Title word cross-reference

(modp) [Pol78], 1/2 + 1 Poly(log N)
ACGS84, $13.95$ [Hig83]. $16.95$
[Ano84a], $19.95$ [HJH85]. $25 \times 10^9$ [PSW80],
2\^m + 1 [BLS75]. 2\^n + 1 [BS67]. 2\^n [QG89].
$34.95$ [Ano82a]. $35.00$ [Lei79a, Lei79b].
$49.95$ [Shu80a, Shu80b]. B [CS83]. D
[Kak85]. F\_q [SX89]. \(1/2 + \frac{1}{\text{poly}(\log N)}\) [CG85].
GF(2\^n) [BMV85]. GF(p) [COS86, PH78].
GF(p^2) [EIG85c]. \(l\) [VGT89]. \(M^3\) [Wil86a].
GF(2\^m) [Mas89]. GF(p^n) [MOVW89]. N
[Kmu87, QG89, VGT89], n = 2 [Lev61a].
NC\^n [Has87]. O(log n) [IW88]. O(log n)
[Bra87a].

-Bit [QG89]. -ciphered [Kmu87]. -tree

[CS83].

0 [ST89]. 0-7248-0274-6 [ST89].

10 [Hel81, Mei81]. 1004 [Mil87b]. 1040
[Lin88]. 1113 [Lin89]. 112 [Hig88b, Nat85a].
113 [Nat85b]. 12 [Bv82]. 121
[Hun85, Wic87]. 1413 [St.93]. 1421 [Lin93].
1474 [Per90]. 1500-1815 [TP63]. 15th
[IEE74], 18 [Riv79]. 1917 [FM76]. 1938
[Shu80a, Shu80b]. 1941 [MB86]. 1942
[Uni79b]. 1943 [Roh75, Roh77]. 1944
[ML87]. 1945 [Uni79b]. 1975 [Ano88e].
[BBB+81]. 1982 [IEE82b]. 1983
[Bur81, Féa83, Had84]. 1984
San86, BC85]. 1985 [Wil86b]. 1986
[ACM86, IEE86a]. 1987
Kno79, Mar76, Wic87]. **Algorithms**
[DS83, Has84, HM83, Knut89b, Knut9a, Knut73, Lak83, QG89, Riv74b, Sh68, She87, AIR83, AG85, Eve98, Gam88, Mor89, ORS+87, PBGV89, Riv74a, SB84, She88].
aios [Hei76]. **Alive** [Ch85a]. **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 [Ano84a, Bam82, Yar40]. American [BBB+81, Bel77, Lew82, Yar31, Yar40]. ammunition [Uni88a]. amplification [BBR88]. Amsterdam [CP87, CP88, Lit87]. Analog [cS85, Kal85, RB88, Die88, Kal84].
alogie [Zaf63]. analogy [Zaf63]. Analyse [SB82]. analyses [Dat85]. Analysis [Ano81a, Ben88, Cal89, Cop89, Gy836, Gy938, HR82, Kal84, Mar76, MM83, RB82, Riv74b, Dem89, Fra89, FF57, Fun78, Her89, JM84, Lag4b, Ma79, Nis89, Wel82b, WW79, SWT+81]. **Analytical**
Anniversary [ML87]. Annotated [Pir83, Lei79a, Lei79b, Shu76]. Annual [ACM89a, ACM89c, IE74, IE79, USE99, ACM82, ACM83, ACM85, ACM86, ACM87, ACM88, IE82a, IE84, IE85, IE86b, IE87a, IE89]. Answering [SDV83].
Antipalindromic [MS87]. any [Ano78b, Dro89, Fak86, GMW87]. aperiendi [Tri06c, Tri21c]. APL [Fra84, Fra85b, Bro86, Vam85, Wor87].
Apparatus [DHM80, Hil31]. apparently [Rou84]. appendix [Bud76]. Application [BCI85, Bis88b, Bis88c, Bis88d, BE79, CP87, CP88, CD85, Gun88b, QV89, Sch83, Yao82b, Bis88a, Fra35c, GT87, LLH89, Lak83, NSS9, Pic86, Rej77, WW84]. **Applications**
[AT&T86, ?, AM85, CG75, GGM85, IE88, Lev61a, RR86, Sie84, Tur41a, Ano78b, BFM88, Fri35a, Fri87, Gol84, Jos85, Kem88, Mei83, NY89b, NY89a, Par85, RF35, Sch84, Sch86, WOo82, Wor75]. **Applied**
[D+83, Mor89, PM78, And79, And80]. approach [GY58, Ho55, Rou84, Sin66, Sin68a, Sin68b, Cam71]. Approaching [PP89]. approximation [Lag84a]. April [ACM83, Bet83, BCI85, CPS, CP88, CM82, Hig88a, Hig88b, Hig88d, IEE80, IEE83, IE87c, Pic86, QV89]. 'Arab [MTA87].
Arabicis [Hei76]. **Arbitrary**
Army [Ano78c]. Arnoldum [Hei76]. Array [VPS88]. Ars [Con39, Tri06c, Tri21c]. arsque [Mer44]. art [Col84, Jos85, Kas63]. Arte [Col64]. Articles [Bur81, Uni42, Ano76, Fri76c]. artificio [Hei76]. Artificial [Nis89]. ASCII [Cam88].
[Smi79c, IM86, Sim79b, Sim82b, Sim82a]. asymptotically [Koo86]. AT&T [AT&T86]. Atkin [Mor88]. Atlantic [Roh75, Uni79b]. Atlantik [Roh75]. atque [Mer44]. attack
[BLO83, BLO84, DO86, GCC88, GC80, Hel81, Hua88, Lag84b, vdAvE86]. Attacks [GMR88, dC86, Hig88e, Odl84]. attributed [FF57, Lea87]. aucta [Sch33]. Auditing
[SK97]. auffzulosen [Sch20]. August [ACM89a, Gle87, USE88b, USE88a, Wil86b, Wal00]. Austria [CSB89, Pic86]. aut
cipher-writing [Hul98]. ciphered [Knu87].

Ciphers
[BD74, EG85b, FF57, HM83, LM85, LP87, PR79, Sie85, Web79, AD81, Alb70, Bar79c, Bar79b, Bos82, CR88a, CE66, D’A39, D’A71, DG57, EE56, Fri35c, Fri56, Gai39, Gai40, Gai43, Gai44, Gai56, Gef73, Hig73, Hig83, Hit43, Laf64, Lew82, Nan36, Nan74, Nor73, Pra39, Shu80a, Shu80b, Wri89].

Ciphertext [RRM78, Sie85].

Cipher-text [RRM78, Sie85]. Circle [BBB +81]. circuits [Wat89].

Citations [Ano88c, Ano88f, Ano88e]. City [ACM87].

Civil [Ano80]. Clandestina [Put27].

Clarissime [Hei76]. Clark [Fil78].

Class [Sie85, Ano39].

Classes [Hit43]. Classic [Fri76b].

Classical [Lau81]. Class-Breaking [ML87].

Class-Breaker [Str89].

Class-breakers [AN86, Gin70, Kah74, Kah67a, Kah67b, Kah69].

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, ADS1, Bar79c, Bar79b, Bla89, EE56, HJH85, Jac87, Kah83, Lew82, MS81, Mor89, Nan36, Nan74, Nor73, Pra39, Shu80a, Shu80b, Sor80, Wel82a, Hig83].

Codewords [BK80].

Cognitata [Mer44]. Cognitive [AWL +88].

Coin [Bhu82, Bhu83a, Bhu84, Sak89].

Coincidence [Fri35a, Fri87]. Collected
Fri41, Fri42, Fri76c, Fri76b, Fri87, Gai39, Gai40, Gai43, Gul83, Gyl36, Gyl38, HS89, Hit43, Ho55a, Kul35, Kul38, Kul67, Kul76, Lev61c, Mil43a, Mil43b, Mil43c, 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].

Cryptanalysis [CR88a].

Cryptic [SD86, WW79].

CRYPTO [BC85, Bra90, Wil86b, CF88, Faï87, O'C81, Wil85, CRS83, CRY81, Ger82, Odl87b, Pom88].

Crypto-ease [O'C81].

Crypto-Functions [Wil85].

Cryptogram [Ano60].

Cryptograms [MM83, Nan36, Nan74].

Cryptographer [Sca86, Wol70].

Cryptographic [Con39, Put27, Col64].

Cryptographic [ARS83, Agn87, Agn88, AT83, BIB89, BCI85, Bry67, CP87, CP88, DLM82, DHH80, Diff2b, EMITT8, Gif81, GJ82, GGM85, Gun88b, Gyl34, Ham71, Hen81, KV89, KMM+80, Lea87, LT85, MTMA85, MM78, QV89, Rittx, San88, Ser85, Sha83a, Sie84, Sni83, Uni88a, Van69, VAYA88, Ano86b, BOCS83, Bla79, Bur88, CF88, Coh87a, D+83, Erd86, FF57, FM76, Gy58, HSF85, HFL+85, Her81, HC88, IN89, Lau81, Lev83, LR86, Mas83, NY89b, NY89a, Odl85, Par85, Pic86, PH78, Sed88, SB84, Uni82a, Uni82b, Wei83].

Cryptographically [BM82, BM84a, KM88, Sha83b, Ayo83, Ste87].

Cryptographic [vN83, S.73, Val92, Bau39, Bau46, Giv25, Giv32, Jos85, LS25, Sac51, dLS02, du 44].

Cryptography [Ame81, Ano76, Ano88c, Ano88b, BBB+81, BP89, BB85, Bet83, BGK77, BE79, Bur84a, Bur84b, CG75, Cop87, CM79, Dav81, DB81, Den82, DH76, Dif88, ECW75, Fei73, Fis84, Fri76c, Gro82, Gud80, GL82, Hel79b, Hil29, Hil31, Hul98, Kon81, LM22, Lan81, Len78, Lev58, Lev61a, Lev61b, Mau4, MM82, Mil86, Mor66, SP89, Sha87, Sha45, SE86, Smi43, Smi44, Smi55, Smi71, Smi83, Tur41a, Wil82a, dRHG+99, AS83, Are21, Are22, BCB88, Bau39, Bau46, BB89, BS82, Bra81, Buc82, Cho86, DK85, Des88, Fri76a, Fri76e, Gag88b, Gal88, Ger82, Giv78, HHL89, Hit43, IL89, vN83, Kil88, Koba87a, Kra86, LS25, LS81, Lec89, Lev61c, MS76, Men39, Mic88, Mil43a, Mil43b, Mil43c, ML67, Nea75, Per85, Pie77, Pri83, Sac36, Sac47, Sac51].

cryptography [Sac77, Sch84, Sch86, SW61, Shu76, Shu82, TP63, Uni42, VS41, Vol41, Wal00, Wei88b, Wei89, Wei87, Wil82b, Wiss2, dLS02, BCKS+83, Col64, du 44, Kon89, Lei79a, Lei79b, Ano82a, ST89].

Cryptography [Hig88b].

Cryptologic [Ale45, Jou88, Sny79, Sny80].

cryptologist [CIA77b, FFW55].

Cryptography [AM85, BC85, Boy86, Bra89b, Bra89a, Cal92, CRS83, CP87, Com87, DKK87, DK+89, Fer87, Kahl66, Kahl79, Kahl84, Kon89, Las85, Len79, LP87, Mar70a, Mar70b, Mei83, Nai89, Por84, QV89, Rug85, She86, She87, She88, Uni79a, Wor75, Bec88, BC85, Boy88, Bra87b, Bra88, Bra90, CP88, Che73, CRY81, D+83, Fra89, Fri56, Fri63, Gal45a, Gal45b, Gal45c, Gal70, Gun88b, Jou88, Kahl63, Kahl82, Kahl83, Oak78, Odi87b, Pat87, Pic86, Pom88, Sie83, Sim88, Sin77, Wil86b, van88, Ano82d, Bau82, Lan46, HJS85].

cryptology [Bec97].
cryptomenytics [Wal00].
cryptoprocessor [MS83].

cryptoprotocols [Yun85a, Per85].

Cryptosystem [CR85, EIG85b, Jun87, WM85, AM88, AM89, AB81, CR88c, DO86, Eck83, EGS85a, EIG85a, GC80, GM85, Gua87, Hel81, Hoo82, HM88, Jun88, Kar89a, Kar89b, Koy82a, Koy82b, Koy83, KM88, Lag84b, LL89, LB88, LM80, Mei81, Nöb88, Odl84, Sal85, SY86a, SY86b, Sal88, SM83, Sha82, Sha84,
Cryptosystems
[Bla85, BR88, Den84a, Koby87b, LP87, Oka88, RSA87, RSA83, Sha85, SSA88, Adl83, Ano88c, Anos88b, AB81, BB79, BLO83, BLO84, Bri86, Bri88, CL88, Dif82a, Gag88a, GS88, IL88, Her78, IM86, JM84, Lag84a, Lak83, LM84, Lid85, Lu79, Lu80, Mer80, Mer82a, MRS87, MRS88, MN81, Mul84, Nie86, Nie88, PR85a, Pop89, RN87, Riv79, RSA82, She87, She88, Sim82a, SX89, Von80a, Wil82c].

