Title word cross-reference

(modp) [Pol78]. 1/2 + 1Poly(log N)
[ACGS84], 25·10⁹ [PSW80]. 2ⁿ + 1 [BLS75],
2ⁿ ± 1 [BS67], 2n [QG89]. $\$35.00 [Lei79].
$49.95 [Shu80]. B [CS83]. D [Kak85]. F_q
[Sx89]. \frac{1}{2} + \frac{1}{\text{poly}(\log N)} [CG85]. GF(2^n)
[BMV85]. GF(p) [COS86, PH78]. GF(p^2)
[EIG85c]. I [VGT89]. M^3 [Wil86a]. GF(2^m)
[Mas89]. GF(p^n) [MOVW89]. N
[Knu87, QG89, VGT89]. n = 2 [Lev61a],
NC⁰ [Hä87]. O(log n) [LW88]. O(log n)
[Bra87a].

- [SS89]. -Bit [QG89]. -ciphered [Knu87].
-tree [CS83].
Acquired [Sim79a, Sim84]. ‘Action [MB86]. Activities [Bur81].

Addition [Lu80]. additional [Bud29, Bud76]. additive [Bar79a]. address [Koy82a]. addresses [Cha79, Cha81].

ADFVGX [Bur85, Kon87]. Adleman [Bar87, BB79, BLO83, BLO84, SP79]. ADP [Un81].

Advanced [Fri76a, Mau14, Van69, Ano84]. Advances [CRS83, CP87, CP88, CRY81, Ger82, Gun88b, Odl87b, Pic86, Pom88, QV89, Sny80, BCI85, BC85, Bra90, Wil86b].

adventure [Yar83]. Advisor [RU88].

Aerospace [IEE88]. AFSC [HFL+85].

After [Mac87]. Against [Dav81, GMR88].

Age [SWT*81, Las85, WTE*85]. Agencies [Cha86b]. agency [Bam82, Ano78b, Bro81, Kol77]. ages [Laf64]. Agreement [DS83]. al [MTA87, Bud76]. al-‘Arab [MTA87].

al-Maskhutah [Bud76]. al-mu’amma [MTA87].

al-ta’imiyah [MTA87]. al-Maskhutah [Bud76].

al-mu’amma [MTA87].

Alan [Hod83]. Alberta [ACM89a]. algebra [EKMN84, Mor89]. Algebraic [Hi29, IM86, Lev58, Lev61a, Lev61b, BO85c, Fra89, KLL88, Lev61c, Mor89, Nie86, RN87, RN89, She86, She87]. algebraic-code [RN89]. algebraic-coded [RN87].

Algorithm [Dav85, Hen81, Kat77, Kno79, KFB79, MTMA85, Mor88, PR79, Aim83, Adl79, Ano85b, APW85, AB81, Bar87, BM84b, Cam88, CS83, ElG85c, Er89, Joh89, LtW88, Mit76, Per85, PH78, PST88, Re87, Roy86, Sha2, Sha4, CA81, CA83a, Hun85, Kno79, Mar76, Wic87].

Algorithms [DS83, Has84, HM83, Knu69, Knu73, Lak83, QG89, Riv74b, She86, She87, AIR83, AG85, Gam88, Mor89, ORS*87, PBGV89, Riv74a].

Alicos [Hei76]. Alive [Cha85a]. Allied [Beh54].

Allies [AWL*88, WTE*85, Koz84a, Koz84b, Mul89a]. Allocation [LB89a, LB89b]. Alone [RRM78].
Alphabet [Hil29]. alphabétiques [S.73]. alphabets [Fri35c, RF35]. Alsbalden [Sch20]. also [Wal00]. Alternating [CG75, Gun88a]. alternatives [Mor83]. always [BB79]. Amer [Mul89b]. America [Bam82, Yar40]. American [BBB81, Bel77, Lew82, Yar31, Yar40]. ammunition [Uni88a]. amplification [BBR88]. Amsterdam [CP87, CP88, Lit87]. Analog [sC85, Kal85, BR88, Die88, Kal84]. analogie [Zaf63]. analogy [Zaf63]. Analyse [SB82]. analyses [Dat85]. Analysis [Ano81a, Cal89, Cop89, Gyl36, Gyl38, HR82, Kal84, Mar76, MM83, RB82, Riv74b, Dem88, Fra89, FF57, Fun78, Her89, JM84, Lag84b, Ma79, Nis89, Wei82b, WW79, SWT+81]. Analytical [Lan46, Gal45a, Gal45b, Gal45c, Gal70]. Analyzing [Kem89]. ancient [Com87]. Anecdotes [SWT+81]. Angeles [IEE87a]. angels [Shu82]. Anglica [Con39]. animi [Tri06c, Tri21c]. Annex [Cop89]. Anniversary [ML87]. Annotated [Pri83, Lei79, Shu76]. Annual [ACM89a, ACM89c, IEE74, IEE79, USE99, ACM82, ACM83, ACM85, ACM86, ACM87, ACM88, IEE82a, IEE84, IEE85, IEE86b, IEE87a, IEE89]. Answering [SDV83]. any [Dro89, GMW87]. aperiendi [Tri06c, Tri21c]. APL [Fra84, Fra85b, Bro86, Van85, Wor87]. Apparatus [DHM80, Hil31]. apparently [Rou84]. appendix [Bud76]. Application [BCI85, Bis88b, Bis88c, Bis88d, BE79, CP87, CP88, CD85, Gun88b, QV89, Sch83, Yao82b, Bis88a, Fri35c, GS78, LLH89, Lak83, NS89, Pic86, Rej77, WW84]. Applications [AT&T86, AM85, CG75, GGM85, IEE88, Lev61a, RR86, SIE84, Tur41a, BFM88, Fri35a, Fri87, GOL84, Jos85, KEM88, MEI83, NY89b, NY89a, Par85, RF35, SCh84, SCh86, Wor75]. Applied [D8+83, Mor89, PM78, And79, And80]. approach [GY58, HoF55, Rou84, Sin66, Sin68a, Sin68b, Cam71]. Approaching [PP89]. approximation [Lag84a]. April [ACM83, Bet83, BC685, CP87, CP88, CM82, IEE80, IEE83, IEE87c, Pie86, QV89]. Arab [MTA87]. Arabicis [Hei76]. Arbitrary [BD74, Sha83a]. architectural [Rou84]. Architecture [Len78, PST88]. architectures [Wat89]. area [CV98, Wan86]. Arguments [SRC84]. arise [Eve85]. Arithmetic [BD74, CR85, CR88b]. Army [Ano78b]. Arnoldum [Hei76]. Array [VPS88]. Ars [Con39, Tri06c, Tri21c]. arsque [Mer44]. Art [Knu73, Col64, Jos85, Kas63]. Arte [Col64]. Articles [Bur81, Uni42, Ano76, Fri76c]. artificialia [Hei76]. Artificial [Nis89]. ASCII [Cam88]. Asimov [BCKS+83]. Aspray [SE86]. Assessment [Ano80, Her89]. Assigning [MTM85]. assisted [WW79]. Association [Jou88]. Associative [Riv74b, Lom83]. Assumption [Bla85]. astounding [Win74b]. Asymmetric [Sim79c, IM86, Sim79b, Sim82b, Sim82a]. asymptotically [Koo86]. AT&T [AT&T86]. Atkin [Mor88]. Atlantic [Roh75, Uni79b]. Atlantik [Roh75]. atque [Mer44]. attack [BLO83, BLO84, DOS6, GCC88, GC80, Hel81, Hua88, Lag84b]. Attacks [GMR88, dC86, Odl84]. attributed [FF57, Lea87]. aucta [Sch33]. auffzulosen [Sch20]. August [ACM89a, Gle87, USE88b, USE88a, WII86b, Wal00]. Austria [CSB89, Pic86]. aut [Hei76]. Authenticated [DS83]. Authentication [Boo81, BAN89b, CV89, EKW74, GJ82, GL79, IW81, IL83, Kar85, Lam81, MRW89, NIS85, Nat85b, NS78b, NS87, NS88, Lin93, Sid81, Sim85a, St.84, St.85, SNS88, Tsn89, WC81, BAN99a, Den84b, Gff81, HHL89, Kaw87, Mer82b, Mll87b, NS78a, OR87, Lin87, Lin88, Lin89, SM83, Tho74, Wan86]. Authenticator [Dav85]. author [FF57, Lea87]. Authority [MM87]. Authorization [GW76]. Automata
[Cam87]. Byzantine
[Bra87a, DS83, LSP82, Rei85].

C [AWL+88, Gyl36, Gyl38, Ste88]. C-36
[Gyl36, Gyl38]. C. [BCKS+83, SE86]. CA
[IEE87a]. Cable [IEE86a]. Caesar [LP87].
Calculating [Ano88b, AWL+88, WTE+85]. calculation
[Hun85, Wic87]. Calculator [AWL+88]. California
[ACM82, ACM86, IEE80, IEE83, IEE87c, USE99, Rud82].
called [Ste76]. Calls [Bir85]. Cambridge
[Man60]. Camera [Mea20]. campaign
[Ben80]. Can [Cha85b]. Canada
[ACM89a, IEE86b, San86]. Cancellation
[BS86, BO85d]. Capabilities [Cha86b].
capability [CF78, Gon89, Lan89, MT86].
capability-based
[CF78, Gon89, Lan89, MT86]. Capacity
[Mil87a]. Capitol [IEE82b]. Capsule
[BCKS+83, SWT+81, SBET85, SE86, WTE+85]. capita
[Hei76]. caracteres [Col64]. card [CSB89]. Cardan
[Men39]. Cardano [Shu80]. cards
[CSB89, McI85]. Carlo [FHJ+84, Pol78]. Carolina
[RR86]. Carpenter [AWL+88]. cartes
[S.73]. carvings [ML67]. Cascade [EG85b].
Cascaded [Pro85, Vog85]. Case
[Dav81, Lev61a, CS83, Sie83]. catalogue
[Sin77]. category [Uni81]. CBI [Bur81].
CCITT [Cop89, UNN85]. CD [KB89D].
CD-ROM [KB89D]. CEC [Muf88].
Cellular [Gua87, Wab87]. certa
[Tri06c, Tri21c]. Certain
[ACGS88, Bla89, CG75, Ham71, Hil31, SS84].
certifiable [Sha88]. Certified [Mer89].
Chadwick [Man60]. Chain [Blu84].
chaining [APW85]. Chaldaicis [Hei76].
Challenge [San86, Frl39a]. Chamber
[Fer87, Yar81, Yar40, Yar83]. change
[Uni83]. Channel
[Mil87a, Sim83, Sim85b, Hol87, OW84].
Channels [Mer78, Sid81]. Character
[Nea75]. characteristic [Cop84].
characteristics [DQD85]. characters
[Col64]. checkers [Sin77]. checking
[BM84b]. chemical [DG57]. chess [Sin77].
Chicago [ACM88, IEE82a, Shu80].
Chiffberyrænas [Gyl31]. chiffrée [S.73].
Chiffriersysteme [SB82].
Chiffrierverfahren [Eck82]. Chinese
[Lec89, Chu89, Yar83]. Chinesische
[Lec89]. Chip [Sed88, Riv80, She86, She87]. chips
[Riv85]. Chosen [GMRR88, DO86].
Chosen-Message [GMRR88].
chrestomathy [Pro80]. Christ [Shu82].
cialach [Kos83]. Cicco [Per90]. Cifra
[Alb70]. Cipher
[AWL+88, BP82, Bur81, Bur85, Esw15, Gaj89, Koz84b, McC75, Mea20, Por52, Pro85, QG89, Rub79, Rus27, Sar28, Ver26, WTE+85, APW85, Bar61, Bar75, Bar84, Bon47, Bow59, Bow60a, Bow60b, Cam88, Cou86, Elv87, Gar77, Hul98, Koz84a, Nea75, Rej77, Rejxx, Riv80, Gyl31]. cipher-writing [Hul98]. ciphered [Knn87].
Ciphers [BD74, EG85b, FF57, HM83, LM85, PR79, Sie85, Web79, AD81, Alb70, Bar79c, Bar79b, Bos82, CE86, D'A39, D'A71, DG57, EE56, Fri35c, Fri56, Gai39, Gai40, Gai43, Gai44, Gai56, Gef73, Hig73, Hit43, Lof64, Lew82, LP87, Nan36, Nan74, Nor73, Pra39, Shu80, Wri89]. Ciphertext [RRM78, Sie85]. Circle [BBB+81]. circuits
[Wat89]. City [ACM87]. civil [Ano80].
Clandestina [Put27]. clarissime [Hei76].
Clark [Fil78]. Class [Sie85, Ano39]. classes
[Hit43]. classic [Fri76b]. classical [Lau81].
Claud [Tri06a, Tri06b, Tri21a, Tri21b].
clear [Wal00]. Clemson [RR86]. climax
[Roh75]. clues [SD86]. CMOS [Roy86]. Co
[Had84, San86]. Code
[Den86, Fer87, Jef86, ML87, Bur79a, Bon47, Cla77a, Plh98, RN89, Ser85, Von80b, Win74b].
Code-Breaking [ML87]. Codebreaker
[Str89]. Codebreakers [AN86, Gin70, Kah67a, Kah67b, Kah74, Kah96].
Codebreaking [And86]. coded [RN87].
Codes [AN86, BK80, Bos82, Cha85b,
D′A39, D′A71, Dro89, Edw15, Fri56, Ham71, Hig73, Laf64, SBET85, Str87, Web79, Wel88b, Wel89, Wri89, Zim48, AD81, Bar79c, Bar79b, Bla89, EE56, Jac87, Kahl83, Lew82, MS81, Mor89, Nan36, Nan74, Nor73, Pra39, Shn80, Sor80, Wel82a]. Codewords [BK80]. Coding [Bla83, GB82, Ham80, Ham86, BP89, CC81, Kak85, Nie86, Riv74a]. Cogitata [Mer44]. Cognitive [AWL+88]. Coin [Blu82, Blu83a, Blu84, Sak89]. coincidence [Fri35a, Fri87]. Collected [AWL+88], collection [Fun78], collections [MS76], collective [Sak89]. College [Ano39]. Collision [PBGV89]. Collision-free [PBGV89]. Colloquium [IEE86a, Mrr87]. Colonel [Ch77a, Ch77b]. Colessus [BWV+88, Cha83a, Coo83, Flo83, Ran82a, WG82]. column [Bra89b, Bra89a]. columnar [Bar61, Cou86]. combinations [S.73]. Combinatorial [AG85]. Combining [Sie84]. Command [RW84]. Comment [Kol77]. Commentaries [AWL+88]. Comments [BWV+88, AM88, AM89]. Committee [ML87]. commonly [FF57]. communicating [Hol87]. Communication [Ano22, Bir85, CG87, Lam81, L889, Sha48a, Sha48b, Sha49, Sid81, Beh54, Cam87, CG88, He81, Koy82a, LM80, Me81, Pe80, Pie77, Sch84, Sch86]. Communications [ARS83, Mer78, Ver6, Ano84, BP82, BP85, Cal89, Cam87, CCS81, HFL+85, MP86, Sim82a, Un84, Wel82b]. compact [CS83]. COMPCON [IEE82b]. Competition [Ano82c]. Completeness [BOGW88, GJ79, GMW87]. Complexity [BS86, GMR89, G84, G88, LT85, RY86, CG88, EY85, IL89, Lie81, Me83, O87a, Per85, RY85, Sim79b, Vog85]. Compliance [Sim79a, Sim84], composed [Wal00]. composite [KP89], composition [LR86]. Comprehensive [SS89]. Compression [KBD89, Joh89, KS89]. Compromise [Mac87]. Computation [AWL+88, CG87, Pol78, Yao82a, JL75]. Computational [Sim79b, Mei83]. Computationally [AIR83, Wil82]. Computations [BOGW88, QSA88]. compute [Per85]. Computer [Ano78a, Ano82c, Boy88, BGK77, BCKS+83, Bur81, CR88a, Dav85, EKW74, Fei73, Gai80a, IEE79, IEE81, IEE82a, IEE82b, IEE84, IEE85, IEE86b, IEE87a, IEE88, IEE89, Kar85, Knu73, Kol77, Kon89, Lau81, Lit87, MZS79, Muf88, NIS85, Nat5b, PK79, Ran82a, San86, Sny80, Sto89, Sun84, Uni78a, WTE+85, WW79, Boy86, CF88, D+83, Dre79, GS78, Koc89, Las85, MM82, Nea75, Pat87, Ple75, Ple77, Rou84, Rud82, SP89, ST89, Sny79, Un81, Wil68a, Wil68b, Wil72, Wil75, BWV+88]. Computerized [Cha85b]. Computers [Che73, GJ79, Goo79, Lev61a, ML87, NS85, Ran82b, SE86, Van69, Bos82, Fey82, NS85, BWV+88]. Computing [ACM82, ACM83, ACM85, ACM86, ACM87, ACM88, ACM89a, ACM89c, BIB89, BM85, Bur81, Den79a, Ass88, Cam87, ELG85c, Hog88, O87a, Pfl89, FH87, Sch84, Sch86]. conceal [BB79], concealability [KL84]. concealed [Lea87]. concept [Des88]. concepts [Ano84]. Concerning [Hil31, Kar89b, WS79]. concinnae [Hei76]. concrete [Her89]. Conditionals [BCKS+83]. Conference [Ano78a, CJB89, CM82, Fe83, HW76, IEE81, IEE82b, IEE87b, IEE88, Ker75, MZS79, RR86, SWT+81, San86, USE88c, USE89b, USE89a, USE99, Ano87, Ano88a, EKMN84, Had84, LHH89, Mor89, Rud82, Uni78a]. conferring [Bud29, Bud76]. confidentiality [Ple77]. confidentially [Ple75]. Confinement [Lam73]. congloabatae [Hei76]. Congress [Gle87]. congruence [Plu82]. congruences [FKH+88]. congruential [Boy89a, Knu80, Knu85, Ree79, Ste87]. conjecture [BSW89, M89b]. conjurationes [Hei76]. Connection [Kol77, Win78]. Consensus [CMS89].
Consequences [IR89]. Considerations [KBD89]. Constant [BIB89, CMS89].

