of elements, 103
  - units in, 103
- quotient ring, 22, 98
- Rabin cryptosystem, 483
- radio frequency identification tag, 496
- random element, 71, 199, 201, 319, 359, 374, 409, 418
  - danger if repeated, 205, 412, 420, 458, 462
  - random number generation, 475
- random number, 45, 70, 474
  - quantum theory generates, 475
- random oracle model, 482, 484
- random perturbation, 409, 412
- random variable, 238
  - entropy, 270
  - expected value, 244
  - for key, plaintext, and ciphertext, 264
  - independent events, 244
  - probability density function, 239
- rational function, 338
  - divisor, 338, 495
  - pole, 338, 495
  - with no zeros or poles, 339
  - with same divisor, 339
  - zero, 338, 495
- rational numbers, 29

- real numbers, 29
- reciprocity, *see* quadratic reciprocity
- reduced basis, 440
  - properties of, 441
- redundancy, 275
- Regev, Oded, 431
- rejection sampling, 431
- relation building, 143
  - number of relations needed, 154
  - quadratic sieve, 155
  - running time, 154, 155
- relatively prime, 17
- remainder, 12, 99
- residue, 169, 309
  - cubic, 190
- restricted choice, 290
- RFC, 487
- RFID tag, 496
- Rhind papyrus, 282
- $\rho$  algorithm, *see* Pollard  $\rho$  algorithm
- Riemann hypothesis, 135
  - generalized, 136
  - implies prime number theorem, 135
- Rijmen, V., 501
- Rijndael, 501
- ring, 10, 95
  - commutative with identity, 95
  - divisibility, 96
  - division with remainder, 99
  - Euclidean, 99
  - examples of, 96
  - greatest common divisor, 100
  - homomorphism, 111, 113, 414, 490
  - ideal, 98
  - identity is unique, 113
  - infinitely many units, 164
  - inverse is unique, 113
  - irreducible element, 97
  - is field if inverses exist, 96
  - modulo  $m$ , 98
  - of integers modulo  $m$ , 21
  - of polynomials with coefficients in, 98
  - polynomial, 96
  - quotient, 22, 98
  - unit, 22, 97
  - zero divisor, 97, 104, 113
- Rivest, Ron, 61, 123
- Rogaway, Phillip, 484
- root
  - modulo  $N$ , 181
    - easier than factorization?, 126
  - modulo  $p$ , 119
  - modulo  $pq$ , 120, 180
- root of unity, 346, 350
  - cube, 370
- rotation, 422
- Rosencrantz and Guildenstern Are Dead*, 240
- rounds, 474
  - zero-knowledge proof, 477
- RSA, 64, 70, 123–126, 483
  - blinded digital signature, 487
  - break if know
    - encryption/decryption pair, 182, 184
  - breaking equivalent to factoring?, 126
  - decryption exponent, 125, 182
  - different exponent attack, 183
  - digital signature, 196, 197
  - encryption exponent, 125
  - lattice reduction attack, 450
  - man-in-the-middle attack, 183
  - modulus, 125
  - multiple exponent attack, 128
  - oracle attack, 127
  - patented cryptosystem, 323, 324
  - security depends on dichotomy, 123
  - small decryption exponent, 125
  - small encryption exponent, 125
  - versus ECC, 323
- running time, 13, 15, 26, 79–82, 89, 90, 136, 154, 155, 161, 165, 169, 250, 256, 329, 427, 428, 443, 446, 450
- Saint Ives riddle, 208, 283
- sample space, 228, 229, 238
- satisfiability (SAT), 280
- Satoh algorithm, 335
- Satoh, Takakazu, 335
- Saxena, N., 136, 281
- S-box, 500, 501
- SBP, *see* shortest basis problem
- Schoof algorithm, 310
- Schoof, Rene, 310
- SEA algorithm, 310, 335



- second derivative test, 272, 297
- secrecy system, 277
- secret sharing scheme, 480
  - Shamir, 480
  - threshold, 480
- Secure Hash Algorithm, *see* SHA
- security versus efficiency, 218
- sequence, superincreasing, 378, 379
- series
  - differentiation trick, 292
  - geometric, 292
- SHA, 473–474