CTTE
[MPS02].

Cuckoo
[Sto89].

Curiosa
[Shu82].

Current
[Muf88].

Curve
[IM86, Len87, SX89].

Curzon
[Jef86].

Cyber
[LM84, Lid85, Lu79, Lu80, Mer80, Mer82a, MRS87, MRS88, MN81, Mul84, Nie86, Nie88, PR85a, Pop89, RN87, Riv79, RSA82, She87, She88, Sim82a, SX89, Von80a, Wil82c].

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

D
[Bv82, Hit43, Cop89].

D0L
[SS86, SS87, TC85, TC86, TIF+88, VGT88, Web88, WS79, Yun85b].

Data
[Ano83, Ano88b].

Data-Flow
[Sha88].

Database
[Ano88f, Ano88e, DWK81, GW76, Ano84b, Ano88c].

Datagram
[Tsu89].

David
[Ano88f, Ano88c, DA79, AYO87].

Day
[MB86].

DBMS
[Fal88].

DBS
[IEE86a].

DC
[BBB+81, IEE82b].

Dec.
[Uni79b].

December
[Ano88c, IEE88].

Decipherability
[Ryt86, AG84].

Decipherable
[BK80].

Deciphered
[Ano81a, Rej81, Cla77a, Zor87].

Deciphering
[Knu80, Knu85, Col87].

Decipherment
[Hen81, Beh54, Hen82, Per90, Sau89, Uni79b, Wil86c].

Dee
[Shu82].

Defeat
[Lew82].

Defies
[SS86].

Defined
[BS86].

Definitions
[Kah63].

Degenerate
[Ber09].

Degree
[Has88].

Degrees
[WTE+85].

Deinde
[Hei76].

Demands
[Fak87].

Demonstrating
[CEvdGP87].

Demotic
[Bud76, Bud29].

D’Ecrire
[S.73].

Decryption
[Hen81, Beh54, Hen82, Per90, Sau89, Uni79b, Wil86c].

Defeat
[Lew82].

Defies
[SS86].

Defined
[BS86].

Definitions
[Kah63].

Degenerate
[Ber09].

Degree
[Has88].

Degrees
[WTE+85].

Deinde
[Hei76].

Demands
[Fak87].

Demonstrating
[CEvdGP87].

Demotic
[Bud76, Bud29].

D’encre
[S.73].

Denies
[Ano79].

Denmark
[Bro86, Wor87].

Denning
[Bv82].

Density
[LO85].

Denudata
[Con39].

DEP
[FMP85].

Dependence
[DP85].

Dependency
[O’S88].

Depositions
[GB82].

Depth
[Dat85].

Description
[Riv80].

D’Ecrire
[du 44].

Desiderata
[Hei76].

Design
[Cha86a, Flo83, Gud80, PW86a, PR85a, SRC84, Sha88, Ayo83, Fak87, FLR77, HL88, KD78, KD79, MM82, MPS02, MT86, PR85b, WT86].

Designed
[Bur88].

Designing
Elsevier [Lit87, San86]. elucidation [Wal00]. elusa [Hei76]. Embedding [BCB88, Sha83a]. enc [Ano87a, Ano88b]. emc [Ano87a, Ano88g]. emp [Ano87a, Ano88g]. employed [Col64]. empregados [Col64]. emulates [Ano87a, Ano88g]. emp [Ano87a, Ano88g]. employed [Col64]. empregados [Col64]. emulates [Ano87a, Ano88g]. emp [Ano87a, Ano88g]. employed [Col64]. empregados [Col64]. enunciates [Bar79a, Lea87]. Enciphering [Kno79, KFB79]. Encipherment [BM75, BM76, FH74, Kon85, Bar79a, PR85b, Lin87, Lin88, Lin89]. Encrypted [VPS88, ALN87a, Ano87b, Ano88i, SSDG81]. Encryption [Ano78a, Ano81b, Ano82c, Ano88f, Ayo68b, Ayo84a, Ayo81, BM89, Bec82, Bet88, Bis88a, Bis88b, Bis88c, Bis88d, BG85, Boo81, Bar88, CA81, CA83b, CA83a, sc85, DW81, Den79b, DB89, DH77, EM87, GMP85, Fra85a, Gai77, Gai80a, Gai80b, Gai80c, GM84, Gul83, HS87, Hig87c, Hig88e, Hoo80, IEE86a, Jue81, KJ77, Kak85, Kal85, Kat77, Kem88, KBD89, Kol77, LS89, Ma79, Mar76, MHS1, Mer88, Mit76, Nat77, Nat84, NS87b, PM78, Pca80, Ple75, Ple77, Pon89, PK79, Lin93, SJ76, SB82, SBC85, Sim79c, TT84a, TT84b, Tho86, Uni78a, Uni78b, Uni87, Uni82c, UNN83, UNN85, Uni84, Uni77, Uni81, Uni83, Uni88b, Ame83, AA88, Ano80, Ano84b, Ano85b, Ano87a, Ano88d, Ano88e, Ano88g, APW85, Aya83, Bar87, Ben88, Ber09, Bis88e, Bis89b, BM84b, Cam88]. encryption [CF78, Chr88, Chu89, Dat85, Den84b, Die88, Dre79, Dro89, Eck85, Fak85, Fal88, Gai78, GYS7, Gam88, GM82, Gol87, Hig87b, Hig87e, Hig87d, Hig88a, Hig88f, Hua88, HW88, Int81a, Int79, Int83b, Int84, Int87, Int88, Joh99, Jon86, Kal84, KDT8, KDT79, KMY82, Kem89, Ker89, Knu80, Knu85, KS89, KL84, Kae84, Kic87, MIO82, MI88, Mei85, MP86, Mi85, Mul81, NM88, NS78a, NUS8, NS89, O'C81, OMS8, ORS87, PP88, Pri80, Rao84, Ree79, R88, Roy86, Sae81, Sim79b, Sim82b, Sor80, Sup88, Tex84, Van86, Vou80b, Wab87, Wan86, Wat89, Wel80, Wel82b, Whe87, Wil80, Wil86a, YY89, Zei79, Gab82]. encryptions [RN89]. Encryptor [Cia86]. Encryptors [Mor83]. Encyclopedia [BCS83]. End [SRC84, Ano84b, KYM82, LS89]. End-to-End [SRC84, KYM82, LS89]. enemy [Zor87]. enforcement [JL75]. engendered [Bla89]. Engine [BCKS+83]. Engineering [Ano88c, Ano88f, Ano88g, Sch75]. Engineers [IEE82b]. England [Mur87]. English [Bud76, MS76]. English-jargon [MS76]. Enhanced [Bur85]. Enhancement [Lin93, Lin87, Lin88, Lin89]. ENIAC [WG82]. Enigma [Ano81a, AWL+88, Dea88, WTE+85, Ber83, Hod83, Ale45, Ano86c, Ano87a, Ano88g, Ber73, Ber83, Elv87, Gaj89, Gar79, Gar80, Koz48a, Koz84b, Rej77, Rej81, Rejxx, Tur99, Wel82a]. enigmatic [Wal00]. énigme [Ber73]. Entities [NS88]. Entering [Mor92]. Entropy [EHMS00]. entry [Gai78]. Enumeration [PM78]. Environment [BW85, Bis89a, KS89, Nai89, PW86b, PW87b]. Environments [LS89, Hog88, Kaw87]. Epiphanes [Bud29, Bud76]. Equality [WC81]. Equations [OSS85, Has88, TIF+88]. equidistribution [Koo86]. equipment [Fak87, HFL+85, Int81b, Int84, Ser85, Uni82a, Uni82b, Uni88a, Uni82c, UNN85]. equivalent [Ayo83], equivocation [vTB86]. era [BB89, Men89]. Ernst [Sch20]. eröffnen [Sch20]. Errata [Ano88h]. Erratum [Ayo86b]. Error [Bla83, CC81, Pro85, SB85, Kut85, Mor89, Rao84, vTB86]. Error-Correcting [SB85, Mor89]. Error-correction [CC81, Kut85]. ErycI [Put27]. escrituras [Col64]. Escrow [ON86]. Espionage [Sto89, TP73, Yar83]. essential [IL89]. est [Tri06c, Tri21c]. Established [Ano82d]. estimation [And79, And80]. Etherphone [TS88]. ethics [Hig88e]. Etruscan [Nis89]. etwas [Sch20]. EUROCRYPT
[BCI85, Pic86, CP87, CP88, Gum88b, QV89].

European [BWV+88]. evaluate [Hig87e].

Evaluation [BLO83, BLO84]. evaluations [Cop84]. Even [Mea20]. Event [BBF83].

ever [Hon19]. evidence [FF57]. evolving [DBS99]. ex [Hei76]. examination [Kah63].

Examined [FF57]. Excellence [BCKS+83].

Excerpts [SWT+81]. Exchange [BLS83b, Ted85, Yao86, AS83, Rab81].

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

Exhaustive [DH77, Jue81]. exhibitent [Hei76]. Exhibit [Bur81]. existence [Lu79, Lu80]. Expanded [Nea75].

Expected [Bra87a]. Experimental [BB89].

Experiments [HM83]. Experts [Jur86].

explicitur [Hei76]. exploiting [She86, She87, She88]. Exponentiation [Kak83].

Expose [RS84]. Extended

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

Extensible [Cha85a]. extrapolation [LR88a].

F [Bv82, Cla77a, Cla77b]. F. [SBT85].

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

facsimile [UNN85]. factor [Guy76, Von80a, Von80b]. factored [Bac88].

Factoring [CD85, Len87, Odj87a, PST88, LrW88a, LtW88b]. Factorization [DH85b, Wil85, KLL88, Pol74].

Factorizations [BS67, BLS75, DH85a].

Factors [RM85, CE86]. Failure [CMS89].

Fair [Ted85]. Fail [IE88a, WTE+85].

family [Tex84]. Famous [Bon47]. Far [Str89].

Fast [AM85, Bis88b, Bis88c, Bis88b, Cop84, DDP85, Hen81, Hen82, SM83, AG84, Bis88a, Bis88c, Bis89b, HC88, Odj84].

Fault [BIB89, BGO88, Rab89].

Fault-Tolerant [BIB89, BGO88]. Faults

[CGMA85]. Fear [Hor85].

February [Ano78a, BBB+81, IEE86a, Mur87, Rud82, Uni78a]. feedback [Nie88]. Fellowship [Bur81].

ferne [Sch20]. Feuerstein [Bet83].

Field [Den84b]. Fields

CR85, CR88c, Cop84, Jur86, Lid85, Mas89, Mul81, Odj85].

fifteen [Dif82b]. fifteenth [ACM83]. Fifth

[HW76, SE86]. figures [VA88]. File [Gud80, RW84, Ano88d, Hoo80, Mul81, OM84]. Files

[BM75, BM76, Cam88]. Final [Cha86b].

Financial [AA88]. find [Gor85]. Finerman [Bur81].

Fingerprinting [Wag83]. Finite

[Blu84, CR85, Eck83, CR88e, KV89, Lid85, Mas83, Mas89, Odj85, TC85, TC86].

Finiteness [Bla85].

FIPS [NIS85, Nat85a, Nat85b, Uni83]. First

[ACM89c, Dif88, Foa83, Sed88, USE88b, Ash87, EE56, Had84, Lew78, Win74b, Wol43a, Wol43c, Wol83].

fixed [SP79, Uni82a, Uni82b]. FL [IE88a].

Flaw [Dem88]. Flip [Rub79]. Flip-Flops [Rub79].

Flipping [Blu82, Blu83a, Sak89]. Flips

[Bls84]. Flips [Rub79]. Florence [CM82].

Florida [IE88]. flow [BR88, Sha88].

Flowers [WG82]. forecast [Dif82b].

Forlag [Br86]. form [Dav79, Wal100]. formal

[KYM82, Kem89]. formulae [KV89].

Forum [MC75]. Foundations

[IEE79, IEE82a, IEE84, IEE85, IEE86b, IEE87a, IEE89, Eck82].

Founding [Kil88].

Four [Eve98, Bow59]. fourteenth [ACM82].