Constant-Time [CMS89]. Construct [GGM86, CS83, LR88b]. constructing [AB81, IM86]. contain [Lea87], contained [Wal00]. containing [Bud76, du 44].

contenant [du 44]. Continued [Por52, Sha48b]. Continuously [MM87]. contracts [EGL85]. Contribution [Gyl34]. Contributions [EKMN84].

Control [AT83, Bla83, Kar85, MTMA85, Pro85, Dat85, Dem88, O'S88, Sal73, San88]. Controlled [AWL+88, Gun88a].

Controlling [O'S88]. Conventional [Dif82a, Mer88]. conversations [Shu82].

convoy [Roh77, Roh75]. coprocessing [Van86]. core [GL89]. Corporation [WTE+85]. Correcting [SBET85, Mor89].

correction [CC81, Kak85, Rao84]. Corrections [Ano81a]. correctness [Gai77, Gai80c, O'S88]. Correlated [Blu84].

Correlation [Sie84]. Correlation-Immunity [Sie84].


Coup [Win74b]. Cours [Giv25, Giv32].

Course [Giv78, Kon89, Ano82a, Gle57, GPW85, Gle86, Kob87a, Wol43a, Wol43b, Wol43c, Wol83]. Covert [Men89, Mil87a].

crypt [SW83, RU88]. Cracking [Ree79, See89]. craft [Wol70]. creating [KS89]. crime [DB89]. criteria [BLS75].

Criticism [McC75]. Critical [Her78, Riv79, Roh77]. crittografia [Sac36, Sac47]. crossword [SD64].

crosswords [WW79]. crypt [Pro80, RW84].

cryptology [Pro80]. Cryptanalysis [And52, Ano60, Bar61, Bar75, Bar77, Bar79a, Bar84, Bee81, BO88, Cam71, CE86, Daw85, DH77, Fos82, Gai44, Gai56, Kon85, Lev61b, Mac87, MN86, Nöb84, Nöb85, Nöb88, RRM78, SS84, Wil86c, dBB88, And79, And80, Ano39, Ano76, Ano82a, Bla75, BB60, BB67, Bri86, Bri88, CR88a, Cou86, DK85, DDOP85, Elv87, Fri35a, Fri35b, Fri39b, Fri41, Fri42, Fri76c, Fri76b, Fri76d, Fri87, Gai39, Gai40, Gai43, Gai83, Gyl36, Gyl38, HS89, Hit43, Hof55, Ku35, Ku38, Ku67, Ku76, Lev61c, Mi43a, Mi43b, Mi43c, Sim04, Sin66, Sin68a, Sin68b, SS86, UG23, Uni42, UU89, Uni70, Uni24b, UU80, UU83, Uni24a, War82, Win74b, Wol43a, Wol43b, Wol43c, Wol83, de 53, vTB86, SE86].

Cryptanalyst [Uni40, Fri39a, GPW85, Gle86].

Cryptanalysts [MB86]. Cryptanalytic [Dea87, Odl84, GC80, Hel81].

Cryptanalytical [Cha86b]. cryptic [SD64, WW79]. CRYPTO [BC85, Bra90, Wil86b, CF88, O'C81, Wil85, CRS83, CRY81, Ger82, Odl87b, Pom88].

Crypto-ease [O'C81]. Crypto-Functions [Wil85]. Cryptogram [Ano60].

Cryptograms [MM83, Nan36, Nan74].

cryptograph [Bar77, Gyl36, Gyl38].

Cryptographer [Sca86, Wol70].

Cryptographia [Con39, Put27, Col64].

Cryptographic [ARS83, Ano87, Agn88, AT83, BIB89, BC85, Bry67, CP87, CP88, DLM82, DHM80, Dif82b, EMMT78, Gif81, GJ82, GGM85, Gun88b, Gyl34, Ham71, Hen81, KV89, KMM+80, Lea87, LT85, MTMA85, MM78, VQ89, Ritxx, San88, Ser85, Sha38a, Sie84, Smi83, Uni88a, Van69, BOCS83, Bla79, CF88, D+83, FF57, FM76, GY58, HS85, HFL+85, Her81, IN89, Lau81, Lev83, LR86, Mas83, NY89b, NY89a, Odl85, Par85, Pic86, PH78, Sed88, Uni82a, Uni82b].

Cryptographically [BM82, BM84a, KM88, Sha83b, Ste87].

Cryptographie [vN83, S.73, Val92, Bau39, Bau46, Giv25, Giv32, Joss85, LS25, Sac51, dIS02, du 44].

Cryptography [Ame81, Ano76, BBB+81, BP89, BB85, Bet83, BGK77, BE79, Bur84a, Bur84b,
CG75, Cop87, CM79, Dav81, DB81, Den82, DH76, Dif88, ECW75, Fei73, Fri76c, Gro82, Gud80, Hei79, Hil29, Hil31, Hul98, Kon81, LM22, Lan81, Len78, Lev58, Lev61a, Lev61b, Man14, MM82, Mor66, SP89, Sha87, Sha45, SE86, Smi43, Smi44, Smi55, Smi71, Smi83, Tur41a, dRHG

Cryptography
[Wal00, Wel88b, Wel89, Wie87, dlS02, BCKS + 83, Col64, du 44, Kon89, Lei79, ST89].

Cryptologic
[Ale45, Jou88, Sny79, Sny80].

Cryptologist
[Cla77b, FFW55].

Cryptology
[AM85, BC85, Boy86, Bra98b, Bra98a, Cal92, CRS83, CP87, Com87, DKKMM87, DK + 89, Fer87, Kah66, Kah79, Kah84, Kon89, Las85, Lem79, LP87, Mar70a, Mar70b, Mei83, Nai89, QV89, Rug65, She66, She87, Uni79a, Wor75, Bec88, BC185, Boy88, Bra87b, Bra88, Bra90, CP88, Che73, CRY81, D + 83, Fra89, Fri56, Fri63, Gal45a, Gal45b, Gal45c, Gal70, Gun88b, Jun88, Kah63, Kah83, Oak78, Odl87b, Pat87, Pic86, Pom88, Sie83, Sim88, Sin77, Wil86b, van88, Ano82c, Lan46].

cryptology
[Bec97].

cryptomenytics
[W]al00].

cryptoprocessor
[MS83].

Cryptoprotocols
[Yun85a, Per85].

Cryptosystem
[CR85, EIG85b, Jun87, WM85, AM88, AM89, ABS81, CR88b, DO86, Eck83, EGS85a, EIG85a, GC80, GM85, Gun87, Hei81, Hoo82, HM85, Kar89a, Kar89b, Koy82a, Koy82b, Koy83, KM88, Lag84b, LLH89, LB88, LM80, Mei81, Nö88, Odl84, Sal85, SY86a, SY86b, SM83, Sha82, Sha84, SS86, SP79, SW83, SSA87, TC85, TC86, TIF + 88, VGT88, Web88, WS79, Yun85b].

Cryptosystems
[Bla85, BR88, Den84a, GS84, Kob87b, Oka88, RSA78, RSA83, Sha85, SSA88, Ad83, ABS1, BB79, BLO80, BS83, BLO84, Bri86, Bri88, CL88, Dif82a, Eck82, GS88, HL88, Her78, IM86, JM84, Lag84a, Lak83, LM84, Lid85, Lu79, Lu80, LP87, Mer80, Mer82a, MRS78, MRS88, MN81, Nie86, Nie88, Pop89, RN87, Riv79, RSA82, She86, She87, Sim82a, SX89, Vou80a, Wu82].

Cuckoo
[Sto89].

curiosa
[Shu82].

Current
[Muf88].

Curve
[Kob87b, CL88].

Curves
[Mi168, Len87, SX89].

Cycurzon
[Jef86].

custom
[She86, She87].

Cyber
[LTW88].

cycle
[Mas83].

Cypher
[Bro86, Den86, Fer87, Jef86, RRM78, Wor87, Fra84, Fra85b, Vam85].

D
[Bv82, Hit43, Cop89].

D.
[WTE + 85].

DOL
[SSA87].

DOL-TOL
[SSA87].

Dabbling
[Ritxx].

Dalgarno
[Shu82].

Dallas
[USE88c].

damage
[Kar87].

dannata
[Hei76].

dan
[Saw55].

dans
[Zaf63].

Dante
[Are21].

Data
[Ano78a, Ano81b, Ano85b, Bis88b, Bis88d, CA81, CA83b, Cia86, DM83, Den79b, DH77, Gai77, Gai80c, Gul83, Int79, Int81b, Int84, Int87, Int88, IWI89, Jon86, KBN88, Kat77, Ker75, Mar76, Nat77, NIS85, Nat85b, Pri80, SB82, Sim79a, Sim84, Tho86, Uni78a, Uni81, YY89, Ame83, ALN87, Ano80, Ber80, Cam88, Dat85, Den82, Dro89, Fun78, Gef73, Gru84, Hol87, Joh89, Kak83, MM82, Mit76, Mul81, Nat84, Nai89, NS89, O’CS81, Pea80, Pri83, Sha88, Sor80, Tex84, Uni87, UNN83, Uni84, Vam86, We10, Zei79, Ano78a, Bec82, Bis88a, Bis88c, CA83a, EMMT89, Fra85a, Gai80a, Gai80b, Jue81, Ma79, Nat84, Sup88, Uni78a, Uni78b, Uni87, Uni82c, UNN83, UNN85, Uni84, Uni77, Uni83, Uni88b].

data-flow
[Sha88].