  - competition to choose new, 474
- Shamir secret sharing scheme, 480
- Shamir, Adi, 61, 123, 359, 383, 480, 500
- Shanks’s babystep–giantstep algorithm, 82
- Shannon, Claude, 263, 269
- Sherlock Holmes, 213
- shift cipher, 2, 23, 34
  - entropy, 274
  - perfect security, 265, 296
- Shor algorithm, 498
- Shor, Peter, 498
- shortest basis problem, 396
- shortest vector problem, 395, 483
  - approximate, 396
  - BKZ-LLL solves approximate, 450
  - cryptosystems based on, 407
  - Gaussian lattice reduction solves, 437
  - Hermite theorem, 397
  - is  $\mathcal{NP}$ -hard, 395
  - LLL solves approximate, 443
  - no harder than CVP, 395
  - no quantum algorithm known, 498
  - NTRU lattice, 427
  - solution  $\leq \sqrt{n} \det(L)^{1/n}$ , 397
  - subset-sum lattice, 403, 451
- Shoup, Victor, 485
- sieve, 150
  - factor base, 157
  - index calculus, 169
  - number field, 162–165, 169
  - of Eratosthenes, 156
  - quadratic, 155–162
  - running time, 161, 165, 329
- signature, *see* digital signature
- signer, 193
- signet ring, 193
- signing algorithm, 194
- signing exponent, 196
- signing key, 194
- Silverman, Joseph, 407
- simple substitution cipher, *see* substitution cipher
- singular point, 361
- size condition, 440
- smooth number, 141, 150
  - counting function, 150, 151
  - power, 187
- soundness, 477
- span, 384
- sparse system of linear equations, 150
- square-and-multiply algorithm, 25, 53, 312
  - computes inverses modulo  $p$ , 32, 54
- square root
  - in finite field, 55, 158, 161, 169, 190, 309, 363
  - modulo  $m$ , 87
  - modulo  $p$ , 55, 86, 108, 158, 161
    - for  $p \equiv 3 \pmod{4}$ , 86, 190, 363
  - modulo  $p^e$ , 55, 112, 161
  - modulo  $pq$ , 176, 177
- square root algorithm, *see* collision algorithm
- standard model, 485
- standard setting body, 486
- Standards for Efficient Cryptography, 488
- statistical zero-knowledge proof, 479
- Stirling’s formula, 139, 400, 424
- Stoppard, Tom, 240
- subexponential growth, 153
  - $L(X)$ , 153, 188
- subexponential-time algorithm, 80, 154, 161, 165, 169, 329
- subset-sum cryptosystem, 282, 380, 381
  - faster than RSA, 382
  - message expansion, 382
- subset-sum lattice, 383
  - Gaussian heuristic, 403, 451
- subset-sum problem, 282, 377
  - associated lattice, 383, 403, 451
  - collision algorithm, 377
  - disguised by congruence, 380
  - is  $\mathcal{NP}$ -complete, 282

- LLL solution, 451
- Pollard  $\rho$  algorithm, 455
- superincreasing, 379
- substitution box, 500
- substitution cipher, 2, 34, 48, 211, 263, 285
  - cryptanalysis of, 4–10
  - homophonic, 34, 56
  - key, 5
  - number of, 4, 49
- Sullivan, A., 213
- sum of points in divisor, 339
- Sun Tzu Suan Ching*, 84, 111
- sup norm, 434
- superexponential growth, 188
- superincreasing sequence, 378
- superincreasing subset-sum problem, 379
- superposition of states, 498
- supersingular elliptic curve, 323, 349
- SVP, *see* shortest vector problem
- swap step in LLL, 443
- symmetric cipher, 37–39, 263, 499
  - built from PRNG, 476
  - examples, 41
  - key, 44
  - one-time pad, 44, 476
  - used to build PRNG, 476
- symmetric group, 109
- symmetric set, 398
- tableau, Vigenère, 216, 284, 285
- Tate–Lichtenbaum pairing, 346
- Tate pairing, 346, 496
  - is bilinear, 346
  - is nondegenerate, 346
  - Miller algorithm, 346
  - modified, 346, 369
  - related to Weil pairing, 369
- $\tau$ -adic expansion, 335, 367
- ternary expansion, 314, 363
- ternary polynomial, 417
  - number of, 423, 424
- Teske, Edlyn, 259
- thermodynamics, 263