Fourth [IEE88, Rud82].

Fraction [Por52].

fracturing [Fri41]. Fragmentation

[Tsl89]. framework [Per85]. Framingham

[Ker75]. France [BC85].

Francisco [ACM82, Rud82].

Franksen

[BCKS+83, Bro86, SBT85, Vam85].

französischen [Kas63]. free [PBGV89].

freedom [Sie83].

French [Pau39, Bau46, Kas63, vN83, LS25, Per90, Sac51, Zaf63, dS02, du 44].

Friedman

[Claz7a, Cla77b]. Führungsprobleme

[Roh75].

Function

[IW81, Mer88, Win83, Win84]. Functional

[SS89]. Functions

[ACGS88, GGM85, GGM86, MRW89, QG89, Sie84, WC81, Wil85, Yao82b, BM89, GL89, IL89, Lev85, LR88b, NY89b, NY89a].

Fundamental [Knu73]. Funds
Further [RF35].

Futrelle [BCKS⁺³].

G [Ano82a, WG82]. G. [BCKS⁺³].

Gaithersburg [Ano78a, Uni78a].

Galland [BCKS⁺³].

Galois [Mul81].

Game [BCKS⁺³].

Gardner [AWL⁺³].

Garnett [Kas63].

Geheime [Sch20, Sch33].

Geheimschriften [Kas63].

Geheizet [BGK77].

Geleitzugschlachten [Roh75].

General [GMT45, Sid81, EKMN84, ISN87, NBWH78].

Generals [Bra87a, LSP82, Rei85, Win74b].

Generate [BM82, BM84a, Yao86, Bac88].

generated [Bar84, Plu82].

generating [Er89].

Generation [MM78, Sha83b, SE86, VV85, RT88, SD86, Vin71, Vin72].

Generators [Boy89b, CG75, Gun88a, Plu83, Gab82, Lev85, LR86, Ste87].

genere [Con39].

geometry [Mil85].

George [Ric74, Shu82].

German [AWL⁺³, Elv87, Lec89, WTE⁺³, Ale45, Bau82, Cha86b, Eck82, Gab82, Gaj89, Kas63, Koz84a, Koz84b, Rei90, Roh75, Uni79b, Win74b].

Germanica [Con39].

Germany [Bet83, Zor87].

gewis [Sch20].

Girls [CN87].

Girolamo [Shu82].

Global [IEEE78, San86].

GLOBECOM [IEEE78].

glossary [SW61].

GMD [Bur81].

Godfather [Ran82a].

goes [Kah79, Lew78, Per88].

gold [Sau89].

Goldstine [Ano81a, SWT⁺³].

Goldwater [Mor88].

Goldwasser-Killian-Atkin [Mor88].

good [AD81, Dro89, Lu79, Lu80, Vou80b].

Gordon [DG57].

Government [Hi88a, Den86, Fer87, Jef86].

Governmental [Dav81].

Graeca [Con39].

Graecis [Hei76].

grand [Kah82].

grand [Ber73].

graph [NM88].

greater [Lu79, Lu80].

Greek [Bra79, Dav79, Lag84b, Sha82, Sha84, Tuc79a, Tuc79b].

Hemel [ST89].

Hierarchical [LS89].

heterogeneous [PW86b, PW87b].

heuristic [Gul83].

Hides [BG85, LW88].

Hiding [MH78].

Hemlock [ST89].

Henry [Ric74].

Herleste [Riv79].
key [Wic87, Wil82b, WS79, Wil80, Wil86a, vTB86]. Key-Lock-Pair [Cha86a]. keyed [Ayo68b, Ayo68a, Ayo81]. keyless [AS83, Yun85b]. Keys [Blu83b, EHMS00, MTMA85, MM78, MS87, Ber09, Bla79, Bv82, CS83, DS81, DMS81, Hig87d, HM88, NM88, Sea86]. Killian [Mor88]. kind [Gar77]. kinds [SX89].


latter [Gyl38]. lattice [VGT88, VGT89]. Law [CM82]. Lawrence [Ano88d].


Logarithms [BM85, EI85b, Mas83, Cop84, COS86, EG85a, ElG85a, ElG85c, Odl85, Odl87a, Ph87]. Logic [BAN89b, CM82, HR82, BAN9a, Kar89a, Le80].


Low-Density [LO85]. low-order [Boy89a]. LPC [S87].

LSI [FMP85, FMC85]. Lu [GC80]. Lu-Lee [GC80]. luck [Bra81]. Lukoff [BKS83].

Luneburg [Wal00].


machinery [Dem88, AW88]. Machines [Ano88a, AWL88a, Bur81, Pl98, WTE85a, DK89, AWL888, WTE85]. Macmillan
Fri76a, Fri76e, Hit43, Men89, Zor87, vN83.

Millikin [Hit43]. Million [Ran55, Ran01].
millions [Gar77]. Mind [AWL*88]. mini
[Ano78b]. mini- [Ano78b]. Minister
[MB86]. Minneapolis [IEE81]. Minnesota
[IEE81]. Mirror [Cl212]. missing [Boy89a].

Model [LHM84, Gyl36]. Models
[CMS89, D*83, MPS02]. Modern
[Ano86a, Bra88, Kah66, SE86, Bia75,
Bra87b, Com87, DK85, Lee89]. moderne
[Lee89]. Modes [CA83a, Nat80, Ame83].
modification [Wil80]. Modular
[Mon85, PR85b, Has88]. modules
[She86, She87, She88]. modulo
[Kak83, Per85, VGT89]. modulus [PP89].

monoalphabetic [Fri35b]. monograph
[Lea87]. Monte [FHJ*84, Pol78].
Monterey [USE99]. Monthly
[Mul89b]. morphisms [Kar89b, SY86a, SY86b]. MOS
[Uni82a, Uni82b]. Most [Jon78b, Ano84a,
Bam82, Jur86, Wal00, Win74b]. movable
[Gyl38]. MPJ [Joh89]. MPQS
[LtW88a, LtW88b]. MPQS-factoring
[LtW88a, LtW88b]. MR [Bv82, Lu80,
Mul89b, Riv79, BCKS*83, SBT85]. Mr.
[Fra84, Fra85b, Fra86, Bro86, Van85, 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, RBO89]. Multiple
[MH81, Sil87, Gyl38, Hei81, LM80, Mei81].
Multiplication
[Mei85, Mon85, Mas89, PP89].
multiplication-permutation [Mei85].
multiplicative [Odl84, Rec79]. Multipliers
[VP888]. multiply [BLO83, BLO84].
Multisignature [Oka88]. Mummy [Pro80].
Museum [Bud29, Bud76, Bur81, WTE*85].
must [Dro89]. mutual [OR87]. Mycenaean
[Zaf63]. mycénienne [Zaf63]. mysteries
[Sea86].

N [SWT*81]. nahe [Sch20]. name
[BO85a, BO85b, Lea87]. name-stamp
[BO85a, BO85b]. National
[Ano78a, DH85b, MZS79, Uni78a, Sie83,
Van87, BGK77, Bro81, Kol77, Mar76].
nature [MS76]. natürliche [Sch20, Sch33].
Naval [Ale45]. navigandi [Mer44].
Navigation [Mur87]. Navy [Mac87]. Nazi
[Win78]. NBS
[Ano81b, DH77]. Gai77, Gai80c, Gai81, Uni81].
NC [IEE89]. Neal [Kon89]. NEC
[LtW88a, LtW88b]. necromantica [Hei76].
negeri [Saw55]. nemine [Hei76]. Nero
[Sto65]. Netherlands [CP87, CP88].

Network [Den79a, KBN88, NS88, SN88,
VK83, Bur88, Dut85, KD78, Tho74].

Networks
[IEE81, Kar85, Mul88, NS88, PW86a,
PW87a, PK79, Ayo83, CV89, KD79, Kar86,
Mei85, NS88a, NBWH87, Wan86, We82b].

Neumann [Ano88i]. Nevada [ACM89b].

Newbold [Sar28]. News
[Ano82d, Bur81, Hig88a, Kol77]. nihil
[Hei76]. nine [Wal00]. nineteenth
[ACM87]. Niv [Ano88i]. NJ [Hig83].
No [Cha66b, Bv82, Hig88a, Ker89, Lu80,
Mul89b, RM85, Tuc79a, Tuc79b].
nominatus [Hei76]. Non
[BIB89, BFM88, Chu89, Dav81, Fed87, Bar75].

Non-Cryptographic [BIB89].

Non-Governmental [Dav81].

Non-homomorphic [Chu89].

Non-Interactive [Fed87, BFM88].
on-pattern [Bar75]. Noncryptographic
[BOG88, Maw98].

Nonlinear
[Sie84, TIF*88, Web88]. nonrandomness
[KLL88]. Nonsingular [PM87]. Norbert
[AWL*88]. Normal
[Ran55, Ran01, MOV89]. Normandy
[Beu80]. Norris [AWL*88]. Norse
[ML67].
North [Had84]. North-Holland [Had84].

Notation [BCKS*83]. Note
[BD74, Lam81, Lam73, Wei88a, Wic87,
Bv82, CM85, Lei80, Mei81, Mul84]. Notes

Notes


PC [Bec97, Dea87]. Peapolitani [Hei76].
Pearl [Far67, Far69]. Pegawai [Saw55].
Pennings [AWL+88], perfectly [Por84].
Performance [Lag84b, Beh54, Lom83].
Period [BE79, Bar79b]. Permutation
[AM85, LM84, KDT8, KDT9, LR86, Mei85].
Permutations [IR98, Ayo86b, Ayo86a,
Ayo81, Ayo83, LR88b, Rej77].
perniciosa [Hei76]. Personal [Ano87d,
Den79a, EHM00, Ste98, Boy86, Win69].
Peter [Hig88b]. Peters [BCKS+83]. PGP
[Saw55]. phaenomena [Nat84, UNN83, Uni84].
[Mer44]. Philippum [Tri06b, Tri21b]. Physica [Mer44].
Physica-Mathematica [Mer44]. physical
[AT83, BCKS+83, BC85, CP87, EKMN84,
Proceedings ACM89b, ACM89c, BC85, CP87, EKMN84,
BLS75, Mil76, Pol74]. prime
[KP89, Per85, MB86]. Primer
[Gro82, Kon81, Ano82a]. Primes
[BD74, Gor85, HW88]. primo [Hei76].
Principem [Tri06b, Tri21b]. Principles
[ACM89a, Jev74, Fri35c, GS87, Hu98, RF35].
Printers [Sch83]. Printing [Ver26].
Prisoner [Sim83]. Privacy [BRR88, Dre79,
Fei73, IEE80, IEE83, IEE87c, Lin87, Lin88,
Lin89, Lin93, Uni87, Pie77, Wil83b].
Private [RN87, RN89, Mi85, Ste89].
Private-key [RN87, RN89, Mi85]. pro
[Hei76]. Probabilistic [BG85, GM82,
GM84, Gol84, CG88, Lei80, MRS87, MRS88].
Probability [Tur41a, Gle57, GP85, Gle86,
KP89, vTB86]. Probable [McC75, KP89].
Probable-Word-Proof [McC75]. Problem
[AT83, BCKS+83, Cal89, CN87, GMR85,
LSP82, Lam73, Mau14, Ryt86, Sim83,
WM85, Bar79a, Com87, Gal78, GY58,
Joa87, Rei85, Tho74, Vou80b, Wil83b].
Problems [BS86, Bhu82, Bhu83a, BOS85d,
CG87, LO85, Eve85, FS87, Fri76b, Jur86,
MP86, Roh75, Rou84, Sus81, Wil82c].
procédés [S.73]. Procedure
[Bin85, Pur74, Wil80]. Procedures
[Lin93, Bau82, Lin87, Lin88, Lin89, Uni88a].
Proceedings
[ACM82, ACM83, ACM85, ACM87, ACM89a,
ACM89b, ACM89c, BC85, CP87, EKMN84,
Gle87, HW76, IEE80, IEE82b, IEE83, IEE87c, Ker75, QV89, RR86, San86, USE88b, USE88c, USE88a, USE89b, USE89a, Ano78a, Ano87a, Ano88g, Bet83, BCI85, CRS83, CP88, CSB89, CRY81, Fˆea83, Gun88b, Had84, Mor89, Odl87b, Pic86, Pom88, Uni78a, Wil86b, ACM86, ACM88, AWL+88, Bra90].

Process [Bv82, Hel81, Mei81].

Processing [ALN87a, Ano88i, Ben88].

Processor [FMP85, Sed88, Bar87].

Produced [Boy89b, Plu83, Boy89a].

Producing [Win83].

product [Ano78b].

products [Ano89].

program [Ben88].