Database
[DWK81, GW76, Ano84].

Datagram
[Tsu89].

David
[Gin70, Lei79].

Davison
[DG57].

Davos
[Gin88b].

dawn
[BB89].
Environments [LS89, Hog88, Kaw87].

Epiphanes [Bud29, Bud76]. Equality [WC81].

Equations [OSS85, Has88, TIF+88]. equidistribution [Koo86].

equipment [HFL+85, Int81b, Int84, Ser85, Uni82a, Uni82b, Uni88a, Uni82c, UNN85].

equivocation [vTB86]. era [BB89, Men89].

Errata [Ano88b]. Erratum [Ayo68b].

Error [Bla83, CC81, Pro85, SBET85, Kak85, Mor89, Rao84, vTB86]. Error-Correcting [SBET85, Mor89]. Error-correction [CC81, Kak85].

ErycI [Put27]. escrituras [Col64].

Escrow [O’N86]. Espionage [Sto89, TP63, Yar83].

essential [IL89]. est [Tri06c, Tri21c].

Established [Ano82c].

estimation [And79, And80].

Examined [FF57].

Excerpts [SWT+81].

Exchange [Blu83b, Ted85, Yao86, AS83, Rab81].

Execution [FH74], exercise [Bec82, Cal89].

Exhaustive [DH77, Jue81].

Exhibit [Bur81].

Even [Mea20].

Event [BBF83].

Evidence [FF57], evolving [DB89].

Examine [FF57].

Excerpts [SWT+81].

Exhibit [Bur81], existence [Lut97, Lu80].

Expected [Bra87a].

Experimental [BB89].

Experiments [HM83].

Explicatur [Hei76], exploiting [She86, She87].

Exponentiation [Kak83].

Expose [RS84].

Extended [BS86, BO85d, GGM85, VV85, CG85, Kon85, Lag84a, MRS87, Ted85, Yun85a].

Extensible [Cha85a].

Extrapolation [LR88a].

F [Bv82, Cla77a, Cla77b].

F. [SBET85].

F.E.A.L [dB88]. fabrication [S.73].

facsimile [UNN85].

factor [Guy76, You80a, You80b]. factorized [Bac88].

Factoring [CD85, Len87, Odl87a, PST88, LtW88].

Factorization [DH85b, Wil85, KLL88, Pol87].

Factorizations [BS67, DH85a].

Factors [RM85, CE86].

Far [Ted85].

Faraday [IEE82b, WTE+85].

family [TeX84].

Fat [Bv82, Cla77a, Cla77b].

fattened [Bac88].

Factoring [CD85, Len87, Odl87a, PST88, LtW88].

Factorizations [BS67, DH85a].

Factors [RM85, CE86].

Failure [CMS89].

Fault [Ted85].

Fault-Tolerant [BI89, BO88b].

February [Ano78a, BBB+81, IEE86a, Mur87, Rud82, Uni78a].

feedback [Nie88].

Fellowship [Bur81].

field [Den84b].

Fields [CR85, CR88b, Cop84, Lid85, Mas89, Mul81, Odl85].

fifteen [Dif82b].

fifteenth [ACM83].

Fifth [HW76, SE86]. File

[Blu84]. Files

First [ACM89c, Dif88, Fia83, Sed88, USE88b, Ash87, Ee56, Had84, Lew78, Win74b, Wol43a, Wol43b, Wol43c, Wol83]. fixed

[SP79, Uni82a, Uni82b].

FL [IEE88].

Flaw [Dem88].

Flip [Rub79]. Flip-Flops [Rub79].

Flipping [Blu84, Blu83a, Sak89].

Flops [Rub84].

Florence [CM82].

Florida [IEE84].

Florida [IEE84]. flow [BR88, Sha88].

Flowers [WG82].

forecast [Dif82b].

Forlag [Bro86].

form [Wal00].

formal [KY82, Kemi89].

formulae [KV89].

Forum [MC75].

Foundations [IEE79, IE82a, IEE84, IEE85, IEE86b, IEE87a, IE89, Eck82].

Founding [Kil88].
four [Bow59], fourteenth [ACM82].
Fourth [IEE88, Rud82], Fraction [Por52].
fractionating [Fri41]. Fragmentation [Tsu89].
framework [Per85]. Framingham [Kar75].
France [BCI85], Francis [Lea87],
Francisco [ACM82, Rud82], Franksen
[BCKS+ 83, Bro86, SBET85, Van85],
franz¨osischen [Kas63].
free [PBGV89].
freedom [Sie83], French
[Bau39, Bau46, Kas63, vN83, LS25, Per90, Sac51, Zaf63, diS02, du 44].
Friedman [Cla77a, Cla77b].
F¨uhrungsprobleme [Roh75].
Function [IW81, Mer88, Win83, Win84].
Functional [SS89].
Functions [ACGS88, GGM85, GGM86, MRW89, QG89, Sie84, WC81, Wil85, Yao82b, BMS9, GL89, IL89, Lev85, LR88b, NY89b, NY89a].
Funds [BW85, Ano85b, Kem83].
Further [RF35].
Futrelle [BCKS+ 83].
Futurelle [BCKS+83]. future
[CSB89, Eck85].
G. [WG82].
G. [BCKS+83]. Gaithersburg
[Ano78a, Uni78a], Galland [Lan46], Gallica
[Con39]. Galois [Mul81]. Game
[GMW87, Yun85a, See89]. Games [Gar77].
Gardner [AWL+88], Garland [Lei79].
Gateways [Tsu89].
geaze [San89]. Geheimer
[Sch20, Sch33]. geheimes [Sch20].
Geheimnissen [Kas63].
Geleitzugschlachten [Roh75].
General
[GTM45, Sid81, EKMN84, ISN87, NBWH78].
generalis [Tri06a, Tri21a]. Generalized
[Kot85, Adl83, GCC88].
Generals
[Bra87a, LSP82, Rei85, Win74b]. Generate
[BM82, BM84a, Yao86, Bae88]. generated
[Bar84, Plu82]. generating [Er89].
Generation
[MM78, Sha93b, SE86, VV85, RT88, SD86, Vin71, Vin72].
Generator
[AM85, BE79, FMC85, Boy89a, KM88, Mit76, Par85].
Generators
[Boy89b, CG75, Gun88a, Plu83a, Plu83b, Gab82, Lev85, LR86, Ste87].
genere
[Con39]. geometry [Mil85]. George
[Ric74, Shu82].
German [AWL+88, Elv87, Lec89, WTE+85, Ale85, Cha86b, Eck82, Gab82, Gaj89, Kas63, Koz84a, Koz84b, Rejxx, Roh75, Uni79b, Win74b].
Germanica [Con39]. Germany [Bau83],
gewiser [Sch20]. Girls [CN87], Girolamo
[Shu82].
Global [IEE87b, San86].
GLOBECOM [IEE87b], glossary [SW61].
GMD [Bur81]. Godfather [Ran82a]. goes
[Kah79, Lew78].
gold [San89].
Goldstine
[Ano81a, SWT+81].
Goldwasser
[SFT85, Vam85, dS02].
Goldwasser-Killian-Atkin
[Mor88], good
[AD81, Dro89, Lu79, Lu80, Verb80b].
Gordon [DG57]. Government
[Den86, Fer87, Jef86]. Governmental
[Dav81]. Graeca
[Con39]. Graecis [Hei76],
grande [Ber73]. graph [NM88].
greater
[Lu79, Lu80].
greatest
[Ber83, Cla77b, Lew78].
Greek
[Bud29, Bud76]. Group
[Bla85, sC85, Bv82, DS81, DMS81, Des88, NBWH78, UNN85, Ano81, BBB+81, DB81].
group-oriented [Des88].
Group-Theoretic [Bla85]. Groups
[CG75, DG57, Mas83, SBET85].
Grubb
[SAR28]. Grundlagen [Eck82].
guerre
[Ber73]. guess [VTG89]. GUEST [HR82].
Guidance
[Mur87]. Guide
[GJ79, CF88, MP86, MM82, Tex84, Uni82b, Uni79b].
Guidelines [Ano81b, Ano81].
Gustavus
[Wa100].
H.
[Ano81a, BCKS+83, SWT+81, SBET85, WG82].
H.
[BCKS+83, SWT+81]. habitat
[Hei76].
Hackers
[WTE+85]. Hagelin
[Bar77, RRM78]. Hall
[ST89]. handbook
[CF88]. Happenings
[ML87].
Harbor
[Far67, Far69].
Hard
[ACGS88, GeF73, GL89, Wil82].
hard-core
[GL89].
harder
[AB81]. Hardware
[Cia86, DDG+85, Gai97, Gai96e, Gru84, HGD85].
Harmonia
[Mer44]. Hartree
[Ano81b, WTE+85, AWL+88]. Harvard
[AWL+88]. Hash
[MRW89, QG89, WC81,
Insecure
[Den79a, Lam81, Mer78, NS88, Kaw87].
Installation [Cha83a, MM78], installing [MP86], Institute [IEE82b], institution [AA88], Instrumenta [Sch20].
Instruments [Ano88b, AWL+88, WTE+85].
Insure [Sim79a, Sim84], integer [DH85a, FHK+88], integers [Len87, Odl87a, PST88].
Integrating [Sat89], intellecta [Hei76].
Intelligence [And86, Jon78a, SBET85, Uni78b, Uni79b, Beh54, Cal89, HT79, HH79, Jon78b, Men89, Nis89].
Interactive [Bec88, Bec97, Bra87b, HW75, Smi83, Bos82, HW79, Nan36, Nan74, SP89, ST89, Sta70, Sta78, War82, van88].
Introductory [Ano39, Coh87], invented [Pli98].
Inversen [Gab82].
Investigation [Gam88].
investigations [Fra85a], involvement [Uni78b].
investigation [Nis89].
interpretation [Nis89].
Interactability [BOGKW88, GJ79].
Intractable [Wil85].
Intrepid [Ste76].
Introduction [Bec88, Bec97, Bra87b, HW75, SMI83, Bos82, HW79, Nan36, Nan74, SP89, ST89, Sta70, Sta78, War82, van88].
Introductory [Ano39, Coh87].
Inversen [Pli98].
Investigation [Gam88].
investigations [Fra85a], involvement [Uni78b].
Inviolable [Un78b].
Invariants [Tri06b, Tri21b].
Invariants [Tri06a, Tri21a].
IPS [KMM+80].
irrelevant [MS76].
ISBN [Bro86, ST89].
ISDN [PP89].
Island [ACM85, IEE84].
ISO [Cop89], ISO/CCITT [Cop89], issue [Gal88].
Issue [Lit87, Cho86, Fra89, Mas83].
Istikhraj [MTA87].
Italian [Alb70, Sac36, Sac47].
I talica [Con39].
Italy [AG85, CM82, Mor89].
Item [Sch20].
Iterated [Bri85, BLO83, BLO84, Kar89b, SY86a, SY86b].
IV [BCKS+83, Fri141].
J [BCKS+83, Mul89b, WTE+85, Rub79].
Jack [Rud82].
Jacob [Hei76].
January [FM76].
Japan [IEE87b, Lew82].
Japanese [Cla77a, Str87], jargon [MS76].
Jennifer [ST89].
Johannes [Shu82, Wal00].
Johannis [Hei76].
John [MS76, Man60, Shu82].
Joint [Rao84].
Josef [ST89].
Journal [Jou88], Jr [Mul89b].
Juan [IEE79].
juillet [Per90].
July [Hel81, Mei81, Mor89, Per90].
June [AG85, EKMN84, MZS79, USE89b, USE99].
juxta [Hei76].
Kahn [Gin70, Kah83].
Keel [Mea20].
Keep [Cha85a].
Keeping [Mea20, GM82].
Kendall [DG57].
Kent [Sar28].
Kerberos [SNS88].
Kernel
[LB89a, LB89b, Sch75, Sil83].
Key
[AS83, BFB83, BW85, BG85, Boo81, Bur84a, Bur84b, Cha86a, Cha85a, CR85, Den84a, DiF88, EMM78, ElG85b, GS84, Hei79, LS89, Oka88, RSA78, RSA83, SBC85, Smi83, TT84a, TT84b, WM85, Wil85, Yum85a, AM88, AM89, ADL83, Bar87, BB79, BM84b, BS83, CM85, Cho86, CR88b, DDOP85, DiF82a, EG85a, ElG85a, ECW75, Fra89, GC80, GM85, G888, Gua87, Gy138, HHL89, HL88, Her78, Hoo82, Hun85, HW88, Kak84, Kar89b, KYM82, KL84, Koy82a, Koy82b, Koy83, Kue87, Lag84a, LLH89, Luk83, LB88, Lom83, Lu79, Lu80, LP77, Mer80, Mer82a, Mer82b, Mic88, Mil85, MN81, NU88, N888, ORS+87, RN87, RN89, Riv79, RASA82, Roy86, Sal85, SY86a, SY86b, SM83, Ses81, SS86, SSA87, TC85, TC86, TIF+88, Web88, Wic87, WS79, Wil80, Wil86a, vTB86].
Key-Lock-Pair [Cha86a].
keyed
[Ay068b, Ay068a, Ayo81].
keyless
[AS83, Yun85b].
Keys [Buu83b, MTMA85, MM78, Ber09, Bla79, Bv82, CS83, DS81, DMS81, HM88, NM88, Sea86].
Killian [Mor88].
kind [Gar77].
kinds [SX89].
Kingdom [ST89].
Knapsack
[CR85, Hen81, Lag84a, Nie86, Ses81, Sha83a,
Adl83, BLO83, BS83, BLO84, Bri86, Bri88, Cho86, CR88b, GM85, HL88, Lag84b, Odl84, Pop89, SM83, Knapsack-type [Nie86, CR88b]. Knowledge [Bri85, MH78, Wil83a]. Knowledge-analysis [GMR89, Has84, BFM88, Nis89].

knowledge-analysis [Nie86, known] [Rou84]. Koblitz [Kon89]. kodowania [Kos83]. korekcyjnego [Kos83]. Kozaczuk [WTE85, AWL88]. Kruh [SE86].

