A Bibliography of Publications on Cryptography:
1606–1989

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA

Tel: +1 801 581 5254
FAX: +1 801 581 4148
E-mail: beebe@math.utah.edu, beebe@acm.org, beebe@computer.org (Internet)
WWW URL: https://www.math.utah.edu/~beebe/

12 October 2023
Version 4.112

Title word cross-reference

(modp) [Pol78]. 1/2 + 1Poly(log N)
[ACGS84]. $\text{13.95}$ [Hig83]. $\text{16.95}$
[Ano84a]. $\text{19.95}$ [HJH85]. 25 · 109 [PSW80].
2$^m$ ± 1 [BLS75]. 2$^n$ ± 1 [BS67]. 2n [QG89].
$\text{34.95}$ [Ano82a]. $\text{35.00}$ [Lei79a, Lei79b].
$\text{49.95}$ [Shu80a, Shu80b]. B [CS83]. $D$
[Kak85]. $F_q$ [SX89]. $\frac{1}{2} + \text{poly(logN)}$ [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]. $N$
[Knu87, QG89, VGT89]. n = 2 [Lev61a].
NC$^0$ [Has87]. O(log n) [IW88]. O(log n)
[Bra87a].

- Bit [QG89]. - ciphered [Knu87]. - 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, BC185]. 1985 [Wil86b]. 1986
[ACM86, IEE86a]. 1987
Mit76, NBS75a, Per85, PH78, PST88, Ree79, Roy86, Sha82, Sha84, Yas76, CA81, CA83a, Hun85, Kno79, Mar76, Wic87. Algorithms [DS83, Has84, HM83, Knu69b, Knu69a, Knu73, QG89, Riv74b, She86, She87, AIR83, Ag85, Eve98, Gam88, Mor89, ORS+87, PBGV89, Riv74a, SB84, She88].

Algorithms [DS83, Has84, HM83, Knu69b, Knu69a, Knu73, QG89, Riv74b, She86, She87, AIR83, Ag85, Eve98, Gam88, Mor89, ORS+87, PBGV89, Riv74a, SB84, She88].

Algorithms [DS83, Has84, HM83, Knu69b, Knu69a, Knu73, QG89, Riv74b, She86, She87, AIR83, Ag85, Eve98, Gam88, Mor89, ORS+87, PBGV89, Riv74a, SB84, She88].
[FF57, Lea87], aucta [Sch33]. Auditing [SK97]. auffzulosen [Sch20]. August [ACM89a, Gle87, USE88b, USE88a, Wil86b, Wal00]. Austria [CSB89, Pie86]. auto [Hei76]. Authenticated [DS83]. Authenticating [Smi87]. Authentication [Boo81, BAN89b, CV97, GJ82, GL79, IW81, IL83, Kar85, Kar86, Lan81, MRW89, NIS85, Nat85b, NS78b, NS78, NS88, PVL86, PW86b, PW87b, Lin93, Sid81, Sim85a, St.84, St.85, SNS88, Tsu89, WC81, ALN87b, Ano86a, Ano87c, Ano87d, Ano87j, BAN89a, Chr88, Den84b, Gif81, HHL89, Kaw87, Mer82b, Mil87b, NS78a, OR87, Lin87, Lin88, Lin89, SM38, Spe87, Tho74, Wan86]. Authenticator [Dav85]. authenticators [FVTS87]. Authority [MM87]. Authorization [GW76]. Automata [IEE74, KV89]. Automated [Gui76, CR88a]. Automatic [AWL88, Hig88f]. Automat [FVTS87]. automaton [Gua87, TC85, TC86]. Available [MM87]. avalanche [DQD85]. AVL [Hol87]. Award [Ano82d, Ash87]. Awards [Bur81].

B [Bv82, Man60, Zaf63, Cas76]. B.C [Bud29, Bud76]. B.S.T.J. [Hen81].


banking [Per88]. Banned [SE86]. Banquet [SWT81]. barbaris [Hei76]. bars [Gyl38].

baru [Saw55]. base [Wel80]. Based [CR85, ElG85b, Gud80, Has84, HR82, IW81, Mer88, OSS85, Rub79, Sha85, WM85, Ale98, BR88, BS82, BS83, CF78, CR88c, CV89, Dem88, Dre79, EG85a, ElG85a, Gon89, Gro74, IL89, Jon86, Kar89a, Kar89b, KM88, Lan89, LB89a, LB89b, Lei80, Lew78, Lid85, MS76, Mil85, Mit76, MT86, MS83, Nie88, Nöb88, PBGV89, Ron84, Sal85, SY86a, SY86b, Sal88, TIF88, YY89]. Bases [Ker75, MOV89, VGT88, VGT89]. Basic [UU89, Uni70, Dagh94, Sha82, Sha84, vdvAvE86, Boy86, War82]. Basic-plus [War82]. Batavia [Con39]. Bateman [Mul89b]. battle [Nor73, Roh77, Mac87, Roh75]. battles [Roh77]. Be [SE86, Hel79a, McC75, MT72, Nai89].