Programming [Pel60, SWT+81, Boy86, Ste88, War82, BCKS+83].

Programowa [Kos83].

Programs [FH74, KMM+80, Dea87].

Progressions [BD74].

Project [Mu88, Bla75].

promissa [Hei76].

Proof [BM84b, GMR89, McC75, Fit89].

Proofs [BOKW88].

Propagation [Pro85].

properties [Chu89].

property [Ale98].

proposal [Rou84].

Proposed [McC75].

propositional [Kar89a].

Prospective [Ano88h, AWL+88, WTE+85].

protect [Gef73].

Protecting [EHMS00].

Protection [Cha86a, Coh87b, HRU76, HP87, Hug88, Sal73, Weil88a, Ale98, Ano86b, BPS2, Ber80, CF87, CF88, Coh87a, SB84, Uni87, Wiel80, vdAV86].

protein [Gy85b].

Protocol [BFF83, Bh82, Bhu83a, Bra87a, St.93, V84, EGL85, Mil87b, Sak89].

Protocols [CCD88, CMS89, DM83, FM85, GMW87, Mer80, Mer82a, Sid81, V83, Yoa82a, BO85a, BO85b, BO85c, Cam87, DLM82, D8+83, Eve85, Kem89, RO89].

Prototype [SBC85, BB89].

Provable [IR89].

provable [NS87].

prove [FS87].

proven [Lea87].

Prover [BOKW88].

provided [Gy85b].

Providence [ACM85].

provides [Uni87].

Proving [FLR77].

Pseudo [AM85, BM82, BM84a, Boy89b, FHI+84, Gab82, LR86, Plu83, VV85, Mit76].

Pseudo-Inversen [Gab82].

Pseudo-Random [BM82, BM84a, Boy89b, Plu83, VV85, FHI+84, LR86, Mit76].

pseudoinverses [Gab82].

pseudonym [Ano60].

pseudonyms [Cha79, Cha81].

Pseudoprimes [PSW80].

Pseudorandom [Por84, Sha83b, KM88, Lev85, LR88b, RT88].

Ptolemy [Bud29, Bud76].

PUB [Nat85a, Nat85b, Uni83, NIS85].

Public [BG85, Boo81, Bur84a, Bur84b, CR85, Den84a, Di88, EG85b, ECW75, G884, Hel79b, HP87, Kvic87, LP87, MI88, Oka88, RSA78, RSA83, SBC85, Smi83, WM85, Wil85, Yun5a, AM88, AM89, Adl83, Bar87, BBR88, BB89, BM48b, BS83, Buc82, Cho86, CR88c, DDO85, Dif82a, EG85a, EL85a, Fra89, Gag88a, GC80, GM85, GS88, Gu87, HHL89, HL88, Her78, Her81, Hoo82, HW88, Kah79, Kar89b, KL84, Koy82b, Koy83, Lag84a, Lak83, LB88, Mer80, Mer82a, Mer82b, MN81, Mul84, Ndb88, ORS+87, PR85a, Ric74, Riv79, RSA82, Roy86, Sal85, SY86a, SY86b, Sal88, SM83, Ses81, SS86, SSA87, TC85, TC86, TIF+88, Web88, Wil82b, WS79, Wil80, Wil86a, Ame81, BBB+81, DB81].

Public-Key [BG85, Den84a, Di88, GS84, Hel79b, Oka88, RSA83, WM85, Wil85, ECW75, LP87, AM88, AM89, Bar87, EG85a, GC80, GS88, Gu87, HHL89, Her78, Hoo82, Kar89b, KL84, Koy82b, Koy83, LB88, MN81, Mul84, Ndb88, ORS+87, Riv79, Sal85, SY86a, SY86b, Sal88, TIF+88, WS79, Wil80, Wil86a].

publication [Uni83, Wei83].

Publications [Lan46, Oak78, Pri83].

Publishers [Lit87].

Publishing [HJH85, Had84, Lei79a, Lei79b, San86].

Puerto [IEE79].

Pugh [WTE+85].

Purple [Cla77a, Cla77b, Fil77, Fil87].

Putani [Put27].

puzzle [Ano84a, Bam82].

puzzles [CM85, Kak84].

Quadratic [Sil87, MI88, PST88].

qua [Con39, Hei76].

quaesquer [Col64].

quality [Dem88].

Quantum [BB85, Wie87, BB89].
Quasi [BE79]. Quasi-Random [BE79]. que [Col64]. Queries [BWV+88, SDV83]. quest [Fit89]. quocunque [Con39]. quodam [Hei76].


radar [Her89]. Radio [Ano22, BCKS+83, Ver26, Cam87, Hol87, Uni79b]. Ralph [Shu80a, Shu80b]. Ramp [BM85]. Random [Agn87, Agn88, AM85, BM75, BM76, BM82, BM84a, Boy89b, BE79, FMC85, FO89, GGM85, GGM86, Plu83, Ran55, Ran01, BM84a, Boy89b, BE79, FMC85, FO89, GGM85, GGM86, Plu83, Ran55, Ran01, Tip27, VV85, Ayo68b, Ayo68a, Ayo81, Bac88, BM89, Cam88, FHJ+84, Gab82, KP89, Koo86, LR86, Mil76, NM88, NU88, Por84, Vin71, Vin72]. Randomized [Bra87a, RS83, EGL85]. randomness [CG88]. Rang [Sto65]. rates [Lu79, Lu80].


Recursiveness [BCKS+83]. Red [Sch20, Sch33]. Rédei [Nöb84, Nöb85]. Rédei-scheme [Nöb84, Nöb85]. Reden [Sch20]. reduced [CE86]. reducing [Hig88b, VGT88, VGT89]. reduction [NM88].

Redundancy [PT89, Hig88b, Lu79, Lu80]. Reed [MS81]. Reference [Lei79a, Lei79b, Kus63, MS76].

Reflections [SiI83, Tho84, Tho87, Her89]. regarding [AM88, AM89]. Register [Gol67, Gol82, Bar84, Nie88]. règles [Per90].


Repetitions [Tur41b]. Report [Ame81, AWL+88, BBB+81, BGK77, DB81, GMT45, WG82, Ano84a, Bamb82, BS83, Ger82, Uni78b]. reports [Uni78b]. reprove [Bet88]. Request [Bur81]. Requirements [FH74, Ano85b, Nat84, Uni82c, UNN83, UNN85, Uni84]. Requiring [EKW74].

Research [Dav81, IEE89, Bla75, Jou88]. reserata [Hei76]. resource [Ano88]. Reste [Lec89]. Restraints [Dav81]. Results [BO88, BS87, CM79, Kais85, Mu88, DH85a, JM84, Per85]. Retail [BW85]. Retrieval [CM79, KBD89, Riv74b, Riv74a].

Retrofitting [RB82]. Retrospect [WG82]. return [Cha79, Cha81]. revealed [Col64].

Revealing [SDV83, CEvdGP87]. revelada [Col64]. reversal [YY89]. Review [Ano82a, Ano84a, Ano88a, Bro86, Fil78, Gin70, HJH85, Hig83, Lei79a, Lei79b, Lit87, Ma79, Man86, Sar85, ST89, Shu80a, Shu80b, Vam85, Wad85, Had84]. Reviews [AWL+88, BCKS+83, Cam71, Kon89, Lan46, SWT+81, SBET85, SE86, WTE+85, Ano81a, Ano88b]. revisited [NS87]. Revolution [AWL+88]. rewriting [Sal85]. RFC [MiI87b, Lin87, Lin88, Lin89, Lin93, St.84, St.85, ST.93, Tho74]. rfi [Ano87a, Ano88g].


roots [Per85, VGT89]. Rosetta [Bud22, Bud29, Bud76]. rotating [Dem88].

Rotation [sC85]. rotations [Er89]. Round
S [BCKS+83, Lan46, Mul89b, Gul83, WT86]. S-box [Gul83]. S-boxes [WT86]. S. [WTE+85]. Saer [MS76]. safe [Ano88d, Koc89]. Safeguarding [Bla79, Cha85a]. safety [Ano89]. Sage [AWL+88]. sampling [Tip27]. Sampson [MS76]. San [ACM82, IEE79, Rud82, Bud76]. Sandia [DH85b]. Satellite [Eck85, MP86, Ano82c]. satisfying [FHK+88]. Saved [Fil77]. SB [Ano79]. SC122 [Roh77]. Scale [AWL+88, She88]. Scheme [BG85, EMMT78, ElG85b, EKW74, Fel87, GMR88, Has84, IW81, Kal85, Kot85, LS89, Oka88, Pon89, SS84, AIR83, Sch20, Sch86]. Seeds [MS76, MS78, Sha84, Sch83, Sha87, Sim82a, IE84, IE85, IE86b, IE87a, IE89, Jev74, Lit87, San86, Gai80a, Sch84, Sch86, Sha87, Smi43, Smi44, Smi55, Smi71]. Scientific [Jon78a, Jon78b, Sie83]. Scientists [Kon89, Pat87]. Scrambling [KJ77, Ano82c]. Script [Sea56, Zaf63]. scripta [Con39]. scripti [Put27]. scripturam [Tri06c, Tri21c]. sea [Bee81]. seal [Far67, Far69]. Sealing [GJ82, Gif81]. Search [BM75, BM76, BCKS+83, Jeu81, Gul83, Sha86, Sie83]. Seattle [ACM89c]. Seberry [ST89]. Sec’83 [Fˆea83, Had84]. Sec’84 [San86]. Second [San86, SBET85, HT79, HH79]. secondary [Fri35c, NBWH78, RF35]. Secrecy [EKW74, Mer82b, Sha49, Gif81]. Secret [Ano22, Blu83b, Cha85a, Cha85b, CGMA85, Cla12, Dro89, EHM500, Fel87, Gin70, Has84, Hig89, Hon19, ISN87, Nan36, Nan74, Nor73, Pie77, Pra39, Ric74, Sea86, Sea56, Sha79, Ste87, TP63, Ver26, Wil41, Win69, Wol70, Yar40, Yun58a, Ano84a, Ano88a, Bam82, Bro86, Cal80, Fra84, Fra85b, Fra86, GM82, Hig88c, Hig88d, Jac87, Jon78b, Kah67a, Kah76b, Kah96, Ker89, Lai64, Lan81, Lew78, MS76, Mic88, NU88, Per90, RBO89, Smi43, Smi44, Smi55, Smi71, Ste76, Vam85, Win74a, Win74b, Win75, Wor87, Wri89, Zim48, Zor87, du 44, Kas63, SBET85]. secret-key [NU88]. Secretdisk [Hig88f]. secr`ete [S.73]. secr`etement [du 44]. secr`etes [Per90]. Secrets [HJH85, MM87, SV83, Sed85, Yao86, Hig88a, Kah38, MS81, Rab81]. Section [Den79b, Sim88]. sector [Ano80]. secundum [Hei76]. Sécuré [ACGS84, BW85, BP85, Bir85, CCD88, CM79, Den79a, GMR88, Gud80, LS89, Mer78, PK79, Sim82a, VV85, Win84, Yao82a, CG85, Hig87d, Hoo82, IN89, KM88, Lan89, MM82, Mit89, Pie77, Sha86, Ste87, Yun85b, KBN88]. Security [ADDS91, AM88, AM89, Ano78c, Ber80, BM85, BGK77, Bro81, Cha85c, DM83, F€a83, GJ82, IE80, IE83, IE87c, IE88, Ko177, Lan89, LHM48, Len78, Lit87, MH81, Mul88,
Pfl89, Pur74, Rab89, RW84, San86, Sat89, Sch83, SS89, Sum84, USE88b, USE88a, VK83, VK84, Ano78a, Ano82c, Ano84b, Ano89, Bec97, BOCS83, BCW86, Bin9a, BO85a, BO85b, Bos82, BS82, Cho86, D+83, Den82, Dre79, Dro89, Eve85, Ful88, FLR77, Fis84, GS78, Gon89, HS85, Had84, Hlg88, Hoo80, JL75, Kak83, KYM82, Ker89, Koc89, LB88, MM82, MRS87, MRS88, Mit76, Nat84, Nai89, Pri83, Rou84, Sch75, SP89, Ser85, Sie83, Sil83, Sin85, Ste89, Uni78a, Uni82c, UNN83, UNN85, Uni84, Uni81, Van87, dC87, Ano79, Fˆea83, Had84, Hig83, ST89]. Security-related [AM88, AM89].