Kryptographie [Kos83]. Kryptographie [Lec89].

Kunsten [Sch20].

L [Mul89b, SWT81, SE86]. Laboratories [DH85b]. Laboratory [AWL88]. Labs [WTE85]. land [Gyl83]. Lands [Gyl83]. language [MS76, Shu82, Wri89]. languages [Kas63, MS76, SSA88, SWT81]. Large [AWL88, Ker75, NS78b, Sat89, Hoo80, NS78a, PST88]. Large-Scale [AWL88].

Lasers [Sch83]. late [MS76]. Latin [MS76].


Letter [MB86, Mul89b]. Level [VK83].


Limiting [Kar87]. Limits [IR89]. linéaire [Zaf63]. Linear [Hi831, Kot85, Man60, RM85, Boy89a, CE86, FHK88, Knu80, Knu85, NU88, Plu82, Ste87, Vog85, Zaf63].


Logarithms [BMV85, EIG85b, Mas83, Cop84, COS86, EIG85a, EIG85c, Odl85, Odl87a, PH78]. Logic [BAN89b, CM82, HR82, BAN89a, Kar89a, Lei80].

London [Mur87]. Long [BE79].

Long-Period [BE79]. looks [FFW55].

Lord [Je86]. Low [LO85, Boy89a, Has88]. Low-Density [LO85]. low-order [Boy89a].

LPC [SJ76]. LSI [FMP85, FMC85]. Lu [GC80]. Lu-Lee [GC80]. Lukoff [BCKS83]. Luneburg [Wal00].


Machine [AWL88, DK85, Gaj89, Koz84b, RRM78, SE86, WTE85, AG84, Elv87, Koz84a, Rejxx, BCKS83, Fut73].

machinery [Dem88, AWL88]. Machines [An88b, AWL88, Bur81, Pl89, WTE85, DK89, AWL88, WTE85]. magic [Lew82, Wal00, Mul89a, Far67, Fur69].

magica [Hei76]. magische [Sch20, Sch33].

Mail [Lin93, Cha79, Cha81, Mit89, Lin87, Lin88, Lin89, Tho74]. Mainframe [Dav85].

Maintenance [Cha83a, Gal80b, Gal80a]. Majority [GMW87, RBO89]. make [Cha85c]. Making [Coo83]. Malaysia [HS89]. Malcotti [Gua04].

Man [Fil78, Cla77a, Cla77b, Ste76].

Management [BW85, EMMT78, LS89, KYM82].

Managing [TS88]. mancherley [Sch20]. manier [du 44]. Manipulations [SJ76].

Manitoba [HW76]. manner [du 44].

Manual [AWL88, Con86, Hit43, Sac77,
Uni40, Uni82a, Wil86c, Sac36, Sac47, Sac51].
Manuale [Sac36, Sac47]. Manuel [Sac51].
manuscripts [MS76]. mapping [Gab82].
Maratea [AG85]. March
[Bet83, Roh75, Roh77]. Markers [BBF83].
mapping [Int87, Int88]. Markov [Bhu84].
Mary [Ano39]. Maryland
[Ano78a, Uni78a, USE89b]. Marz [Roh75].
Marzolla [Nis89]. Masani [AWL+88].
Markov [Blu84]. markets [Int87, Int88]. Markov
[Al84].
match [Riv74a]. matched [Sor80].
Matching [MM87, AG84]. Math
[BBF83]. Mathematica [Mer44]. Mathematical
[Ano88b, AWL+88, BD74, Cam71, Fra85a, Gar77, Kon89, Mar70b, Pat87, Por52, Sha45, Sha48a, Sha48b, WTE+85, Eck82, Hof55, Sin66, Sin68a, Sin68b, Wor75].
Mathematicians [Ano81a, Gle87, Rej81, Pat87, Kon89].
Mathematics [HW76, Hel79, RR86].
mathematischen [Eck82]. Matrices
[PM78]. Matrix [Lev58, Bou85, Vou80b].
Matsumoto [DDOP85]. Matter [Ano85a].
Matyas [BCKS+83]. Maverick [AWL+88].
Maximum [And79, And80]. May
[ACM82, ACM85, ACM86, ACM87, ACM88, ACM89c, Fea83, Gun88b, RR86, Un179b].
Maze [Sto89]. McEliece
[AM88, AM98, LB88]. McLean [AWL+88].
MD [USE89a]. measure [Hoo80].
Measures [GS84, GS88]. MEASAS [KS89].
Mechanica [Mer44]. Mechanism
[Cha86a, GW76]. Mechanisms
[Mul88, VK83, VK84, CV89, O’S88].
medieval [ML67]. Mediterranean [Ben89].
Meetings [WG82]. members [Ano39].
Memorandum [Je86]. Memories
[WTE+85]. Memory [LB89a, LB89b].
mensuris [Mer44]. Mental
[GMW87, Yun85a, GM82]. Mercury
[Wil41]. Merkle [Lag84b, Sha82, Sha84].
Mersenne [Mul89b, BSW89]. Message
[Dav85, GMR88, LHM84, MRW89, Lin87, Lin88, Lin93, Lu79, Lu80, MI88, Lin89].
Messages
[Rus27, AA88, BB79, KL84, SP79].
Messenger [Wil41]. metamodel [Nis89].
metatheory [Nis89]. Meteor [Cam87].
Method [ARS83, Bla75, DHM80, Mor66, O’N86, Rejxx, RSA78, RSA83, Bar79a, CM85, Kak84, Lon83, NM88, RSA82].
Methods
[Cam88, Ga89, Pol78, DK+89, Dem88, IM86, Kuk35, Kul38, Kul67, Kul76, de 53].
Meyer [BCKS+83]. Microcomputer
[Sto89, Tex84]. Microcomputers
[SM83, Ano89, Fos82]. Microelectronics
[AWL+88]. microprocessor [CV89, MS83].
microprocessor-based [CV89, MS83].
Midway [Mac87]. Migration [GL79].
Militaire [Ros85]. Military
[Cha86b, Fri35b, Fri39b, Fri41, Fri42, LHM84, Sin77, Fri76a, Fri76e, Hit43, Men89, vN83].
Millikan [Hit43]. Million [Ran55, Ran01].
millions [Gar77]. Mind [AWL+88].
Minister [MB86]. Minneapolis [IEE81].
Minnesota [IEE81]. Mirror [Cla12].
missing [Boy89a]. Model [LHM84, Gyl36].
Models [CMS89, D+83]. Modern
[Bra88, Kah66, SE86, Bla75, Bra87b, Com87, DK85, Lec89]. moderner [Lec89]. Modes
[CA83a, Nat80, Ame83]. modification
[Wil80]. Modular [MB85, Hå88].
modules [She86, She87]. modulo
[Kak83, Per85, VGT89]. modulus [PP89].
monoalphabetic [Fri35b]. monograph
[Lea87]. Monte [FHJ+84, Pol78].
Monterey [USE99]. Monthly [Mul89b].
morphisms [Kar89b, SY86a, SY86b]. MOS
[Un82a, Un82b]. Most
[Jon78b, Bam82, Wal00, Win74b]. movable
[Gyl38]. MPJ [Joh89]. MPQS [LtW88].
MPQS-factoring [LtW88]. MR [Bv82, Lu80, Mul89b, Riv79, BCKS+83, SBE85].
Mr.
[Fra84, Fra85b, Fra86, Bro86, Vam85, Wor87].
mu’amma [MTA87]. Multi 
[BOGKW88, Mit89, Yun85a, Koy82a].
multi-address [Koy82a].
Multi-destination [Mit89]. Multi-Player
[Yun85a]. Multi-Prover [BOGKW88].
Multics [Sal73, Sch75]. multilevel [FLR77].
Multiparty [CCD88, ROB89]. Multiple
[MH81, Sl87, Gy83, He81, LM80, Me81].
Multiplication
[Me85, Mon85, Mas89, PP89].
Multiplication-permutation [Me85].
multiplicative [Odl84, Ree79].
Multipliers [VPS88].
multiply [BLO83, BLO84].
Multisignature [Oka88].
mummy [Pro80].
Museum [Bud29, Bud76, Bur81, WTE + 85].
must [Dro89].
multiple [OR87].
Mycenaean [Zaf63].
mysteries [Sea86].

N [SWT + 81]. nahe [Sch20]. name
[BO5a, BO5b, Lea87]. name-stamp
[BO5a, BO5b].
National
[Ano78a, DHI85b, MZS79, U78a, Sie83, 
Van87, BGK77, Bro81, K77, Mar76].
nature [M576]. naturliche [Sch20, Sch33].
Naval [Ale45]. navigandi [Mer44].
Navigation [Mur87]. Navy [Mac87]. Nazi
[Win78]. NBS
[Ano81b, DH77, Gai77, Gai80c, Gui83, Uni81].
NC [IEE89]. Neat [Kon89]. NEC [LTW88].
necromantica [Hei76]. negeri [Saw55].
nemine [Hei76]. Nero [Sto65].
Netherlands [CP87, CP88]. Network
[Den79a, KB88, NS88, SNS88, VK83, 
Dat85, KD78, Tho74]. Networks
[IEE81, Kar85, Mu88, NS78b, PW6, PW87, 
PK79, CV89, KD79, Mi85, NS78a, 
NBWH78, W86, We82b]. Nevada
[ACM89b]. Newbold [Sar28]. News
[Ano82c, Bur81, K77]. nihil [Hei76]. nine
[Wal00]. nineteenth [ACM87]. No [Cha86b, 
Bv82, Ker89, Lu80, Mu89b, RM85, Tuc79].
nominibus [Hei76]. Non
[BIB89, BFM88, Chu89, Dav81, Fel87, Bar75].

Non-Cryptographic [BIB89].
Non-Governmental [Dav81].
Non-homomorphic [Chu89].
Non-Interactive [Fed87, BFM88].
non-pattern [Bar75]. Noncryptographic
[BOGKW88, Sak89]. Nonlinear
[Sie84, TIF 88, Web88]. nonrandomness
[KL88]. Nonsingular [PM78]. Norbert
[AWL + 88]. Normal
[Ran55, Ran01, MOV89]. Normandy
[Ben80]. Norris [AWL + 88]. Norse [ML67].
North [Had84]. North-Holland [Had84].
Notation [BCKS + 83]. Note
[BD74, Lam81, Lam73, We88a, Wic83, BV82, 
CM85, Lei80, Me81]. Notes [BD74, Por52].
notice [Uni83]. Notices [Ano82c, Bur81].
notion [MRS87, MR88]. Nov [IEE87b].

nov [Hei76, Sch20]. Novel [Sto65].
November [ACM89b, EIE82a, EIE89]. NP
[GJ79, VV86]. NP-Completeness [GJ79].
NSA [Uni78b]. Number
[BIB89, Boy89b, BE79, FMC85, Kon89, 
Ph83a, Ph83b, Sch84, Sch86, VV85, CE86, 
Guy76, Jac87, Kob77a, KM88, Mit76, Per85, 
RT88, Sta70, Sta78]. Numbers [HW75, 
Bac88, HW79, KLL88, Tip27, Vin71, Vin72].
Numerical [Ano81a, HW76, SWT + 81].
nunnis [Mer44]. nunc [Hei76].

O [Bro86]. O. [BCKS + 83, SBET85].
Oakland [IEE80, EIE83, EIE87c]. Object
[GL79]. Objects [Bla85]. oblivious
[Kil88, Rab81]. obscure [Col64]. obscure
[Col64]. Observability [PW6, PW87].
observation [LB88]. Observations
[Kar89b]. obsolete [Cha85c]. Obtaining
RSA78, RSA83, RSA82. occultam
[Tri06c, Tri21c]. occulte [Con39]. Oct
[IEE79]. October
[CSB89, HW76, IEE74, EIE81, EIE84, 
IE85, EIE86b, EIE87a, EIE89, MB86]. off
[Ste88]. Office [IL83]. official [Lew78].
Ogham [MS76]. Oh [Wei88]. Okamoto
[VGT88]. Ole [Van85]. ology [Pro80].
Omura [WW84]. One
[BBB+81, Has87, IR89, IL89, IW81, Kno79, KFB79, Lev85, Sed88, Win83, Win84, AIR83, Arc22, GL89, NY89b, NY89a, Sha88, Wa00].
One-Chip [Sed88], one-time [AIR83].
One-Way [IR89, IW81, Kno79, KFB79, Win83, Win84, Has87, IL89, Lev85, GL89, NY89b, NY89a, Sha88]. Only [Sie85].
Ontario [San86]. Open [CG87, SNS88].
OpenBSD [dHRG+99]. Operating
[HRU76, Hoo80, MT86, SII83]. Operation
[AWL+88, CA83a, Nat80, Ame83, Far67, Far69]. operations
[Cal89, Gyl13, HT79, HH79, Uni81].
Optimal [MTMA85, MOVW89].
Optimization [LtW88]. Options [PW86]. order [Boy89a]. ordered [CS83]. Orderly
[PM78]. orders [Koo86]. Organizational
[AWL+88]. Organizations
[Sny80, Sny79]. organized [DB89]. oriented [Des88].
Origin [BCKS+83, Ano78b, Bro81, MS76].
Origins [Ran82b, Kah84]. Orlando [IEE88].
Orleans [IEE74]. ornithological [Daw85].
Osborne [WTE+85]. Other
[AWL+88, Den84a, AB81, FF57]. output
[DQD85]. overflow [NBWH78]. Overview
[Den79b, Mat79, Sum84, dHRG+99].