- three prisoners problem, 235
- threshold secret sharing scheme, 480
- Tom (trusted authority), 358
- torsion point, 337
  - embedding degree, 347
- totient function, *see* Euler  $\phi$  function
- trace of Frobenius, 309, 362
- transcript attack, 195, 430, 431
- transposition cipher, 34, 56
- trapdoor function, 47, 63
  - $\mathcal{NP}$ -hard problem, 281
- trigram, 223, 224, 275, 286
  - entropy, 276, 298
- ternary expansion, *see* ternary expansion
- ternary polynomial, 417
- tripartite Diffie–Hellman key exchange, 356, 370, 371
- triple DES, 500
- trusted authority, 358, 481
- Turing, Alan, 278
- ULTRA project, 36
- uncertainty, 272
- undecidable problem, 278
  - Post correspondence problem, 278
- uniform distribution, 239
  - expected value, 245, 292
- union, probability of, 230, 288
- unique factorization, 27, 102
  - fails in  $\mathbb{Z}[\beta]$ , 164
- unit, 22, 97
  - in polynomial ring, 101, 113
  - infinitely many, 164
  - product of two is, 52
- unitary linear transformation, 498
- United States Patents and Trademark Office, 324
- urn problem, 228, 235, 240, 242, 247, 289
- USPTO, 324
- valuation, 54
- Van Assche, G., 474
- Vanstone, Scott, 323, 348
- vector, 43, 115, 147, 373, 384
  - angle between, 386
  - independence of, 384
  - norm, 386
  - of coefficients of polynomial, 413
  - orthogonal, 385
  - orthogonal projection, 436
- vector space, 115, 147, 373, 384

- angle between vectors, 386
- basis, 385
- bounded set, 398
- Cauchy–Schwarz inequality, 386
- change-of-basis formula, 385
- closed ball, 397
- closed set, 398
- convex set, 398
- convolution product, 414
- dimension, 385
- direct sum, 465
- discrete additive subgroup, 390, 455
- dot product, 385
- Gram–Schmidt algorithm, 387, 439
- norm of vector, 386
- orthogonal basis, 386
- orthogonal complement, 440, 465
- orthogonal projection, 440
- orthogonality, 385
- orthonormal basis, 386
- projection map, 449
- symmetric set, 398
- volume of ball, 400
- VENONA project, 269
- verification algorithm, 194
- verification exponent, 196
- verification key, 194
- verifier, 193
- Vernam’s one-time pad, 44, 269, 476
  - has perfect secrecy, 269
- Verne, Jules, 298
- Vigenère cipher, 35, 214–227, 263, 284–287
  - blocksize, 219
  - cryptanalysis, 218
  - Kasiski method, 219, 286
- Vigenère tableau, 216, 284, 285
- Vigenère, Blaise de, 214, 288
- volume of fundamental domain, 392, 393, 457
- von Neumann, J., 431
- Weierstrass equation, 299, 330
  - addition algorithm for generalized, 365
- Weil descent, 349
- Weil pairing, 340, 496
  - and the determinant, 341
  - applications, 356
  - double-and-add method to compute, 343
  - equals determinant, 369
  - Galois invariance, 342
  - is alternating, 341, 350, 368
  - is bilinear, 341
  - is nondegenerate, 352
  - is well-defined, 368
  - Miller algorithm, 343, 355
  - modified, 352, 356, 359
  - related to Tate pairing, 369
  - values are  $m^{\text{th}}$  roots of unity, 341
- Weil, André, 309, 496
- Western, A.E., 167
- Wiles, Andrew, 31
- Williamson, Malcolm, 61
- witness, 130
  - Miller–Rabin, 131, 136, 291
- woman-in-the-middle attack, 126
- World War I, 35
- World War II, 36, 269
- XOR, 44, 58, 59, 359, 473
- youth, lack thereof, 485
- $\mathbb{Z}$ , 10
- zero, 338
  - multiplicity, 338, 495
- zero divisor, 97, 104, 113
- zero-knowledge proof, 477, 482
  - completeness, 477
  - computational, 479
  - perfect, 479
  - rounds, 477
  - soundness, 477
  - square modulo  $N$ , 477
  - statistical, 479
- zeta function, 135
- Zimmerman telegram, 35