solutions [Com83, FS87, Tuc79a, Tuc79b, VV86]. solver [Fri76b]. solves [Rou84]. Solving [Blu82, Blu83a, Has88, LO85, MP86, Rejxx, TIF+88]. solvuntur [Hei76]. Some [BS86, BS67, Gag88b, GS78, HC88, JM84, Lev81a, Lev61b, Lev61c, MN81, Nie88, WS79, Wil85, dC87, DO86, Eck82, Eve85, FF57, Her78, Hog88, KLL88, Koo86, Riv79, dC86]. sonderlichen [Sch20]. Sons [Ano82a]. sophisticated [Hor85]. Sorting [DG57]. Sound [Hon19]. Source [Blu84, Wil82c]. Sources [Agn87, Agn88, CG88]. South [RR86]. Space [Ryt86]. Spanheimensis [Hei76, Tri21b, Tri06b]. spawned [Hor85]. Speaks [Bur81]. Special [Den79b, DB81, Gai88b, GS78, HC88, JM84, Lev81a, Lev61b, Lev61c, MN81, Nie88, WS79, Wil85, dC87, DO86, Eck82, Eve85, FF57, Her78, Hog88, KLL88, Koo86, Riv79, dC86]. specifically [S.73]. specialist [HFL+85]. specialties [Jur86]. Specification [SS89]. Spectral [Chr78, Gul83]. Spectroscope [Ano22]. spectrum [Kah84]. Speech [KJ77, SJ76, BP85, Hol87]. Speed [Lev61a, Sed88, Ano87b, PP89]. Sphere [SBET85]. Spirit [Hau74]. spectrum [Kah84]. spread [Kah84]. spring [Rud82]. Spy [Sto89, Win89]. spying [Hor85]. square [Bow59, Per85]. staff [Uni78b]. stamp [BO85a, BO85b]. Standard [Ano78a, Ano81b, Ano88, Bis88b, Bis88d, Bur88, CA81, CA83b, CA83a, Kat77, Nat77, Nat85a, Nat85b, SB82, Uni78a, Ano88e, Bar87, Bet88, Hig87b, Ame83, Ano78a, Bee82, Bis88a, Bis88c, DH77, EMM778, Fra85a, Gai77, Gai80a, Gai80b, Gai80c, Gul83, Jue81, Ma79, Nat84, Uni78a, Uni78b, Uni87, Uni82c, UNN83, UNN85, Uni84, Uni77, Uni81, Uni83, Uni88b]. Standardization [Kra84]. Standards [Ano78a, BGK77, Mar76, Uni78a, BS82]. Stars [Rus27]. State [Blu84, Sha87]. States [Shu80a, Shu80b, Sin77, Bar79c, Bar79b, Lev83, Web79]. Statistical [Kul35, Kul38, Kul67, Kul76, de 53]. statistically [Sor80]. Statistics [Tur41b, FO89]. status [BS83]. Steganographia [Tri06c, Tri21c, Sch20, Sch33, Hei76, Wal00]. Steganographiae [Tri21b, Tri06b]. steganographica [Hei76]. steganographicos [Tri06a, Tri21a]. Steganologia [Sch20, Sch33]. stelae [Bud76]. Step [Gun88a]. Stockholm [Fea83]. Stokes [BCKS+83]. Stone [Bud22, Bud29, Bud76]. Stones [Hau74]. Storage [CM79, Ano87b]. storage/backup [Ano87b]. Stored [TS88]. stories [Bon47, Fut73]. Storing [KBD89]. Story [Sin77, Ritxx, Far67, Far69, Kah67a, Kah67b, Kah96, Pra39, Wel82a, BCKS+83]. Strandberg [Wor87]. Strandbergs [Bro86]. strategy [Ben89, HT79, HH79]. Stream [Rub79, Sie85, Bar84]. Strong [BM82, BM84a, Gor85, Sha83b]. Structure [MS87, Wil83a]. Structured [KD79, KD78, War82]. structures [ISN87]. studies [Uni79a]. Study [Ame81, BBB+81, DB81, Bue82, Cou86, Gai39, Gai40, Gai43, Gai44, Gai56, Lju81, Per85, Sie83]. subcategory [Uni81]. subexponential-time [Adl79, ELG5c]. subkey [Wel80, Wel82b]. Subkeys [DK81]. Subliminal [Sim83, Sim85b, Hol87]. Subscription [Yun85a]. subsequences [Koo86]. Subset [LO85, IN89]. Substitution [HM83, Lev58, PR79, Bar75, Bow59, Fri35b,Fri35c, KCD78, KCD79, Ljul81, Mil76]. substitution-permutation [KCD78, KCD79]. substitutions [SY86a, SY86b]. subtle [du 44]. suitable [du 44]. Subtractive [Mor83]. sui [Tri06c, Tri21c]. Suitable [Dav85]. Sum [LO85, IN89]. summary [Uni78b]. summe [Hei76]. Summer [Bur81, Ass88, USE89b, USE89a]. sunt [Con39]. Supercomputing [ACM89b, Bis89a]. Superincreasing [Wil83a]. Support
supposititia [Hei76]. surveillance [Uni88a].
Survey
[BO88, Cha86b, Tho86, PVL86, Pop89].
Sweden [Fae83]. Swedish [Gyl31].
Survey [BO88, Cha86b, Tho86, PV86, Pic86, RS83, Wil86c].
technologies [DB89]. Technology
[Ano87d, AWL88, Gra82].
Telecommunications [IEE87b, Uni87].
Telecryptograph [Gua04].
Telegraph [Ver26].
Telegraphic [Ver26].
Telecommunications
[IEE87b, Uni87].
Telegraph [Ver26].
Telegraphing [Gua04].
telematics [GL82].
Telephone
[Blu82, Blu83a, Gua04, Hon19, NBWH78].
telematics [Wab87].
Telephoning [Mea20].
Teletrust [Rih87].
televising [Poll88].
telegraph [Ver26].
teletypewriter [GUA04].
teletypewriting [Gua04].
teletypewriter [FVTS87].
televisions [Eck85].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
telephones [Wab87].
Thomas [Sea56]. Thompson [SBET85].
Thousands [Fil77]. threat [Ano88a].
Three [Per85, Pon89, WTE+85].
Threshold [Cha85a, Kot85, LHL89].
throughout [Win74b]. Thwarting [Hor85].
tilings [Gab82]. Till [Gyl31]. Time
[CMS89, FH74, QSA88, Wil68a, Wil68b, Wil72, Wil75, AIR83, Bra81, ElG85c, Hig88a, Sha82, Sha84, Wal00, YY89].
time-luck [Wil82, Wil72, Wil75, AIR83, Bra81, ElG85c, Hig88a, Sha82, Sha84, Wal00, YY89].

Till [Gyl31]. Time-sharing
[Wil68a, Wil68b, Wil72, Wil75]. timely
[OR87]. Times [Hig88d, NBWH78]. tips
[MP86]. tissue [Fun78]. titles [Sin77]. TLP
[BE79]. TMS7500 [Tex84]. TMS75C00
[Tex84]. today [DKKM87, Fak86]. tokens
[Spe87]. Tokyo [IEE87b]. Tolerance
[Rab89]. Tolerant [BIB89, BOGW88].
tomorrow [DKKM87]. tool [Mic88].

Toolbox [Sca86]. Tools
[Die88, Ano86a, DB89]. Top
[Cal80, Hig88c, Hig88d, Zor87]. top-secret
[Zor87]. Topic [Mar70b, Mar70a]. Tore
[Riv79]. Toronto [IEE86b, San86]. totally
[Hel79a]. Tracking [Sto89]. tract [Sim04].
Tractatus [Mer44]. tradecut [Bra81].
traduzir [Col64]. Traffic
[Cal89, Hol87, Uni79b, Wel82b]. trails
[Cam87]. Trainer [Uni82b]. Traité
[LS25, dS02]. Trans [Lu80]. transaction
[Cha85c, ADDS91]. Transactional [O’N86].
transcendental [KLL88]. Transfer [BW85, Ano85b, Gra82, Kem88, Kil88, Rab81].
Transformation [Hill31, NM88].
transformations [YY89]. transformed
[MO182]. Transition [Len79]. translating
[Col64]. translations [Bud76].
transmission [Ano88d]. transparent
[Hig88f]. Transport [VK84].
Transposition [Fri41, Bar61, Con86]. Trap
[IW81, MHT78]. Trap-Door [IW81].
Trapdoor [Wil83a, Yao82b, GM85, SM83].
trapdoor-knapsack [SM83]. Trapdoors
[Sha83a]. TRASEX [Van87]. Trattati
[Alb70]. Treatise
[LS81, Tur99, LS25, dS02]. Treatises
[Alb70]. Treaty [Sim79a, Sim84]. tree
[CS83, San88]. Trees
[BM75, BM76, Er89, FJH+84]. trend
[Nai89]. tres [du 44]. tres-subtile [du 44].
Trial [Mon85]. Triangle [IEE89]. trifid
[Bow60b]. Triple [Cla12]. triplex
[Tri06a, Tri12a]. Trithemii [Hei76, Hei76].
Trithemij [Tri06a, Tri06b, Tri21a, Tri21b].
Trithemio [Hei76]. Trithemius
[Shu82, Wal00]. Trojan [Kar87]. Troubled
[Lit87]. truly [Vin71, Vin72]. truncated
[FHK+88, HS85]. Trust [Tho84, Tho87].
Trusted [MM87, SK97, CBC88]. Trusting
[Tho84, Tho87]. Trustworthy
[Sim79a, Sim84]. Tsarist [AN86]. tube
[Zor87]. Tubes [BCS+83]. Tunny
[GMT45]. tuples [MI88]. Turing
[Ash87, AWL+88, Hod83, Tur99]. tutorial
[Bra88, Wil82b]. TV [MP86]. TVROs
[MP86]. twentieth [ACM88]. Twenty
[ACM89c, Ash87, Rud82]. twenty-fourth
[Rud82]. Two
[BR80, Cho86, Fra89, SX89, TC86, AB81, BO85c, Cop84, Sha86, Sha87, AWL+88, BWV+88, Koz84a, Koz84b, WTE+85].
two-part [Sha86, Sha87]. two-party
[BO85c]. TX [USE88c]. Type
[CR85, Cho86, CR88c, Gyl38, Nie86].

U [Beh54]. U-boat [Beh54]. U.S.
[Gr82, Sny79]. ubi [Hei76]. ue [Hei76].
ultimate [Wil86c]. ultra
[Cal80, Mul89a, Bel77, Ben80, Ben89, Lew78, Wel86, Win74a, Win74b, Win75, Win89].
ultrasound [Fun78]. unabridged [Kah63].
Unbiased [Bla84, CG88]. Unclassified
[Uni78]. Unconditionally [CCD88].
Undergraduate [Ano82d]. Uniform
[Lie81]. Unique
[LR88a, Ryt86, AG84, VV86]. Uniquely
[BK80]. United
[ST89, Uni78b, Bar79a, Bar79b, Lev83, Sin77, Web79, Shu80a, Shu80b]. Universal
[NY89b, NY89a, Shu82, SP79, Lom83].

**University** [IEE74, Man60, RR86, Gra82].

**UNIX** [AT&T86, ?, Bis89a, RW84, USE88a].

**Unknown** [NS88]. Untraceable

[Cha79, Cha81, Cha83b]. Untrusted [NS88].

**Update** [BB85, DH85b]. upgrading

[MP86]. Upon [Gua04, MS76, YY89].

**urgent** [Pra39].

USA [IEE88, Ker75, USE88b, USE88c, USE89b, USE99].

**Usage** [Nat85a, S.73].

**Use** [IW81, Smi83, Sor80, WC81, Hit43, KS89, Nat84, UNN83, UNN85, Uni84, Wel80, Wel82b]. used

[Bar79a, Ben88, FF57, SX89].

**useful** [Yun85b].

Usenix [USE99].

**User** [EKW74, Has84, PW86a, PW87a, ALN87b, Ano84b, Ano86a, CF88, O’S88, OM84, Tex84].

user-controlled [OM84].

users [Ano88j, Smi87, Spe87].

Uses [Ano22, Edw15, Mi86, Ano80]. Using

[BBF83, Bir85, Boo81, CM79, KJ77, NS87a, NS78b, PR79, QG89, SK97, SBC85, Sio85, Wan86, AS83, Ano81b, Ano87c, Ayo83, Bar75, BM89, CF78, DG57, Dre79, Er89, HS87, HHL89, HW88, Kak85, Kem89, Koy82a, Mui81, NS89, Oka88, PR85a, PP89, Uni82c, Uni81, Von80b]. ut [Hei76]. utility

[Sup88].

V [Bud29, Bud76, Bra79].