P [Mul89b], package
[Bis86e, Bis89b, Gru84]. Packings
[SBET85]. pad [AIR83]. pages
[Fil78, Wor87]. Pair [Chase86a]. palace
[Bam82]. Paper
[Ano82c, Fri35a, Fri35c, Klu35, RF35].
paperback [ST89]. Papers
[Ran82b, CM82, Rdu82, AWL+88]. papers/
Compon [Rud82]. Paradoxical [GMR85].
paradoxos [Hei76]. Parallel
[QSA88, VPS88, PP89, RT88, Sal85].
Parameters [SJ76]. Paris [BC185]. Park
[IEE89, MB86]. Part
[Are22, Bur84a, Bur84b, Fri35b, Fri41, Lin87, Lin88, Lin89, Lin93, Vol41, She86, She87].
Partial
[BG85, Cha85a, GM82, PP89, Riv74a]. partial-match [Riv74a]. Partitioned
[GY87]. partitioning [GY87]. partly
[MS76]. Parts [ACG88]. party [BO85c].
Pascal [APW85]. Pass [Has84].
Pass-Algorithms [Has84], passa [Hei76].
passin [Hei76]. Password [HHL89, Lam81, Nat85a, RU88, See89, BCW86, GAf87, Sin85].
past [Riv85]. past/present/future [Riv85].
patents [Lev83]. Pattern [AG84, Bar75].
Patterson [Kon89]. payments [Cha83b].
PC [Bec97, Dea87]. Peapolitani [Hei76].
Pearl [Far67, Far69]. Pegawai [Saw55]. 38
Ber80]. Coding [Sim85a]. Compon
[Rud82]. future [Riv85]. IEICE [IEE87b].
London [Lei79]. present [Riv85]. Rabin
[ACG84, CG85]. ri [Ano87, Ano88a].
SC122 [Roh77]. Sec’83 [Had84]. Sec’84
[San86]. TH4 [Uni88a]. Pennings
[AWL+88]. Performance
[Lag84b, Beh54, Lom83]. Period
[BE79, Bar79b]. Permutation
[AM85, LM84, KD78, KD79, LR86, Mei85].
Permutations [IR89, Ay68b, Ay68a, Ay81, Has87, LR88b, Rej77]. pernicioso
[Hei76]. Personal
[Den79a, Ste89, Boy86, Win69]. Peters
[BCKS+83]. PGP [Saw55]. phaenomena
[Mer44]. Philippum [Tri06b, Tri21b].
Physica [Mer44]. Physica-Mathematica
[Mer44]. physical [Nat84, UNN83, Uni84].
Physics [Ano88b, AWL+88, WTE+85, Fey82, Sch84, Sch86]. picture [SSA88].
Pieprzyk [ST89]. Pioneer [Ano82c].
Pioneered [Sny80]. Pioneers [Wei88].
pipeline [PST88]. placing [She86, She87].
Plaintext [Kah63]. plane [Mil85]. Play
[GMW87, GM82]. Player [Yun85a].
Playfair [Bow59]. plays [FF57, Lea87].
Pless [Hua88]. plus [Ber73, War82]. PN
[Vou80b]. pneumatica [Mer44]. Poe
[Sau89]. poems [Lea87]. Point
[Sin77, Gyl38]. Poker
[FM85, Yun85a, GM82]. policies [JL75].
D+83, Eve85, Kem89, RBO89. **Prototype** [SBC85, BB89]. **Provable** [IR89]. provably [IN89, Sha86]. prove [FS87]. proven [Lea87]. **Prover** [BOGKW88]. provided [Gyl83]. **Providence** [ACM85], provides [Uni87]. **Proving** [FLR77]. **Pseudo** [AM85, BM82, BM84a, Boy89b, FHJ+84, Gab82, LR86, Plu83a, Plu83b, VV85, Mit76]. **Pseudo-Inversen** [Gab82]. **Pseudo-Random** [BM82, BM84a, Boy89b, Plu83a, Plu83b, VV85, FHJ+84, LR86, Mit76]. pseudoinvers [Gab82]. pseudonym [Ano60]. pseudonyms [Cha79, Cha81], **Pseudoprimes** [PSW80]. **Pseudorandom** [Sha83b, KM88, Lev85, LR88b, RT88]. **Ptolemy** [Bud29, Bud76]. **PUB** [Nat85a, Nat85b, Uni83, NIS85]. **Public** [BG85, Boo81, Bur84a, Bur84b, CR85, Den84a, Dif88, ElG85b, ECW75, G84, Hel79, HP87, Kuc87, MI88, Oka88, RSA87, RSA83, SBC85, Sni83, WM85, Wil85, Yun85a, AM88, AM89, Ad83, Bar87, BBR88, BB79, BM84b, BS83, Cho86, CR88b, DDP85, Dif82a, EG85a, ElG85a, Fra89, GC80, GM85, G88, Gua87, HHL89, HL88, Her78, Her81, Hoo82, HW88, Kah79, Kar89b, KL84, Koy82b, Koy83, Lag84a, Luk83, LB88, LP87, Mer80, Mer82a, Mer82b, MN81, Nöb88, ORS+87, Riv74, Riv79, RSA82, Roy86, Sal85, SY86a, SY86b, SM83, Sse81, SS86, SSA87, TC85, TC86, TIF+88, Web88, WS79, Wil80, Wil86a, Ame81, B81, DB81]. **Public-Key** [BG85, Den84a, Dif88, G84, Hel79, Oka88, RSA83, WM85, Wil85, ECW75, AM88, AM89, Bar87, EG85a, GC80, G88, Gua87, HHL89, Her78, Hoo82, Kar89b, KL84, Koy82b, Koy83, LB88, LP87, MN81, Nöb88, ORS+87, Riv79, Sal85, SY86a, SY86b, TIF+88, WS79, Wil80, Wil86a]. **publication** [Uni83]. **Publications** [Lan46, Oak78, Pri83]. **Publishers** [Lit87]. **Publishing** [Had84, Lei79, San86]. **Puerto** [IEE79]. **Pugh** [WTE+85]. **Purple** [Cla77a, Cla77b, Fil77, Fil87]. **Puteani** [Put27]. **puzzle** [Bam82]. **puzzles** [CM85, Kalk84]. **Quadratic** [Sil87, MI88, PST88]. quae [Con39, Hei76]. quaesquer [Col64]. quality [Dem88]. **Quantum** [BB85, Wie87, BB89]. **Quasi** [BE79]. Quasi-Random [BE79]. queue [Col64]. **Queries** [WW84, SDV83]. quocunque [Con39]. quodam [Hei76]. R. **R.** [BCKS+83, WTE+85]. R. **R.** [BCKS+83, SWT+81]. rôle [Zaf63]. **Rabin** [ACG88, Koy83, SS84]. radars [Her89]. **Radio** [Ano22, BCKS+83, Ver26, Cam87, Hol87, Uni79b]. **Ralph** [Shu80]. **Ramp** [BM85]. **Random** [Agn87, Agn88, AM85, BM75, BM76, BM82, BM84a, Boy89b, BE79, FMC85, GGM85, GGM86, Plu83a, Plu83b, Ran55, Ran01, Tip27, VV85, Ayo87, Ayo85a, Ayo87, Bac88, BM89, Cam88, FHZ+84, Gab82, KP89, Koo86, LR86, Mit76, NM88, NU88, Vin71, Vin72]. **Randomized** [Bra87a, RS83, EGU85]. randomness [CG88]. **Rang** [Sto5]. rates [Lu79, Lu80]. **Read** [AWL+88, Koz84b, WTE+85, Koz84a, Win74b]. reading [Sea86]. Readings [AT&T86]. Real [QSA88]. Realistic [CMS89]. realizacja [Kos83]. **Realization** [WW84]. realizing [ISN87]. really [Gef73]. **Receive** [Bur81]. reception [MP86]. reciprocal [KM88]. **Reconstructing** [FHK+88]. record [IEE78b]. records [Ric74]. recurrences [LR88a]. **Recessiveness** [BCKS+83]. Red [Sch20, Sch33]. Rédei [Nöb84, Nöb85]. Rédei-scheme [Nöb84, Nöb85]. Reden [Sch20]. reduced [CE86]. reducing [VGT88, VGT89]. reduction [NM88]. redundancy [Lu79, Lu80]. **Reed** [MS81]. **Reference** [Lei79, Kas63, MS76]. Reflections [Sil83, Tho84, Tho87, Her89]. regarding [AM88, AM89]. Register
scripti [Put27]. scripturam [Tri06c, Tri21c]. sea [Bee81]. seal [Far67, Far69]. Sealing [GJ82, Gib81]. Search [BM75, BM76, BCKS+83, Jee81, Gul83, Sha86, Sie83]. Seattle [ACM89c]. Seberry [ST89]. Sec'83 [Fˆea83]. Second [San86, SBET85, HT79, HH79]. secondary [Fri35c, NBWH78, RF83]. Secrecy [EKW74, Mer82b, Sha49, Gif81]. Secret [Ano22, Blu83b, Cha85a, Cha85b, CGMA85, Cla12, Dro89, Fe87, Gin70, Has84, Hon19, ISN87, Nan36, Nan74, Nor73, Pie77, Pra39, Ric74, Sha86, Sha79, Ste87, TP63, Ver26, Wil41, Win69, Wol70, Yar40, Yun85a, Bam82, Bro86, Cal80, Fra84, Fra85b, Fra86, GM82, Jac87, Jon78b, Kah67a, Kah67b, Kah96, Ker89, Laf64, Lan81, Lew78, MS76, Mic88, NU88, Per90, RBO89, Smi43, Smi44, Smi55, Smi71, Ste76, Vam85, Win74a, Win74b, Win75, Wor89, Wri98, du 44, Kas63, SBET85]. secret-key [NU88]. secr`ete [S.73]. secr`etement [du 44]. secr`etes [Per90]. Secrets [MM87, SDV83, Ted85, Yao86, Kah83, MS81, Rab81]. Section [Den79b, Sim88]. sector [Ano80]. secundum [Hei76]. Secure [ACGS84, BW85, BP85, Bir85, CCD88, CM79, Den79a, GMR88, Gud80, LS89, Mer78, PK79, Sim82a, VV85, Win84, Yao82a, CG55, Hoo82, IN89, KM88, Lan89, MM82, Mit89, Pie77, Sha86, Ste87, Yun85b, KBN88]. Security [AM88, AM89, Ano78b, Ber80, BM85, BGK77, Bro81, Cha85c, DM83, FFea83, GJ82, IEE80, IEE83, IEE87c, IE88, Kol77, Lan89, LH84, Len78, Lit87, MHB1, Mu88, Pf89, Pur74, Rab89, RW84, San86, Sat89, Sch83, SS80, Som84, USE88b, USE88a, VK83, VK84, Ano78a, Ano82b, Ano84, Ano97, Bec97, BOCS83, BCW86, Bis89a, BO85a, BO85b, Bos82, Cho68, D+83, Den82, Dre79, Dro89, Eve85, Fal88, FLRT77, GST8, Gou89, HS85, Had84, HL88, Hog88, Hoo80, JL75, Kak83, KYM82, Ker89, Koe98, LB88, MM82, MRS87, MRS88, Mit76, Nat84, Nai89, Pri83, Rou84, Sch75, SP89, Ser85, Sie83, Sil83, Sin85, Ste89, Uni82a, Uni82c, UNN83, UNN85, Uni84, Uni81, Van78, dC87, FFea83, Had84, ST89]. Security-related [AM88, AM89]. sed [Hei76]. seed [Bou85]. seen [Uni79b]. sj`ao [du 44]. Selected [Ran82b, CM82]. Sel`enus [Wai100]. Self [Pro85, Sch86]. self-similarity [Sch86]. Self-Synchronizing [Pro85]. Selfcipher [Pel60]. Sel`eridge [Mul89b]. semigroups [Eck83]. Seminar [Mar70b, Mar70a]. Seminumerical [Km69, Km73]. Senate [Uni78b]. Senior [Mar70b, Mar70a]. sententi`am [Hei76]. Sentinel [Sup88]. September [BGK77, Ker75, San86]. Sequence [AWL+88, LT85, KM88, Phu82]. Sequences [BM82, BM84a, Boy89b, BE79, Gol67, Gol82, Gun88a, Phu83a, Phu83b, Sha83b, Boy89a, CE86, Kak85, Koo86, Nie88, Vos85, Von80b]. Serenissimum [Tri06b, Tri21b]. server [St.85]. Service [SS89, SNS88, NBWH78, St.84, Yar40]. ses [Jos85]. Set [Ne85, WC81, SX89]. seventeenth [ACM85]. Sex [Tri18]. Shakespeare [Arc22, FFW55, FF57, Lea87]. Shakespearean [FF57]. Shamir [BB79, SP79, Bar87, Lag84b, Od84]. Shaped [WTE+85]. Share [Sha79]. Shared [IW81, Fra89]. Sharing [CGMA85, FFe87, Bv82, DS81, DMS81, ISN87, MS81, RBO89, Sal73, Wil68a, Wil68b, Wil72, Wil75]. Shelta [MS76]. Shift [Gol67, Gol82, Bar84, Nie84]. shift-register [Bar84]. short [Bud76]. shortcut [Tuc79]. Should [SE86, Nai89]. shuffling [NS89]. Shulman [Lei79]. SIAM [RR86]. sic [Pie75]. Sieve [Sli87, PST88]. signal [Ano82b, Bar87, Eck85]. Signaling [Cla12]. signalling [Hol87]. Signals [And86, sC85, Win74b]. Signature [ElG85b, GMR85, GMR88, Ham71, HR82, Mer89, Mer89, OSS85, RB82, SS84, Sha85, Dem88, EG85a, ElG85a, FS87, Fun78, Her89,
[KD79, KD78, War82]. structures [ISN87]. studies [Uni79]. Study [Ame81, BBB+81, DB81, Cou86, Gai39, Gai40, Gai43, Gai44, Gai56, Lan81, Per85, Sie83]. subcategory [Uni81]. subexponential [Adl79, EI85c]. subexponential-time [EI85c]. subkey [Wel80, Wel82b]. Subkeys [DWK81]. Subliminal [Sim83, Sim85b, Hol87]. Subscription [Yun85a]. subsequences [Koo86]. Subset [LO85, IN89]. Substitution [HM83, Lev58, PR79, Bar75, Fri41, Fri45c, KD78, KD79, Lan81, Mit76]. substitution-permutation [K78, K79, K82]. subtle [du 44]. Subtractive [Mor83]. suit [Tri66c, Tri21c]. Suitable [Dav85]. Sum [LO85, IN89]. summary [Hei76]. Summer [Bur81, Ass88, USE99, USE99a, USE99b]. sunt [Con39]. Supercomputing [ACM89b, Bis89a, Hol87]. Superincreasing [Wil83a]. Support [BGK77]. supposititia [Hei76]. surveillance [Uni88a]. Survey [BO88, Ame86, Tho86, Pop89]. Sweden [Feea83]. Swedish [Gyl81]. Swift [Wei84]. Switching [IEE74]. Switzerland [Gua88b]. SX [LTW88]. SX-2 [LtW88]. Symmetric [QG89, Sim79, Sim82b]. symmetry [Fri45c, RF35]. sympathiques [S.73]. Symposium [ACM82, ACM83, ACM85, ACM86, ACM87, ACM88, ACM90a, ACM90c, AWL+88, IEE74, IEE94, IEE80, IEE82a, IEE83, IEE84, IEE85, IEE86b, IEE87a, IEE87c, IEE89]. Synchronizing [Pro85]. Synthese [SB82]. synthesis [GY58]. System [AT&T86, ARS83, Bur84a, Bur84b, Bur85, DWK81, GW76, Gmai80, Hen81, HR82, IL83, LHI84, LBI89a, LBI89b, Pro85, QSA88, RW84, SRC84, Sat89, SBC85, Sim83, TS88, TT84a, TT84b, BC88, BCW86, Cho86, Dro89, FLR77, Fra89, Fun78, Her81, Lan89, Lei80, Mil85, Mul81, MT86, SII83, Sor80, TIF+88, Van87, Van86, Ber80, KBN88]. System/38 [Ber80]. systèmes [S.73]. Systems [Agn87, Agn88, Ame86a, Ame85a, GMR89, HUR76, KBD89, Kon85, LT85, Mur87, Sha33a, Sha49, SNS88, As88, Ver26, Ame83, Bar84, BP82, Bla89, Cha85c, CF88, Del79, Fri35b, Fri41, FF75, Gon89, Hoe80, HW88, Lan81, Mer82b, MMA82, NBW87, PEA80, SC81, WIL86b, OIL72, WIL75, CA83b, CA83a].


Sweden [FAS83]. Swedish [Gyl81]. Swift [WEI84]. Switching [IEE74]. Switzerland [Gua88b]. SX [LTW88]. SX-2 [LTW88]. Symmetric [QG89, Sim79c, Sim82b]. symmetry [FRI35C, RF35]. sympathiques [S.73]. Symposium [ACM82, ACM83, ACM85, ACM86, ACM87, ACM88, ACM90a, ACM90c, AWL+88, IEE74, IEE79, IEE80, IEE82a, IEE83, IEE84, IEE85, IEE86b, IEE87a, IEE87c, IEE89]. Synchronizing [PRO85]. Synthese [SB82]. synthesis [GY58]. System [AT&T86, ARS83, Bur84a, Bur84b, Bur85, DWK81, GW76, Gmai80, Hen81, HR82, IL83, LHI84, LBI89a, LBI89b, Pro85, QSA88, RW84, SRC84, Sat89, SBC85, Sim83, TS88, TT84a, TT84b, BC88, BCW86, Cho86, Dro89, FLR77, Fra89, Fun78, Her81, Lan89, Lei80, Mil85, Mul81, MT86, SII83, Sor80, TIF+88, Van87, Van86, Ber80, KBN88]. System/38 [Ber80]. systèmes [S.73]. Systems [AGN87, AGN88, Ame86a, Ame85a, GMR89, HUR76, KBD89, Kon85, LT85, Mur87, Sha33a, Sha49, SNS88, As88, Ver26, Ame83, Bar84, BP82, Bla89, Cha85c, CF88, Del79, Fri35b, Fri41, FF75, Gon89, Hoe80, HW88, Lan81, Mer82b, MMA82, NBW87, PEA80, SC81, WIL86b, OIL72, WIL75, CA83b, CA83a].

REFERENCES

**wits** [See89]. **Wizard** [Jon78a]. **Wolfe** [Sto65]. **woln** [Sch20]. **Word** [BS86, BO85d, McC75, WM85, Bar75, Eve85]. **words** [AG85]. **Work** [Goo79]. **working** [BB89]. **Works** [AWL88]. **Workshop** [Bet83, BCI87, CP87, CP88, Gun88b, QV89, USE88b, USE88a, Pic86].

**Workstations** [NS88]. **World** [AWL88, HT79, HH79, Ritxx, SBET85, WTE85, Cla77b, Bar79c, Bar79b, Cla77a, Elv87, Gyl31, Gyl34, Koz84a, Koz84b, Lew78, Lit87, Men89, Win74b]. **worldwide** [Int87, Int88]. **Worthy** [AWL88]. **would** [Gar77]. **writing** [Hul98, Kah67a, Kah67b, Kah96, Kas63, Laf64, Nan36, Nan74, Ric74, Sea86, Smi43, Smi44, Smi55, Smi71, Wol70, Zim48, du 44, Gin80]. **writings** [Col64, Lan81, Per90]. **wrong** [HM88]. **wrote** [FF57]. **WW** [Pli98].

**X.509** [Cop89]. **X3** [ML87]. **X.9.23** [AA88]. **Xvi** [Lei79]. **xviii** [Shu80].

**year** [Dif82b]. **Years** [BCKS83, Dif88, Ash87, Gar77]. **yesterday** [DKKM87]. **York** [ACM87, Lei79, MZS79, Sin77]. **York/London** [Lei79]. **yourself** [FS87].

**Z** [Kno79]. **zastosowan** [Kos83]. **Zeit** [Sch20]. **Zendian** [Cal89]. **Zero** [WTE85, BFM88]. **zero-knowledge** [BFM88]. **Zimmermann** [FM76, Tuc66]. **zone** [Ano89]. **Zufallsgeneratoren** [Gab82]. **Zur** [SB82].

References


REFERENCES


[ACM89c] ACM, editor. *Proceedings of the Twenty First Annual ACM Symposium on*
REFERENCES


REFERENCES

Akritas:1983:CEA


Alberti:1470:TC

[Alb70] Leon Battista Alberti. *Trattati in Cifra. (Italian) [Treatises in ciphers]*. ????, ????, 1470. ????.

Alexander:1945:CHG


Ahituv:1987:PED


Akl:1985:FPR


Adams:1988:SRC


Adams:1989:SRC


ACE:1981:RPC


Anonymous. Introductory talk to members of the William and Mary College cryptanalysis class. Technical report, William and Mary College, Williamsburg, VA, USA, 1939. 7 pp.
REFERENCES

Anonymous:1976:CCA


Anonymous:1978:CSD


Anonymous:1981:CHP


Anonymous:1981:GIU


Anonymous:1982:CC

REFERENCES

[Ano82b] Anonymous. Encryption scrambling the satellite signal for security, 1982. 1 sound cassette (75 min.).


Anonymous:1989:SZS

Aruliah:1985:PIE

Arensberg:1921:CD

Arensberg:1922:CSP

Adleman:1983:CCS

Alpern:1983:KEU

Ashenhurst:1987:ATA

USENIX:1988:CSSb

Akl:1983:CSP
Selim G. Akl and Peter D. Taylor. Cryptographic solution to a problem of access control in
REFERENCES


**ATT:1986:AUS**


**Aspray:1988:RCD**


**Ayoub:1968:EKR**


**Ayoub:1968:EEK**


REFERENCES


REFERENCES


Held at the University of Paris, Sorbonne.
REFERENCES


Birnbaum:1986:VPS


Borucki:1974:MNN


Bright:1979:QRN


Becker:1982:EDE


Beckett:1988:IC


Beckett:1997:ICP

Brian Beckett. Introduction to cryptology and PC security. McGraw-Hill, New York, NY,
REFERENCES


Beesly:1981:CIW


Behrens:1954:EUP


Bell:1977:IVU


Bennett:1980:UWN


Bennett:1989:UMS


Bertrand:1973:EOP


Berstis:1980:SPD


Bertrand:1983:EGE


Bergmann:2009:DKR


Beth:1983:CPW

REFERENCES


Blum:1985:EPP


Branstad:1977:RWC


Bar-Ilan:1989:NFC


Birrell:1985:SCU


Bishop:1988:AFDa

Matt Bishop. An application of a fast Data Encryption Standard implementation. Technical report PCS-TR 88-138, Department of Mathematics and Computer Science, Dartmouth Col-
REFERENCES


REFERENCES


[Blu83b] Manuel Blum. How to exchange (secret) keys. *ACM Transactions on Computer Systems*, 1
REFERENCES


REFERENCES


Beale:1989:EUR


Blake:1985:CLG


Book:1985:SNP


Book:1985:SNS


Book:1985:VTA


Book:1985:CRE

REFERENCES


**Brickell:1988:CSR**

**Ben-Or:1983:CSS**

**Ben-Or:1988:MIP**

**Ben-Or:1988:CTN**

**Bond:1947:FSC**

**Booth:1981:ASU**

**Bosworth:1982:CCC**

**Bounas:1985:DDS**

**Bowers:1959:DSP**
William Maxwell Bowers. *Digraphic substitution: the Playfair cipher, the four square cipher*. Practical cryptanalysis; v.


REFERENCES


Blakley:1988:CBA


Bracha:1987:ERR


Brassard:1988:MCT


Brassard:1989:CCb


Brassard:1989:CCa


Brassard:1990:ACC

REFERENCES


REFERENCES


[BW89] P. T. Bateman, J. L. Selfridge, and S. S. Wagstaff, Jr. The new Mersenne conjecture. *American Mathematical Monthly*, 96(2):125–128, February 1989. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic). See letter to the editor [Mul89b]. The authors state: NEW MERSSENNE CONJECTURE. *If two of the following statements about an odd positive integer $p$ are true, then the third one is also true. (a) $p = 2^k \pm 1$ or $p = 4^k \pm 3$. (b) $M_p (= 2^p - 1)$ is prime. (c) $(2^p + 1)/3$ is prime.*


REFERENCES

[Budge:1976:RSB]

[Burchard:1981:NNF]

[Bur84b]

[Bur85]

[Bv82]

[Beker:1985:KMS]


[Cal89] Lambros D. Callimahos. Traffic Analysis and the Zendian Problem: an exercise in communications intelligence operations. Aegean Park Press, La-
REFERENCES


Chaum:1978:ICP


Christoffersson:1988:CUH


Coppersmith:1975:GCA

Don Coppersmith and Edna Grossman. Generators for certain alternating groups with applications to cryptography.


Chor:1985:RRL


Cover:1987:OPC


Chor:1988:UBS

Benny Chor and Oded Gol-
REFERENCES


REFERENCES

by the International Association for Cryptologic Research.


[Chu89] Ta-Fu Chuang. Non-homomorphically encryption schemes and properties of Chinese remainder theo-


[


REFERENCES


Chor:1989:SCT


Crilly:1987:BPB


Cohen:1987:IP


Colaco:1864:CRO

F. N. Colaço. A cryptographia revelada, ou, Arte de traduzir e decifrar as escrituras obscuras, quaesquer que sejao os caracteres empregados. (Portuguese) [Cryptography revealed, or, the art of translating and deciphering obscure writings, whatever the characters employed]. De Santos e Cia, Pernambuco, Brazil, 1864. 93 pp. LCCN Z104.C68 1846.

Cominsky:1987:CAP


Conradi:1739:CDS


Coombs:1983:MC

Coppersmith:1984:FEL


Coppersmith:1987:C


Coppersmith:1989:AID


Coppersmith:1986:DL


Courville:1986:MCC


Chaum:1987:ACE


Chaum:1988:ACE


Chor:1985:KTP

[CR85] Benny Chor and Ronald L. Rivest. A knapsack type pub-


DeMillo:1983:ACC


D'Agapeyeff:1939:CC


D'Agapeyeff:1971:CC


DRC:1985:AAN


Davida:1981:CAR

George I. Davida. The case against restraints on non-governmental research in cryptography. Communications of the Association for Computing Machinery, 24(7):445–450, July 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). This is an opposing view published with [Ame81].