**vacuum** [Zor87].

**vacuum-tube** [Zor87].

**Validating** [Gai77, Gai80c]. Validation [Has84].

**valuable** [Un87].

**Value** [MM83, Evc98].

value-adding [Evc98]. Values [BCKS+83].

**Variable** [Lev58]. variables

[FHK88, HS85].

**Variants** [SS84].

**variations** [Ano87a, Ano88g, dC87].

**varieties** [TC86].

**V¨arldskriget** [Gyl31].

**Vehicle** [Mur87]. verbis [Hei76].

verborgene [Sch20]. verborgens [Sch20].

Verfahren [Bau82]. verifiability [BO85c].

**Verifiable** [CGMA85, Fel87, RBO89].

**verification**

[KYM82, Kem89, MI88, Sii83, WCG86].

**verified** [SSDG81]. Verify [Sim79a, Sim84].

Verifying [ALN87b].

Verschl¨usselungsabbildungen [Gab82].

version [SS85]. versions [CM82]. versus [Dif82a, Fäk86]. verwandt [SB82].

Very [Ker75, She88, du 44]. via [Cam87].

Vienna [EKMN84]. view [Bel77, Gy138]. viewpoint

[Gr82, Gy136].

VIII [Ric74, HJH85, Hg83]. vindicata [Hei76]. vindicias [Hei76].

viruses [Ano88a]. Visible [Hon19]. VLSI

[Mas89, ORS87, She86, She87, She88, Wat89].

vnd [Sch20]. vne [du 44]. vnnd

[Sch20, Sch33].

**value** [Hg138].

vocabulary [MS76].

**Voice** [BCW86, TS88, Wab87, Int79, Int81b, Int84, Int87, Int88].

**Vol** [Lei79a, Lei79b].

voluntatem [Tri06c, Tri21c]. vs

[Jue81].

vulnerable [Hg138].

V.

[SE86, WTE85].

wa [MTA87].

wa-istikhraj [MTA87]. Wagstaff [Mul89].

**War** [AWL88, Bar79c, Cla77a, Elv87, Jon78a, Koz84a, Koz84b, Men89, WTE85, Win74b, Bee81, Ber83, Gar79, Gar80, Jon78b, Lew78, Ste76, Uni79b, Gy131, Gy134, HT79, HH79, BET85].

**warfare** [Men89, Nor73].

Wars [Bar79b, Den86].

Was [AWL88, Koz84b, WTE85, Koz84a].

**Washington** [ACM89c, BBB81, IEE82b].

**watch** [Ano87d].

**Watermark** [BCKS+83].

**Watermark-based** [LB89a, LB89b].

**Watermarks** [Est80].

**Waveform** [KJ77].

**Waves** [Hon19].

**Way** [IR89, IW81, Kno79, KFB79, Win83, Win84, GL89, Hä87, IL89, Lev85, NY89b, NY89a, Sha88].

**Wayne** [Kon89].

**Wayner** [Hig88b].

**weak** [CG88, HC88].

weaken [Gra82].

**weaknesses** [She86, She87, She88].

**weapon** [Bel77].

Web [Aale89].

Webber [Shu80a, Shu80b].

**Webster** [Kah63].

Wednesday [IEE86a, Mur87].

**Weiss** [Ano88].

**Welchman** [BCKS+83].

West [Sin77, Ben80].

**Wexelblat** [SWT81].

**WGs** [CSB89].

**whatever** [Col64].

**wheels** [Gy138].
where [Bar79a], wherein [Lea87, Wal00]. Which [BG85, AB81, Rou84]. Whitehall [Fer87]. Who [Fil78, Cla77a, Cla77b]. Whole [ACGS88], wholesale [AA88]. whose [Hor85]. Whitehall [Fer87]. Who [Fil78, Cla77a, Cla77b]. Whole [ACGS88]. within [Hel79a]. Without [Mon85, PW86a, PW87a, Bla85, Cha85c, CevdGP87, SDV83, Wil83a], wits [See89]. Wizard [Jon78a]. Wolfe [Sto65], woln [Sch20]. World [BS86, BO85d, McC75, WM85, Bar75, Ben88, Eve85, Smi87]. WordPerfect [Ben88]. words [AG85]. Work [Goo79]. working [BB89]. Works [AWL+88]. Workshop [Bet83, BC85, BGK77, CP87, CP88, Gun88b, QV89, USE88b, USE88a, Pic86]. Workstations [NS88]. World [AWL+88, HT79, HH79, Ritxx, SBET85, WTE+85, Cla77b, Ale98, Bar79c, Bar79b, Cla77a, Elv87, Gyl31, Gyl34, Koz84a, Koz84b, Lew78, Lit87, Men89, Win74b]. worldwide [Int87, Int88]. Worthy [AWL+88]. would [Gar77]. Writing [Gel74, Hu98, Kah67a, Kah67b, Kah96, Kas63, Lef64, Nan86, Nan74, Ric74, Sea86, Smi43, Smi44, Smi55, Smi71, Wol70, Zim48, du 44, Gu70], writings [Col64, Lan81, Per90], wrong [HM88]. wrote [FF57]. WW [Ph98]. Wyner [Kal84, Kal85].

X.509 [Cop89]. X3 [ML87]. X9.23 [AA88]. xiv [Ano82a], xvi [Lei79a, Lei79b]. xviii [Shu80a, Shu80b].

year [Dif82b, Hel79a]. Years [BCKS+83, Dif88, Ash87, Gar77]. Yeheskel [Ano88i]. yesterday [DKK87]. York [ACM87, Ano82a, HJH85, Hig88d, Lei79a, Lei79b, MZ879, Sin77]. York/London [Lei79a, Lei79b]. yourself [FS87].


References


REFERENCES

LCCN QA 76 S979 1984. IEEE catalog no. 84CH2085-9.


REFERENCES


ACM:1989:PSN


ACM:1989:PTF


Ahlswede:1981:BCG


Abraham:1991:TSS

Adleman:1979:SAD


Adleman:1983:BGK


Adleman:1987:PRD


Apostolico:1984:PMM


Apostolico:1985:CAW

REFERENCES


Agnew:1987:RSC


Agnew:1988:RSC


Akritas:1983:CEA


Ahituv:1987:PED


Ahituv:1987:VAI


Alexander:1945:CHG


Alexandre:1998:JBP

REFERENCES

Akl:1985:FPR

[AM85]

Adams:1988:SRC

[AM88]

Adams:1989:SRC

[AM89]

ACE:1981:RPC

[ACE:1981:RPC]

ANSI:1983:ANS

[ANSI:1983:ANS]

Andrew:1986:TCB

[Andrew:1986:TCB]

Andree:1952:C


Anonymous:1978:ODA


Anonymous:1979:SSA


Anonymous:1980:ACS


Anonymous:1981:CHP


Anonymous:1981:GIU


Anonymous:1982:BRCa


Anonymous:1982:CC

REFERENCES

Anonymous, 1982. 1 sound cassette (75 min.).

Anonymous:1982:NNPa


Anonymous:1984:BRP


Anonymous:1984:ESC


Anonymous:1985:BM


Anonymous:1985:DEA


Anonymous:1986:MTT

Anonymous:1986:CPC


Anonymous:1986:RE


Anonymous:1987:EVE


Anonymous:1987:HSE


Anonymous:1987:MAU


Anonymous:1987:TWP


Anonymous:1988:BRCb


Anonymous:1988:CCJc

Anonymous:1988:CCJb


Anonymous:1988:DEK


Anonymous:1988:DESb


Anonymous:1988:EVE


Anonymous:1988:ERH


Anonymous:1988:PED

Anonymous. Processing encrypted data: Niv Ahituv,

Anonymous:1988:RIA


Anonymous:1989:SZS


Aruliah:1985:PIE


Arensberg:1922:CSP


Adleman:1983:CCS


Alpern:1983:KEU


Ashenhurst:1987:ATA

REFERENCES

USENIX:1988:CSSb


Akl:1983:CSP


ATT:1986:AUS


Aspray:1988:RCD


Ayoub:1968:EKR

REFERENCES

Ayoub:1968:EEK

Ayoub:1981:EKR

Ayoub:1983:DCE

Bach:1988:HGF

Bamford:1982:PPR

Burrows:1989:LAab

Burrows:1989:LAa

Barker:1961:CSC

Barker:1975:CSS


REFERENCES


Baum:1981:RPC


Bauer:1983:KDP


Bennett:1988:PAP


Blakley:1985:ACP


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.

Barker:1988:ECT

catalog number 88CH2629-5. IEEE Computer Society order number 895.


REFERENCES

Bennett:1989:UMS

Bertrand:1973:EOP

Berstis:1980:SPD

Bertrand:1983:EGE

Bergmann:2009:DKR
Seth D. Bergmann. Degenerate keys for RSA encryption.


Beth:1983:CPW

Betts:1988:ESG

Blum:1988:NIZ
REFERENCES

Blum:1985:EPP

Branstad:1977:RWC

Bar-Ilan:1989:NFC

Birrell:1985:SCU

Bishop:1988:AFDa

Bishop:1988:AFDb

Bishop:1988:AFDc
REFERENCES

Summer 1988. CODEN CM-SYE2. ISSN 0895-6340.


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.

Blanchard:1989:CSS


Brickell:1983:EAA


Brickell:1984:EAA


Brillhart:1975:NPC


Blum:1982:CFT


Blum:1983:CFT


Blum:1983:HES


Blum:1984:IUC

REFERENCES

(paperback), 0-8186-4591-1 (microfiche). ISSN 0272-5428.
LCCN QA 76 S979 1984. IEEE catalog no. 84CH2085-9.


by the International Association for Cryptologic Research.


REFERENCES


REFERENCES


REFERENCES

Blakley:1988:CBA


Branstad:1979:VHD


Brassard:1981:TLT


Brach:1987:ERR


Brassard:1987:IMC


Brassard:1988:MCT


Brassard:1989:CCb


Brassard:1989:CCa

Brassard:1990:ACC


Conference held Aug. 20–24, 1989 at the University of California, Santa Barbara.

Brickell:1985:BIK


Brickell:1986:CKC


Brickell:1988:CKC


Brown:1975:BL


Brownell:1981:ODN

the United States, George A. Brownell, chairman.

Brooke:1986:BRB


Brickell:1983:SRK


Benois:1986:CSE


Bateman:1989:NMC

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 MERSENNE 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.

Buck:1982:PCS

R. Creighton Buck. The public cryptography study group.
REFERENCES


Budge:1922:RS


Budge:1929:RSB


Budge:1976:RSB


Burchard:1981:NNF


Burton:1984:RPKa


Burton:1984:RPKb

Burton:1985:EAC

Burnham:1988:DES

Brouwer:1982:NMK

Beker:1985:KMS

Buchholz:1988:CQDc

CBEMA:1981:ANS
Computer and Business Equipment Manufacturers Association and American National Standards Institute. American National Standard Data En-


[Cam88] William Ervin Cammack. Methods of data encryption and a


REFERENCES

Coppersmith:1975:GCA

Chor:1985:RRL

Cover:1987:OPC

Chor:1988:UBS

Chor:1985:VSS

Chaum:1979:UEM
David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Thesis (M.S. in Computer Science), University of California, Berkeley, Berkeley, CA, USA, June 1979.

Chaum:1981:UEM
D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the Association for Computing Machinery*,
REFERENCES

Chandler:1983:IMC


Chaum:1983:BSU


Chaum:1985:HKS


Chaum:1985:NSC


Chaum:1985:SIT

REFERENCES


REFERENCES


REFERENCES


REFERENCES

9448 (print), 1557-9654 (electronic).