Davies:1985:MAA

Dawson:1985:COL


Denning:1981:SRR


Denning:1989:EET


DeJonge:1986:ASR


DeJonge:1987:SVR


Davio:1985:EHS

[DDG+85] Marc Davio, Yvo Desmedt, Jo Goubert, Frank Hoornaert, and Jean-Jacques Quisquater. Efficient hardware and software implementations for the DES. In Blakley and Chaum [BC85], pages 144–146. CODEN LNCS-09. ISBN 0-387-15658-
Delsarte:1985:FCM


Deavours:1987:CP1


Deavours:1988:BPS


Demirdogen:1988:FDM


Denning:1979:SPC


Denning:1979:EOS

Peter J. Denning. Editor’s overview — special section on
REFERENCES


REFERENCES


[DH77]


[Die88]


[Dif82a]


[Dif82b]

REFERENCES

[Deavours:1985:MCM]

[Deavours:1989:CMH]

[Deavours:1987:CYT]

[DeMillo:1982:CP]

[delaStelle:1902:TCF]

[DeMillo:1983:PDS]

[Denning:1981:MMK]

[Desmedt:1986:CTA]
References


[du 44] Maistre Iean Robert du Carlet. La cryptographic: contenant
vne tres-subtile manier d'escrire secrètement. (French) [Cryptography: containing a very subtle manner of secret writing]. Imprimeur ordinaire du Roy et R. Aurelhe, Marchand libraire, Paris, France, 1644. 234 + 2 pp. LCCN Z103.5 .D82 1644b.

Davida:1981:DES


Ecker:1982:MGE


Ecker:1983:FSR


Ecker:1985:STS


Ellis:1975:PKC


Edwards:1915:CCT


Epstein:1956:FBC

Sam Epstein and Beryl Epstein. The first book of codes and ciphers. Franklin Watts, New York, NY, USA, 1956. LCCN
Z104 .E68. Pictures by Laszlo Roth.

El-Gamal:1985:PCS


Even:1985:PCC


ElGamal:1985:PKCa


ElGamal:1985:PKCb

REFERENCES

??&volume=0&issue=0&spage=10. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

ElGamal:1985:STA


Elvin:1987:CWW


Ehrsam:1978:CKM


Er:1989:NAG


Estell:1980:BW


Even:1985:CSW


Falk:1988:DST

REFERENCES

**Farago:1967:BSS**


**Farago:1969:BSS**


**Feak:1983:SIS**


**Feistel:1973:CCP**


**Feldman:1987:PSN**


**Ferris:1987:WBC**


**Feynman:1982:SPC**


**Friedman:1957:SCE**


**Friedman:1955:CLS**

REFERENCES


REFERENCES


REFERENCES

Franklin:1985:MID


Franksen:1985:MBS


Franksen:1986:SHM


Frankel:1989:TIC


Friedman:1935:ICA


Friedman:1935:MCP


Friedman:1935:PI


Friedman:1939:MC

REFERENCES


REFERENCES


Fiat:1987:HPY


Funk:1978:DUS


Futrelle:1973:BTM


Gabriel:1982:VPI


Gaines:1939:ECS


Gaines:1940:ECS


Gaines:1943:ECS

REFERENCES


Galland:1945:HABb


Galland:1945:HABc


Galland:1970:HAB


Galil:1988:SIC


Gamble:1988:IDL


Gardner:1977:MGN


Garlinski:1979:IEW


Garlinski:1980:EW


Gilmour-Bryson:1982:CDT

REFERENCES

LCCN K662.14 I58. From Computing Reviews: “The article reports on the progress of an historical study using a computer for statistical analysis. The subject of the study is a mass of trial depositions of the Knights Templar. The purpose of the project is to find statistical regularities in the large amount of testimony and to create a model for similar studies. The Order of the Knights Templar, founded around 1100, was the first Christian military order. After the Crusades, in the early fourteenth century, 127 articles of accusation were brought against the order, including charges of idolatry, sacrilege, and sodomy. The data being studied are the responses of 900 men to each of 127 accusations. The article details the accusations and the way in which the responses are being coded. The statistical package SAS (Statistical Analysis System) will be used. Examples of the results to be sought are: tallies of guilty/innocent responses, tallies of offenses committed versus seen versus heard about, and correlations between, for example, age and other responses. Depositions that differ markedly from the average response will be identified.”

Goethals:1980:CAL

Girault:1988:GBA

Geffe:1973:HPD
P. Geffe. How to protect data with ciphers that are really hard to break. Electronics, 46(1): 99–101, 1973. ISSN 0883-4989. This cipher was later broken by [Sie85].

Gersho:1982:ACR

Goldreich:1985:CAR

Goldreich:1986:HCR


Garey:1979:CIG

REFERENCES


Gifford:1982:CSI

Gligor:1979:OMA

Goldreich:1989:HCP

Gleason:1957:ECP

Gleason:1986:ECP

Gleason:1987:PIC

Goldwasser:1982:PEH
Goldwasser:1984:PE


Goldwasser:1985:NTK


Good:1945:GRT

Goldreich:1987:HPM


Goldreich:1987:HPM

Golomb:1967:SRS

REFERENCES


Golomb:1982:SRS

[Gol82]

Goldwasser:1984:PET

[Gol84]

Gong:1989:SCB

[Gon89]

Good:1979:EWC

[Goo79]

Gordon:1985:SPE

[Gor85]

Held at the University of Paris, Sorbonne.

Gleason:1985:ECP

[GPW85]

Grover:1982:CP

[Gro82]
Grundler:1984:DEH


Gaines:1978:SSP


Grollmann:1984:CMP


Grollmann:1988:CMP


Guarini:1904:MTT


Guan:1987:CAP


Gudes:1980:DCB


Gullichsen:1983:BHS


Gunther:1988:ASG

REFERENCES


Gunther:1988:ACE


[Gun88b]

Gamow:1958:CAP


Galil:1987:PEA


Gylden:1931:CEI


Gylden:1933:CCB

REFERENCES


[Gyl38] Yves Gylden. Analysis from the point of view of cryptanalysis of “cryptograph type C-36,” provided with six key wheels, 27 slide bars, the latter having movable projections, single or multiple. A. B. Teknik co., Stockholm, Sweden, 1938. 10 pp.


[Ham88] Johan Hästad. Solving simultaneous modular equations of


REFERENCES

Hershey:1981:DLP


Hersch:1989:DSA


Hardy:1985:ECC


Hoornaert:1985:EHI


Hinsley:1979:BISb


Harn:1989:PAU

REFERENCES


Higenbottam:1973:CC


Hill:1929:CAA


Hill:1931:CCL


Hitt:1943: MSM


He:1988:SDK


Hunter:1983:ERA


Hule:1988:RCW


Hodges:1983:ATE


Hoffer:1955:MAC


Hogan:1988:PIS

Carole B. Hogan. Protection imperfect: the security of some
REFERENCES


[Hollis:1987:TCA]


[Honore:1919:STS]


[Hood:1980:EFS]


[Hoogendoorn:1982:SPK]


[Herzberg:1987:PPS]


[Holland:1982:GSA]


[Harrison:1976:POS]


[Haastad:1985:CST]

REFERENCES

Hammer:1987:EUH

Hardjono:1989:TCB

Hinsley:1979:BISa

Huang:1988:APE

Hulme:1898:CHP

Hunter:1985:ARK
REFERENCES

Hotrdy:1975:ITN


Hartnell:1976:PFM


Hardy:1979:ITN


Huthnance:1988:UPP


IEEE:1974:ASS


IEEE:1981:CLC


IEEE:1982:ASF

[IEE82a] IEEE, editor. *23rd annual Symposium on Foundations of Com-
REFERENCES


REFERENCES


[IL89] R. Impagliazzo and M. Luby. One-way functions are essen-
REFERENCES

tial for complexity based crypt-
ography. In IEEE [IEE89],
pages 230–235. CODEN ASF-
PDV. ISBN 0-8186-1982-
1 (casebound), 0-8186-5982-3
(microfiche). ISSN 0272-5428.
LCCN QA 76 S979 1989. IEEE
catalog number 89CH2808-4.

[IM86] Hideki Imai and Tsutomu Mat-
sumoto. Algebraic methods for
constructing asymmetric cryp-
tosystems. Lecture Notes in
Computer Science, 229:108–119,
1986. CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349
(electronic).

[IN89] Russell Impagliazzo and Moni
Naor. Efficient cryptographic
schemes provably as secure as
subset sum. In IEEE [IEE89],
pages 236–241. CODEN ASF-
ISSN 0272-5428. LCCN QA 76
S979 1989. IEEE catalog num-
ber 89CH2808-4.

[Int81b] International Resource Devel-
opment, Inc. Data, text, and voice
cryptosystems. Report 81, Inter-
national Resource Develop-
ment, Inc., 54 Prowitt St., Nor-
walk, CT 06851, USA, 1981. vi + 154
pp.

[Int84] International Resource Devel-
opment, Inc. Data, text, and voice
cryptosystems. Report 630, Interna-
tional Resource Development, 6 Prowitt St., Nor-
walk, CT 06855, USA, 1984. vi + 184 pp.

[Int87] International Resource Devel-
opment, Inc. Data, text and voice
cryptosystems worldwide markets.
Report 727, International Re-
source Development, 6 Prowitt
St., Norwalk, CT 06855, USA,

[Int88] International Resource Devel-
opment, Inc. Data, text and voice
cryptosystems worldwide markets.
Report 754, International Re-
source Development, New Canaan,
Conn., U.S.A. (21 Locust Ave., New Canaan

Limits on the provable con-
sequences of one-way permu-
REFERENCES

Ito:1987:SSS

[ISN87]

Ingemarsson:1981:UAS

[IW81]

Jackson:1987:NTS

[Jac87]

Jeffery:1986:GCC

[Jef86]

Jevons:1874:PS

[Jev74]

Jones:1975:ESP

[Joh89]

Jurgensen:1984:SRI

[JM84]

Johnson:1989:BDC

[Joh89]

Jones:1978:WWB

[Jon78a]

Jones:1978:MSW
Reginald V. Jones. Most secret war: [British scientific in-
REFERENCES


REFERENCES


REFERENCES


REFERENCES

0190 (print), 1872-6119 (electronic).


REFERENCES

**Knoble:1979:EOW**


**Kilian:1988:FCO**


**Kak:1977:SEU**


**Kothari:1984:CMW**


**Kannan:1988:PFN**


**Kurosawa:1988:CSP**


**Konheim:1980:ICP**


**Knoble:1979:AEO**

REFERENCES


Knu80 Donald E. Knuth. Deciphering a linear congruential encryption. Report 024800, Department of Computer Science, Stanford University, Stanford, CA, USA, 1980.


REFERENCES

Konheim:1981:CP


Konheim:1985:CAE


Konheim:1989:RMC


Koopman:1986:OES


Koscielny:1983:PRD


Kothari:1985:GLT

REFERENCES


Kordes:1989:UMC


Kuchlin:1987:PKE


Kullback:1935:SMC


Kullback:1938:SMC


Kullback:1967:SMC


Kullback:1976:SMC


Kearns:1989:CLL


Kasami:1982:KMS

REFERENCES

Laffin:1964:CCS


Lagarias:1984:KPK


Lagarias:1984:PAS


Lakshmivarahan:1983:APK


Lampson:1973:NCP


Lamport:1981:TNP


Landers:1946:RPR


Langie:1981:CSS


Landau:1989:SSC

[Lan89] Charles R. Landau. Security in a secure capability-based sys-
REFERENCES

Lassek:1985:CCA

Teresa A. Lassek. Cryptology and the computer age. Thesis (Honors), University of Nebraska at Omaha, Omaha, NE, USA, 1985. 58 pp.

Lauer:1981:CSC


Lee:1988:OSM


Lee:1989:WBL


Leary:1987:CSM


Leclerc:1989:CRM


Leighton:1979:BRB

REFERENCES

Leiss:1980:NSS


Lempel:1979:CT


Lennon:1978:CAI


Lenstra:1987:FIE


Levine:1958:VMS


Levine:1961:SAH


Levine:1961:SECa


Levine:1961:SECb


Levine:1983:USC


Levin:1985:OWF

REFERENCES


Lewin:1978:UGW

Lewin:1982:AMC

Landwehr:1984:SMM

Lidl:1985:CBP

Lieberherr:1981:UCD

RFC0989

RFC1040
REFERENCES

111

Obsoleted by RFC1113 [Lin89]. Obsoletes RFC0989 [Lin87]. Status: UNKNOWN.

RFC1113


RFC1421


1872-6119 (electronic). See notes [Mei81, Hel81].

[Lidl:1984:PPR]

[Leighton:1985:HBC]

[Lagarias:1985:SLD]

[Lomet:1983:HPU]

[Luciano:1987:CCC]

[Luby:1986:PRP]
REFERENCES


REFERENCES


Lioen:1988:OMA


Lu:1979:EGC


Lu:1980:AEG


Long:1988:DLH


Ma:1979:RAD


Meijer:1981:DSS


MacPherson:1987:CUN

REFERENCES

Mandelbrot:1960:BRJa


Massey:1983:LFC


Marsh:1970:CSS


Marsh:1970:MEC


Mastrovito:1989:VDM


Matyas:1979:DSO


Mauborgne:1914:APC

REFERENCES

Milner-Barry:1986:ADL

P. S. Milner-Barry. ‘Action This Day’: The letter from Bletchley Park cryptanalysts to the Prime Minister, 21 October 1941. Intelligence and National Security, 1(2):??, 1986. ISSN 0268-4527 (print), 1743-9019 (electronic).

McCarthy:1975:AFP


McIvor:1985:SC


Meador:1920:KCE


Meijer:1981:NCM


Meijer:1983:CCC

Henk Meijer. Cryptology computational complexity and applications. Thesis (Ph.D.), Queen’s University, Ottawa, ON, Canada, 1983. 2 microfiches (179 fr.).