REFERENCES


Carroll:1988:ACP


Carroll:1988:CC


Carroll:1988:KTP


Chaum:1983:ACP


Crypto:1981:ACP


Cesarini:1983:ACC

Chaum:1989:SCF


Chaum:1988:ACP

REFERENCES


REFERENCES

Dawson:1985:COL


Denning:1981:SRR


Denning:1989:EET


de Jonge:1986:ASR


de Jonge:1987:SVR

REFERENCES

Davio:1985:EHS

DeVries:1953:SMC

Deavours:1987:CPI

Deavours:1988:BPS

Demirdogen:1988:FDM
REFERENCES


[Dif82b] Whitfield Diffie. Cryptographic
REFERENCES


**Diffie:1988:FTY**


**Deavours:1985:MCM**


**Deavours:1989:CMH**


**Deavours:1987:CYT**


**DeMillo:1982:CP**


**DelaStelle:1902:TCF**


**DeMillo:1983:PDS**


**Denning:1981:MMK**

REFERENCES

Desmedt:1986:CTA


Desmedt:1985:DOI


Dreher:1979:PSC


deRaadt:1999:COO


Dror:1989:SCG


Denning:1981:MKG

REFERENCES


<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Title</th>
<th>Journal/Book Details</th>
</tr>
</thead>
</table>


Erdem:1986:HCO

Estell:1980:BW

Even:1985:CSW

Even:1998:FVA

Faak:1986:SVH

Faak:1987:CMM

Falk:1988:DST

Farago:1967:BSS
REFERENCES

Farago:1969:BSS

Feak:1983:SIS

Feistel:1973:CCP

Feldman:1987:PSN

Ferris:1987:WBC

Feynman:1982:SPC

Friedman:1957:SCE

Friedman:1955:CLS

Friedman:1974:ETR
Theodore D. Friedman and Lance J. Hoffman. Execution time requirements for encryption programs. Communications of the Association for Computing Machinery, 17
REFERENCES


REFERENCES

[FM76] William F. (William Frederick) Friedman and Charles Jas- 

trow Mendelsohn. *The Zimmermann telegram of January 16, 1917, and its cy- 

ptographic background*. A Cryptographic series. Aegean Park Press, 


[FM85] Steven Fortune and Michael Merritt. *Poker protocols*. In 

Blakley and Chaum [BC85], pages 454–464. CODEN 

LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302- 

9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 


springerlink.com/openurl. 

asp?genre=article&issn=?? 

??&volume=0&issue=0&spage= 203. CRYPTO 84: a Work- 

shop on the Theory and Application of Cryptographic Tech- 

niques, held at the University of California, Santa Barbara, 

August 19–22, 1984, sponsored by the International Association 

for Cryptologic Research.

[FMP85] R. C. Fairfield, A. Matuse- 

vich, and J. Plany. *An LSI Digital Encryption Processor 

(DEP)*. In Blakley and Chaum [BC85], pages 115–143. CODEN 

LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302- 

9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 


springerlink.com/openurl. 

asp?genre=article&issn=?? 

??&volume=0&issue=0&spage= 115. CRYPTO 84: a Work- 

shop on the Theory and Application of Cryptographic Tech- 

niques, held at the University of California, Santa Barbara, 

August 19–22, 1984, sponsored by the International Association 

for Cryptologic Research.

[BC85], pages 203–230. CODEN 

LNCSD9. ISBN 0-387-15658- 

5; 3-540-39568-7. ISSN 0302- 

9743 (print), 1611-3349 (elec- 

tronic). LCCN QA76.9.A25 


no.196. URL http://www. 

springerlink.com/openurl. 

asp?genre=article&issn=?? 

??&volume=0&issue=0&spage= 203. CRYPTO 84: a Work- 

shop on the Theory and Application of Cryptographic Tech- 

niques, held at the University of California, Santa Barbara, 

August 19–22, 1984, sponsored by the International Association 

for Cryptologic Research.
REFERENCES

Flajolet:1989:RMS


Foster:1982:CM


Franksen:1984:MBS


Franklin:1985:MID


Frankel:1989:TIC


Friedman:1935:ICA


Friedman:1935:MCP

REFERENCES


REFERENCES


REFERENCES


Gabriel:1982:VPI


Gabriel:1982:VPI

Gaglione:1988:ITP


Gaglione:1988:ITP

Gaglione:1988:SCT


Gaglione:1988:SCT

Gaines:1940:ECS


Gaines:1940:ECS

Gaines:1943:ECS


Gaines:1943:ECS

Gaines:1944:CSC


Gaines:1944:CSC

Gaines:1956:CSC

REFERENCES


REFERENCES

**Galland:1970:HAB**

**Galil:1988:SIC**

**Gamble:1988:IDL**

**Gardner:1977:MGN**

**Garlinski:1979:IEW**

**Garlinski:1980:EW**

**Gilmour-Bryson:1982:CDT**
A. Gilmour-Bryson. Coding of the depositions of the Templars. In Ciampi and Martino [CM82], pages 451–467. ISBN 0-444-86413-X (set), 0-444-86414-8 (vol. 1), 0-444-86415-6 (vol. 2). LCCN K662.I4 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.”.


REFERENCES

springerlink.com/openurl.asp?genre=article&issn=??
??&volume=0&issue=0&spage=276. 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.

Goldreich:1986:HCR


Gifford:1981:CSI


Gingerich:1970:BRB


Girling:1987:CCL


Givierge:1925:CC


Givierge:1932:CC


Givierge:1978:CC


Garey:1979:CIG

REFERENCES


REFERENCES

Goldwasser:1982:PEH


Goldwasser:1984:PE


Goodman:1985:NTK


Goldwasser:1985:PPS


Goldreich:1987:HPM


Goldwasser:1988:DSS


Goldwasser:1989:KCI


Good:1945:GRT

References


Gray:1982:ICT


Grover:1982:CP


Grundler:1984:DEH


Grollmann:1984:CMP


Grollmann:1988:CMP


Guarini:1904:MTT


Guan:1987:CAP

Gudes:1980:DCB


Gullichsen:1983:BHS


Gunther:1988:ASG


Gunther:1988:ACE


Guy:1976:HFN

R. K. Guy. How to factor a number. In Hartnell and Williams [HW76], pages 49–89.

Griffiths:1976:AMR


Gamow:1958:CAP

George Gamow and Martynas Ycas. The cryptographic approach to the problem of pro-
tein synthesis. In Das Universum. Unser Bild vom Weltall. (German) [The Universe. Our picture of the Universe], page ???. Wiesbaden, Germany, 1958.

Galil:1987:PEA


Gylden:1931:CEI

Yves Gyldén. Chifferbyråernas insatser i världskriget till lands. (Swedish) [Cipher bureaus’ operations in the World War on land]. Stockholm, Sweden, 1931.

Gylden:1933:CCB


Gylden:1936:AMC


Gylden:1938:APV

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.

Haddon:1984:BRS


Hammer:1971:SSC


Hamming:1980:CIT


Hamming:1986:CIT

R. W. (Richard Wesley) Hamming. Coding and informa-
REFERENCES


REFERENCES

Wormatiense, Moguntiae. Sumptibus Joannis Petri Zubrodt, 1676. 8 + 394 (or 396) + 4 pp. LCCN Z103.T84 1676. Includes Heidel’s life of Trithemius and his vindication of the Steganographia.

Hellman:1979:WTI


Hellman:1979:MPK


Hellman:1981:ACA


Henry:1979:WTI


Henry:1982:FDA


Herlestam:1978:CRS


Hershey:1981:DLP

J. E. (John E.) Hershey. The discrete logarithm public cryptographic system. NTIA report 81-81, PB82-130097, U.S. Dept. of Commerce, National
REFERENCES

Telecommunications and Information Administration, Washington, DC, USA (??), September 1981. iv + 40 pp.


[Hoornaert:1985:EHI]
REFERENCES

0-340-12493-8. 180 (est.) pp. LCCN ????


REFERENCES


CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic).


CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic).


REFERENCES

(3):135–154, March 1931. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Hitt:1943:MSM


HJH:1985:BRK


He:1988:SDK


Hunter:1983:ERA


Hule:1988:RCW


Hodges:1983:ATE


Hoffer:1955:MAC


Hogan:1988:PIS


Hollis:1987:TCA

J. B. Hollis. A technique for communicating AVL traffic by subliminal data signalling over a speech radio channel. In Muraszko [Mur87], pages 13/1–
REFERENCES


REFERENCES


REFERENCES


REFERENCES


IEEE:1982:CFP


IEEE:1983:PSS


IEEE:1984:ASF


IEEE:1985:FOC


IEEE:1986:CEC


IEEE:1986:ASF


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

Imai:1986:AMC

Impagliazzo:1989:ECS

Impagliazzo:1989:LPC

IRD:1981:DVE

IRD:1984:DVE

IRD:1987:DVE

IRD:1988:DVE
REFERENCES


Ito:1987:SSS


Ingemarsson:1981:UAS


Jackson:1987:NTS


Jeffery:1986:GCC


Jevons:1874:PS


Jones:1975:ESP


Jurgensen:1984:SRI


Johnson:1989:BDC


Jones:1978:WWB


Jones:1978:MSW

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


REFERENCES

Kahn:1967:CSSa  

Kahn:1967:CSSb  

Kahn:1974:C  

Kahn:1979:CGP  

Kahn:1982:GLC  

Kahn:1983:KCS  

Kahn:1984:COS  

Kahn:1996:CSS  

Kak:1983:EMP  

Kak:1984:MPK  
REFERENCES


REFERENCES

[113]

DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

[Kari:1989:OCP]


[Kas63]

Friedrich Wilhelm Kasiski. Die Geheimschriften und die Dechiffirunkunst, Mit besonderer Berücksichtigung der deutschen und französischen Sprache. (German) [Secret writing and the art of deciphering, with special reference to the German and French languages]. E. S. Mittler und Sohn, Berlin, Germany, 1863. viii + 95 + 4 pp. LCCN ????

[Katzan:1977:SDE]


[Kawai:1987:LAI]


[Klein:1989:STR]


[Karp:1988:SDN]


[Kam:1978:SDS]


[Kam:1979:SDS]

REFERENCES


Kemp:1988:EEF


Kemmerer:1989:AEP


Kerr:1975:PIC


Kerr:1989:SNM


Knoble:1979:EOW


Kilian:1988:FCO


Kak:1977:SEU


Kothari:1984:CMW

REFERENCES

0898-1221 (print), 1873-7668 (electronic).


<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
</table>
REFERENCES

by the International Association for Cryptologic Research.

**Konheim:1989:RMC**


**Koopman:1986:OES**


**Koscielny:1983:PRD**


**Kothari:1985:GLT**


**Koyama:1982:CUM**


**Koyama:1982:MKR**

[Koy82b] Kenji Koyama. A master key
for the RSA public-key cryptosystem. *Systems-Comput.-

Koyama:1983:MKR


Kozaczuk:1984:EHGa


Kozaczuk:1984:EHGb


Kim:1989:PRP


Krause:1984:DEI


Kranakis:1986:PC


Kordes:1989:UMC

REFERENCES

Kuchlin:1987:PKE


Kullback:1935:SMC


Kullback:1938:SMC


Kullback:1967:SMC


Kullback:1976:SMC


Kears:1989:CLL


Kasami:1982:KMS


Laffin:1964:CCS


Lagarias:1984:KPK


Lagarias:1984:PAS

J. C. Lagarias. Performance analysis of Shamir’s attack on


[Las85] Teresa A. Lassek. Cryptology and the computer age. Thesis (Honors), University of Nebraska at Omaha, Omaha, NE, USA, 1985. 58 pp.

REFERENCES


Lee:1988:OSM


Lee:1989:WBL


Lee:1989:WLB


Leary:1987:CSM


Leclerc:1989:CRM


Leighton:1979:BRA


Leighton:1979:BRB


Leiss:1980:NSS

E. Leiss. A note on a signature system based on probabilis-

**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

//www.acm.org/pubs/citations/proceedings/stoc/22145/p363-levin/. ACM order no. 508850.  [Liev81]

Lewin:1978:UGW


Lewin:1982:AMC


Landwehr:1984:SMM


Lidl:1985:CBP


Lieberherr:1981:UCD


RFC0989


RFC1040

REFERENCES


REFERENCES


Lagarias:1988:UEP


Luby:1988:HCP


Lange:1925:TC


Lange:1981:TC


Lu:1989:SCI


Lamport:1982:BGP


They proved that Byzantine agreement cannot be reached unless fewer than one-third of the processes are faulty. This result assumes that authentication, i.e., the crypting of messages to make them unforgeable, is not used. With unforgeable messages, they show that the problem is solvable for any \( n \geq t > 0 \), where \( n \) is the total number of processes and \( t \) is the number of faulty processes.

Leung:1985:SCT


Lu:1980:AEG

Lu:1979:EGC

Ma:1979:RAD

Meijer:1981:DSS
MacPherson:1987:CUN

Mandelbrot:1960:BRJa

Marsh:1970:MEC

Marion:1976:ANB

Massey:1983:LFC

Mastrovito:1989:VDM

Matyas:1979:DSO
REFERENCES

Mauborgne:1914:APC


Milner-Barry:1986:ADL


McCarthy:1975:AFP


McIvor:1985:SC


Meijer:1981:NCM


McIvor:1920:KCE


Meijer:1983:CCC

[Mei83] Henk Meijer. Cryptology computational complexity and applications. Thesis (Ph.D.), Queen’s University, Ottawa, ON, Canada, 1983. 2 microfiches (179 fr.).

Meijer:1985:MEN


Menelsohn:1939:CC

REFERENCES

ography of . . . cryptology, 1945, p. 124.