Meijer:1985:MEN


Mendelsohn:1939:CC


Mendelsohn:1989:CWI

REFERENCES


[Mersenne:1644:CPM]
Marin Mersenne. Cogitata Physica-Mathematica ... [Tractatus de mensuris ponderibus atque nummis ... Hydraulica pneumatica; arsque navigandi. Harmonia theorica, practica. Et Mechanica phaenomena. Ballistica et acontismologia]. Antonii Bertier, Paris, France, April 1, 1644. [30], 40 [24], 41–370, [16], 96, [8], 138, [34] + 40 pp. URL http://www.mersenne.org/prime.htm; http://www.mersenne.org/status.htm. Three volumes. This is the book that introduced the conjecture that numbers of the form \( M(n) = 2^n - 1 \) are prime for \( n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 \), and 257, but could not test this claim. Euler showed in 1750 that \( M(31) \) is prime. Lucas showed in 1876 that \( M(127) \) is prime. Pervouchine showed in 1883 that \( M(61) \) is prime, finally disproving the Mersenne conjecture. Powers in the early 1900s showed that \( M(89) \) and \( M(107) \) are prime, both missed by Mersenne. By 1947, it was known that the correct list is 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 and 127, so Mersenne had five errors in his list: 67 and 257 should have been removed, and 61, 89, and 107 added. By late 2001, 39 Mersenne primes were known, the five largest having been found by mas-

[Merkle:1978:SCI]

[Merkle:1980:PPK]

[Merkle:1982:PPK]

[Merkle:1982:SAP]
REFERENCES

Merkle:1988:DSB


Merkle:1989:CDS


Merkle:1978:HIS


Merkle:1981:SME


Matsunoto:1988:PQP


Michener:1988:TSK


Millkin:1943:ECCa


Millkin:1943:ECCb

REFERENCES


REFERENCES


REFERENCES


REFERENCES


[C. Müller-Schloer. A microprocessor-]

**Mullender:1986:DCD**


**Marayati:1987:AWA**


**Mackinnon:1985:OAA**


**Muftic:1988:SMC**

Sead Muftic. Security mechanisms for computer networks. current results of the CEC COST-11 ter project. *Computer Networks and ISDN Sys-


REFERENCES


REFERENCES

[NIST:1985:FPC]

[Nissan:1989:AIM]

[Nakamura:1988:DRM]

[Nobauer:1984:CRS]

[Nobauer:1985:CRS]

[Nobauer:1988:CPK]

[Norman:1973:SWB]

[Needham:1978:UEAa]

[Needham:1978:UEAb]
REFERENCES


REFERENCES

[Odlyzko:1985:DLF]

[Odlyzko:1987:CCD]

[Odlyzko:1987:ACC]

[Okamoto:1988:DMS]
Patrick E. O’Neil. The Escrow transactional method. ACM Transactions on Database Sys-
REFERENCE


Otway:1987:ETM

Orton:1987:VIP

O'Shea:1988:CDU

Ong:1985:ESS

Ozarow:1984:WTC
Lawrence H. Ozarow and Aaron D. Wyner. Wire-tap channel II. ATT Bell Lab. tech. j, 63(10 part 1):2135–2157, 1984. CODEN ABLJER. ISSN 0748-612X.

Parthasarathy:1985:DSG

Patterson:1987:MCC
Wayne Patterson. Mathematical
REFERENCES


Preneel:1989:CHB


Percy:1980:EDS


Pelt:1960:SP


Perret:1890:RCS


Peralta:1985:TRN

[Rene Caupolican Peralta. Three results in number theory and cryptography: a new algorithm to compute square roots modulo a prime number; On the bit complexity of the discrete logarithm; A framework for the study of cryptoprotocols. Thesis (Ph.D.), Department of Computer Science, University of California, Berkeley, Berkeley, CA, USA, December 1985. 52 pp.]

Pfleeger:1989:SC


Pohlig:1978:IAC

[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(1):]
REFERENCES


REFERENCES

Posch:1989:AEA


Peleg:1979:BSC


Pratt:1939:SUS


Pritchard:1980:DE


Price:1983:ABR


Pronzini:1980:MCC


Proctor:1985:SSC

REFERENCES


Pomerance:1988:PAF


Pomerance:1980:P


Purdy:1974:HSL


Purdy:1974:HSL


Pfitzmann:1986:NUO


Pfitzmann:1987:NUO


Quisquater:1989:BHF

J. J. Quisquater and M. Girault. $2n$-bit hash-functions using $n$-

**Rabin:1981:HES**

**Rabin:1989:EDI**

**Rand:1955:MRD**

**Randell:1982:CGC**
Randell:1982:ODC


Rand:2001:MRD


Rao:1984:JEE


Rhodes-Burke:1982:RSA


Rabin:1989:VSS


Reeds:1979:CMC


Reischuk:1985:NSB


Rejewski:1977:ATP


Rejewski:1981:HPM

Afterwords by Cipher A. Deavours and I. J. Good. This article was entitled “Jak matematycy polscy rozszyfrowali Enigmgę” in the Annals of the Polish Mathematical Society, Series II, Wiadomości Matematyczne, Volume 23, 1980, 1-28, translated by Joan Stepenske. See minor correction [Ano81a].


Sheila R. Richards. Secret writing in the public records: Henry VIII–George II. London, 1974. x + 173 + 4 plates pp. UK£4.50. Contains one hundred documents, all but one of which are written wholly or partially in cipher and are now deciphered and printed in full for the first time. Includes letters in French or Italian, with a summary in English.


Rivest:1979:CRC


Rivest:1980:DSC


Rivest:1985:RCP


Rivest:1987:EDR


Reeds:1985:NPR


Rao:1987:PKA

[RN87] T. R. N. Rao and Kil-Hyun Nam. Private-key algebraic-coded cryptosystems. Lec-
REFERENCES


[Roy86] Marc Paul Roy. A CMOS bit-slice implementation of the RSA public key encryption algorithm. Thesis (M.Sc.(Eng.)), Queen’s University, Ottawa, ON, Canada, 1986. 3 microfiches (210 fr.).

REFERENCES


[RS84] Rivest:1984:HEE

[RSA78] Rivest:1978:MOD

[RSA82] Rivest:1982:MOD

[RT88] Reif:1988:EPP

[RU88] Raleigh:1988:CDP

[Rub79] Rubin:1979:DSC
Rudolph:1982:HTI


Ruggiu:1985:CCT


Russell:1927:CMS


Reeds:1984:FSU


Rytter:1986:SCU


S:1873:COD


Sacco:1936:MC

REFERENCES


Saltzer:1973:PCI


Saltzer:1978:DS


Salomaa:1985:PKC


Sansom:1986:BRC


Sandhu:1988:CIT

REFERENCES


REFERENCES


Chen:1985:RGE

Scacchitti:1986:CT

Schwenter:1620:SSN

Schwenter:1633:SSA

Schroeder:1975:ESK
REFERENCES

1975. CODEN OSRED8. ISSN 0163-5980.


REFERENCES


“If the base 2 is used the resulting units may be called binary digits, or more briefly, bits, a word suggested by J. W. Tukey.”. This is the first known printed instance of the word ‘bit’ with the meaning of binary digit.

Shannon:1948:MTCb


Shannon:1949:CTS


Shamir:1979:HSS


Shamir:1982:PTA


Shamir:1983:ECS


Shamir:1983:GCS


Shamir:1984:PTA

Shamir:1985:IBC


Shamir:1986:SPS


Shamir:1987:CSS


Sherman:1986:CVT


Sherman:1987:CVT


Sharp:1988:DCO


Shulman:1976:ABC

REFERENCES


REFERENCES


Simonetta:1404:LTC


Simmons:1979:HID


Simmons:1979:CCA


Simmons:1979:SAE


Simmons:1982:SCA


Simmons:1982:SAE


Simmons:1983:PPS


Simmons:1984:HID

REFERENCES

Simmons:1985:ATC


Simmons:1985:SCD


Simmons:1988:SSC


Sinkov:1966:ECM


Sinkov:1968:ECMa


Sinkov:1968:ECMb


Sinnott:1977:CTC

REFERENCES

Singh:1985:IPS


Sambur:1976:SEM


Schobi:1983:FAT


Smith:1943:CSS


Smith:1971:CSS


Smith:1983:PKC

John Smith. Public key cryptography: An introduction to a powerful cryptographic system for use on microcomputers. *BYTE Magazine*, 7(??):198–218, January 1983. CODEN BYTEDJ. ISSN 0360-5280. This is a simple exposition of public key cryptography.

Smith:1944:CSS


Steiner:1988:KAS

REFERENCES


IBM (United Kingdom Laboratories), Hursley Park, Winchester, UK, May 1989.

Subramanian:1987:DTP


Siromoney:1988:CPL


St.Johns:1985:RAS


Shawe-Taylor:1989:BRB


St.Johns:1993:RIP

edupub/tex/bib/cryptography bib. Obsoletes RFC0931 [St.85]. Status: PROPOSED STANDARD.

Stark:1970:INT


Stark:1978:INT


Stevenson:1976:MCI


Stern:1987:SLC


Stevens:1988:CPR


Stephenson:1989:PPM


Stout:1965:DRN


Stoll:1989:CET


Stripp:1987:BJC

REFERENCES

**Stripp:1989:CFE**


**Summers:1984:OCS**


**SuperMacSoftware:1988:SDE**


**Shulman:1961:GC**


**Smith:1983:HCR**


**Salzer:1981:RHH**


**Sun:1989:TKE**


**Salomaa:1986:PCB**


**Salomaa:1986:PKC**

REFERENCES


[Tex84] Texas Instruments Inc. TMS7500 TMS75C00 user’s guide, data encryption device: 8-bit microcomputer family. Texas Instruments, Dallas, TX, USA, 1984. various pp.


REFERENCES

[158]


[Tsujii:1988:PKC]

[Tippett:1927:RSN]

[Thompson:1963:SDE]

[Trithemius:1518:PLS]

[Trithemius:1606:CGT]

[Trithemius:1606:CSI]

[Trithemius:1606:SHE]
Johannes Trithemius. *Steganographia: hoc est, ars per occultam scripturam animi sui voluntatem absentium aperiendi certa*. Matthiae Beckeri, Frankfurt, Germany, 1606. 8 + 180 pp. LCCN Z103.T84 S 1606. Authore ... Ioanne Trithemio ...; praefixa est huic operi sua clausis, seu vera introduction ab ipso authore concinmata ... nunc vero in gratiam secretioris philosophiae studiosorum publici iuris facta. Francofurti. Ex officina typographica Matthiae Beckeri, sumptibus Ioannis Berneri, anno 1606.
REFERENCES

Trithemius:1621:CGT


Trithemius:1621:CSI


Trithemius:1621:SHE


Terry:1988:MSV


Tsudik:1989:DAI


Tbersites:1984:IKE


Thomas:1984:IKE

REFERENCES


REFERENCES

**USASC:1942:ACC**


**USDOS:1970:BC**


**USNBS:1977:DES**


**USCSC:1978:CSD**


**USCSC:1978:USN**


**USNA:1979:CS**


**USNSG:1979:IRW**


**USNBS:1981:GIU**

REFERENCES

USDA:1982:SMM

USDA:1982:TGM

USGSA:1982:TGS

USNBS:1983:FPD

USGSAOIRM:1984:ISR

USGAOPEMD:1987:PDD

USDA:1988:CED

USNBS:1988:DES


REFERENCES


[Van86] Ronald D. Vandeberg. Implementation of a coprocessing sys-
REFERENCES


VanHeurck:1987:TNS


VanTilborg:1988:IC


Vernam:1926:CPT


Vallee:1988:HBO


Vallee:1989:HGR


Vincent:1971:PAG


Vincent:1972:CPA


Voydock:1983:SMH

Voydock:1984:SMT

Kerckhoffs:1883:CMF

Vogel:1985:LCC

Vassiliadis:1988:PEA

Volts:1941:BCP

Voukalis:1980:DFC

Voukalis:1980:GSE

Vassiliadis:1988:PEA

Volts:1941:BC
heavy leaves precede sections II-IV (not included in pagination). This copy was made especially for the United States Army from the original manuscript. Third copy: pencilled note on cover. Contents: pt.1. Cryptography; pt.2. Titles relating indirectly to cryptography; pt.3. Rejected titles; pt.4. Author index.

vanTilburg:1986:DBK


Vazirani:1985:ESP


Valiant:1986:NED


Waber:1987:VEC


Wagner:1983:F


Walden:1900:ADB

Wang:1986:UEA


Warren:1982:BTC


Watler:1989:VAC


Wegman:1981:NHF


Weber:1979:USD


Weiss:1988:BOP


Wells:1980:ADB


Welchman:1982:HSS


Wells:1982:USE

[Wel82b] David L. Wells. The use of subkey encryption to counter traffic analysis in communications networks. Technical report CSE 8201, Department of Computer Science and Engineering, South
ern Methodist University, Dallas, TX, USA, February 1982. 24 pp.


REFERENCES

Wilkins:1641:MSS


Wilkes:1968:TSCa


Wilkes:1968:TSCb


Wilkes:1972:TSC


Wilkes:1975:TSC


Williams:1980:MRP


Williams:1982:CHP


Willett:1983:TKS


Williams:1983:PAP


Williams:1985:SPK

REFERENCES


[Win74b] F. W. (Frederick William) Winterbotham. The Ultra secret: the first account of the most astounding cryptanalysis coup of World War II — how the British broke the German code and read most of the signals between Hitler and his generals throughout the war. Harper & Row, New York, NY, USA,
REFERENCES


Winterbotham:1978:NC

Winternitz:1983:POW

Winternitz:1984:SOH

Winterbotham:1989:US


Wolfe:1943:FCCc


Wolfe:1970:SWC


Wolfe:1983:FCC


Worth:1975:CMA


Wortmann:1987:BRB


Wrixon:1989:CCS


Williams:1979:SRC


Webster:1986:DB

REFERENCES


Yardley:1931:ABC

Yardley:1940:SSA

Yardley:1983:CBC

Yung:1985:SUK

Yu:1989:DEB

Zafiropulo:1963:RAD
Jean Zafiropulo. Le rôle de

Zeidler:1979:DDE


Zim:1948:CSW