[Mendelsohn:1989:CWI]

[Mersenne:1644:CPM]
Marin Mersenne. Cogitata Physica-Mathematica . . . [Tractatus de mensuris ponderibus atque nummis . . . Hydraulica pneumatica; arsque navigandi. Harmonia theoretica, 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 massive distributed computing efforts through the Great Internet Mersenne Primes Search (GIMPS) project. The largest of these is \( M(13466917) \), a number containing 4,053,946 digits.

[Merkle:1978:SCI]

[Merkle:1980:PPK]

[Merkle:1982:PPK]
REFERENCES

Merkle:1982:SAP


Merkle:1988:DSB


Merkle:1989:CDS


Merkle:1978:HIS


Matsumoto:1988:PQP


Michener:1988:TSK


Millikin:1943:ECCa

REFERENCES


James Melvin Mitchell. Encryption algorithm for data security based on a polyalphabetic substitution scheme and...


Muller:1981:SRP


Muller:1986:CDS


Muller:1986:CDS


Matsumoto:1982:DTL


Morrice:1692:EB


Morrison:1983:SEA


Morain:1988:IGP

REFERENCES

[Mora:1989:AAA]

[Mullin:1988:ONB]

[Mevis:1986:SCP]

[Mori:2002:CSD]

[Micali:1987:NSP]

[Micali:1988:NSP]


[Macalister:1976:SLI]
Robert Alexander Stewart Macalister and John Sampson. *The secret languages of Ireland: Ogham, Hisperic, Bearlagair na Saer, Bog-Latin, and*


REFERENCES

Marayati:1987:AWA

Mackinnon:1985:OAA

Mulherin:1981:FDE

Mullin:1984:NMP

Mulligan:1989:UMA

Mullin:1989:LEN
"$M_n(= 2^n - 1)$ is the product of two distinct primes only if $n$ is either a prime $p$ or the square of a prime $q$, in which case precisely one prime factor of $M_n$ is Mersenne, viz. $M_q$."


REFERENCES


REFERENCES

Nemetz:1988:RLS


Naor:1989:UOW


Naor:1989:UOH


Oakley:1978:RPC


O’Connell:1981:CDE


Odlyzko:1984:CAM


Odlyzko:1985:DLF

REFERENCES


Conference held at the University of California, Santa Barbara, Aug. 11–15, 1986.


REFERENCES
REFERENCES

Pearcey:1980:EDS

Pelta:1960:SP

Perret:1890:RCS

Peralta:1985:TRN

Perry:1988:EBG

Pfleeger:1989:SC

Pohlig:1978:IAC

Pichler:1986:ACE
Franz Pichler, editor. Advances in cryptology: Eurocrypt 85: proceedings of a workshop on the theory and application of
REFERENCES


W. H. Payne and K. L. McMillen. Orderly enumeration
REFERENCES


REFERENCES

Posch:1989:AEA


Peleg:1979:BSC


Pieprzyk:1985:DPK


Pieprzyk:1985:MDI


Pronzini:1980:MCC

Bill Pronzini. *Mummy!: a chrestomathy of crypt-ology*.


REFERENCES

DEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).


REFERENCES


 REFERENCES


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

A. Deavours and I. J. Good. This article was entitled “Jak matematycy polscy rozszyfrowały 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].

Rejewski:19xx:EMH


Rowlett:1935:FAP


Richards:1974:SWP

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.
REFERENCES

Rivest:1979:CRC

Rivest:1980:DSC

Rivest:1985:RCP

Rivest:1987:EDR

Reeds:1985:NPR

Rao:1987:PKA
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

ogy, Laboratory for Computer Science, Cambridge, MA, USA, 1983. 20 pp. [RSA83]

Rivest:1984:HEE


Rivest:1978:MOD


Rivest:1982:MOD


Rivest:1983:MOD


Reif:1988:EPP


Raleigh:1988:CDP


Rubin:1979:DSC

REFERENCES


<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Publication Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ravinderpal S. Sandhu</td>
<td>Cryptographic implementation of a</td>
<td></td>
</tr>
</tbody>
</table>

*Sarton:1928:BRBn*


*Satinanarayan:1989:ISL*


*Saunders:1989:IDE*


*Sawirudin:1955:PND*


*Schaumuller-Bichl:1982:ADE*


*Sorkin:1984:MCC*


*Serpell:1985:PES*

REFERENCES

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.

Smillie:1985:RFM


Chen:1985:RGE


Scacchitti:1986:CT


Schwenter:1620:SSN


Schwenter:1633:SSA

[Sch33] Daniel Schwenter. Steganologia & [i.e. et] steganographia aucta: geheime, magische, natürliche
REFERENCES


Schroeder:1969:IC


Schroeder:1975:ESK


Schell:1983:SPA


Schroeder:1984:NTS


Schroeder:1986:NTS


Smith:1986:GCC


Sicherman:1983:AQR

REFERENCES

161


**Smillie:1986:RWA**


**Sedlak:1988:RCP**


**Seeley:1989:PCG**

REFERENCES

Serpell:1985:CES


Seshadri:1981:KPP


Shannon:1945:MTC


Shannon:1948:MTCa

Claude Shannon. A mathematical theory of communication. The Bell System Technical Journal, 27(3):379–423, July 1948. CODEN BSTJAN. ISSN 0005-8580. From the first page: “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

Adi Shamir. A polynomial time algorithm for breaking the basic Merkle–Hellman cryptosystem. In 23rd annual symposium
REFERENCES


Shamir:1983:ECT

Shamir:1983:GCS

Shamir:1984:PTA

Shamir:1985:IBC

Shamir:1986:SPS

Shamir:1987:CSS

Sharp:1988:DCO

Sherman:1986:CVT
Alan T. Sherman. Cryptology and VLSI (a two-part disserta-
REFERENCES


Sherman:1987:CVT

Sherman:1988:CVV


Shulman:1980:BRB


Shulman:1980:BRU


Shumaker:1982:RCJ

Wayne Shumaker. Renaissance curiosas: John Dee’s conversations with angels, Girolamo Cardano’s horoscope of Christ, Johannes Trithemius and cryptography, George Dalgarno’s Universal language, volume 8 of Medieval and Renaissance texts

[Si81]

[Si83]
Sidhu:1981:APG

[Si84]

[Sie84]
Sieminski:1983:SBB

[Si85]

[Sie85]
Siegenthaler:1984:CIN

[Sie79a]

[Sim79]
Siegenthaler:1985:DCS

[Sim79a]

[Sim79b]
Silverman:1987:MPQ

[Sim83]

[Sim04]
Silverman:1983:RVS

[Sim04]
Cicco Simonetta. [Little tract on cryptanalysis]. ????-????, 1404. ???? pp.

[Sim97]
Simonetta:1404:LTC

[Sim79]

[Sim79b]
Simmons:1979:HID

[Sim79]
Gustavus J. Simmons. Computational complexity and asym-


Simmons:1979:SAE


Simmons:1982:SCA


Simmons:1982:SAE


Simmons:1983:PPS


Simmons:1984:HID


Simmons:1985:ATC

[Sim85b] Gustavus J. Simmons. The subliminal channel and digital signatures. In Beth et al.
REFERENCES


Simmons:1988:SSC


Sinkov:1966:ECM


Sinkov:1968:ECMa


Sinkov:1968:ECMb


Singh:1985:IPS


Sambur:1976:SEM


Schneier:1997:RAS

REFERENCES

html; http://www.elsevier.com/gej-ng/10/19/19/28/17/17/abstract.html.


[Smi71] Samuel S. Snyder. Influence of U.S. Cryptologic Organizations
REFERENCES


REFERENCES

Shepherd:1989:CSS


Subramanian:1987:DTP


Siromoney:1988:CPL


Smith:1981:VEP


StJohns:1984:RAS


StJohns:1985:RAS


Shawe-Taylor:1989:BRB

REFERENCES


StJohns:1993:RIP


Stark:1970:INT


Stark:1978:INT


Stevenson:1976:MCI


Stern:1987:SLC


Stevens:1988:CPR


Stephenson:1989:PPM


Stout:1965:DRN


Stoll:1989:CET

REFERENCES


Salomaa:1986:PKC


Tao:1985:FAP


Tao:1986:TVF


Tedrick:1985:FES


Tao:1986:TVF


Thomas:1974:RPS


Thomas:1984:RTT

REFERENCES

174

Thomas:1986:SDE


Thompson:1987:RTT


Tsujii:1988:PKC


Tippett:1927:RSN


Thompson:1963:SDE


Trithemius:1518:PLS


Trithemius:1606:CGT


Trithemius:1606:CSI


Trithemius:1606:SHE

[Tri06c] Johannes Trithemius. *Steganographia. hoc est, ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa. Matthiae Beckeri, Frankfurt, Germany, 1606. 8 + 180 pp. LCCN Z103.T84 S 1606. Authore ... Ioanne Trithemio
REFERENCES


176

REFERENCES


[Tur99] Alan Turing. Turing’s treatise on Enigma. Technical report, CERN, Geneva, Switzerland, 1999. URL http://home.cern.ch/~frode/crypto/Turing/index.html. This document is retyped from the original (undated??) Turing typescript by the editors Ralph Erskine, Philip Marks and Frode Weierud. Chapters 1, 2, and 6 (of 8) are available; the remainder are in preparation.

REFERENCES


USWarDept:1924:EC


USWD:1924:EC


USASC:1940:CML


USASC:1942:ACC


USDOS:1970:BC


USNBS:1977:DES


USCSSC:1978:CSD


USCSSC:1978:USN


USNA:1979:CS

[Uni79a] United States. National Archives and Records Service. Cryp-
REFERENCES


USNSG:1979:IRW


USNBS:1981:GIU


USDA:1982:SMM


USDA:1982:TGM


USGSA:1982:TGS


USNBS:1983:FPD


USGSAOIRM:1984:ISR


USGAOPEMD:1987:PDD

[Uni87] United States. General Accounting Office. Program Evaluation and Methodology Divi-
REFERENCES


REFERENCES

USENIX:1988:USWa


USENIX:1988:PFU


USENIX:1988:UCPb


USENIX:1989:UCPb


USENIX:1989:PSU


USENIX:1999:UAT


USWD:1980:EC


USWD:1983:EC


USDOA:1989:BC

[UU89] United States. Dept. of the Army and United States Army Intelligence School. Basic cryptography. United States Army

**VanderBank:1988:CFM**


**Valerio:1892:C**


**Vamos:1985:BRB**


**VanTassel:1969:ACT**


**Vandeberg:1986:ICS**


**VanHeurck:1987:TNS**


**vanTilborg:1988:IC**


**vandenAssem:1986:CPA**

REFERENCES

Vernam:1926:CPT


Vallee:1988:HBO


Vallee:1989:HGR


Vincent:1971:PAG


Vincent:1972:CPA


Voydock:1983:SMH


Voydock:1984:SMT


Kerckhoffs:1883:CMF


https://
REFERENCES


Voukalis:1980:GSE

Vassiliadis:1980:GSE

Volts:1941:BC

vanTilburg:1986:DBK
Johan van Tilburg and Dick E. Boekée. Divergence bounds on key equivocation and error probability in cryptanalysis. Lecture Notes in Computer Science, 218:489–513, 1986. CO-
REFERENCES

DEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic).

[Vazirani:1985:ESP]

[VV85]

[Wagner:1983:F]

[Pen1900:ADB]

[Wab87]

[Wab87]

[Wang:1986:UEA]

[War1982:BTC]

[Wat1989:VAC]
Miguel Watler. VLSI architectures and circuits for RSA encryption. Thesis (M.Sc.),
REFERENCES

Queen’s University, Ottawa, ON, Canada, 1989. 137 pp.


REFERENCES


as a source for cryptosystems.

**Willett:1983:TKS**

**Willett:1983:PAP**

**Williams:1985:SPK**

**Williams:1986:PKE**

**Williams:1986:ACC**

**Williams:1986:CTU**
John J. Williams. *Cryptanalysis techniques: the ultimate decrypt-
REFERENCES

Winterbotham:1969:SP


Winterbotham:1974:USF


Winterbotham:1978:NC


Winternitz:1983:POW


Winternitz:1984:SOH


Winterbotham:1989:US


Wagner:1985:PKC

REFERENCES


[Wolfe:1943:FCCa]

[Wolfe:1943:FCCb]

[Wolfe:1943:FCCc]


[Wol83]

[Woo82]

[Worth:1975:CMA]

[Wortmann:1987:BRB]
REFERENCES

191

ciencedirect.com/science/article/pii/02217879011844.


REFERENCES


[Yun85a] Mordechai Yung. Cryptoprotocols: Subscription to a