Bibliography [Lan46, Vol41, Gal45a, Gal45b, Gal45c, Gal70, Lei79a, Lei79b, Pri83, Shu76]. Bijective [Oka88].

Biao [PM78, Bou85, Er89, Vin71, Vin72]. Biographical [BCKS83]. Biographies [We88]. biology [Sch84]. bipolar [Ano78b].

Birkeroed [War87]. Birth [Wel86]. Birthday [CN87, GCC88]. BIT [Riv79, QG89, Cho86, Per85, Roy86, Tex84].

bit-slice [Roy86]. Bits [ACGS84, BM82, BM84a, BOCS83, Boy89a, CG85, CG88, LLL88, LW88, BCKS83]. Black [Yar31, Yar40, Yar83, Fer87].

Bletchley [Goo79, MB86]. Blind [Cha83b]. Block [Fei74, QG89, Whe87, APW85, CE86, Hor85, Smi74]. blockcipher [PBGV89].

Blocking [Yum85a]. board [Ano78b]. boat [Beh54]. Bodyguard [Br75]. Bog [MS76].

Bog-Latin [MS76]. Bomba [Wel86]. Bombe [Wel86]. Book [Ano82a, Ano84a, ...
Ano88a, Bro86, Fil78, Gin70, HJH85, Had84, Hig83, Lei79a, Lei79b, LM55, Lit87, Man60, Mor82, San86, Sar28, ST89, Shu80a, Shu80b, Vam85, Wor87, EE56, Wal00]. books [Wal00]. Boolean [BM89, KV89]. Boston [Hei76]. Bosworth [Hig83]. Bowditch [BWV88]. Boyds [CN87]. Brainerd [WG82]. Braunschweig [Wal00]. Braunschweig-Luneburg [Wal00]. Break [Pon89, AB81, Gar77, Gef73, VGT88]. Breaking [Bri85, Gaj89, HM83, AN86, PR79, Str87, Con88, Rie87, Jon78b, Jon87a, Wel86b, Win74b, Zor87]. broadband [Eck85]. Broke [Fil78, Cla77a, Cla77b, Win74b]. Broken [AWL88, Koz84b, WTE85, Far67, Far69, Koz84a]. Brother [Cha85b, Cha85c]. Brown [Fil78]. Bruce [Hig83]. Bruijn [Gun88a]. Buddy [LB89a, LB89b]. bug [Sau89]. Buifendam [AWL88]. Build [Cla86]. Built [Win84]. Bureau [Ano78a, BGK77, Dif75, Mar76, Uni78a, Gyl31]. Bureaus [Gyl34]. Burg [Bet83]. burst [Cam87]. Byzantine [Bra87a, DS83, LSP82, Rei85].

chrestomathy [Pro80]. Christ [Shu82].
cialach [Kos83]. Cicco [Per90]. Cifra [Alb70]. Cipher [AWL+88, BP82, Bur81, Bur85, Edw15, Gaj89, Hig87a, Koz84b, McC75, Men20, Pof52, Pro85, QG89, Rub79, Rus27, Sar28, Ver26, WTE+85, APW85, Bar61, Bar75, Bar84, Bon47, Bow59, Bow60a, Bow60b, Cam28, Cum88, Elv87, Fle74, Gar77, Hen82, Hig88b, Hul98, Koz84a, Nea75, Rej77, Rejxx, Riv80, Smi74, Gyl31].
cipher-writing [Hul98]. ciphered [Knu87]. Ciphers [BD74, EG85b, FF57, HM83, LM85, LP87, PR79, Sie85, Web79, AD81, Alb70, Bar79b, Bar97, Bos84, CR88a, CE65, D’A39, D’A71, DG57, EE56, Fri35c, Fri56, Gai39, Gai40, Gai43, Gal44, Gal56, Gef73, Hig73, Hig83, Hit43, Lau64, Lew82, Nan36, Nan74, Nor73, Pra39, Shu80a, Shu80b, Wir89].
Ciphertext [RRM78, Sie85].
circle [BBB81].
circuits [Wat89].
citations [Ano88c, Ano88f, Ano88e]. City [ACM87].
civil [Ano80].
clairissime [Hei76]. Clark [Fil78].
Class [Sie85, Ano39]. classes [Hit43].
classical [Lau81].
Claudios [AWL88, FF57].
Colloquium [IEE86a, Mur87].
Colonel [Cla77a, Cla77b].
Colossus [BWV+88, Cha83a, Coo83, Flo83, Ran82a, WGG82, Zor87].
column [Bra89b, Bra89a].
combinations [S.73].
Combinatorial [AG85].
combined [Chr88].
Combining [Sie84].
Command [RW84].
Comment [Kol77].
Commentaries [AWL88].
Comments [BWV+88, Am88, Am89, NBS75a].
Committee [ML87].
commonly [FF57].
communicating [Hol87].
Communication [An82d].
complete [Oyo83].
Completeness [BOGW88, GGJ97, GMW87].
Compression [KBD89, Joh89, KS89].
Compromise [Mac87]. Computation [AWL+88, CG87, Pol78, Yao82a, FVTS87, JL75]. Computational [Sim79b, Mei83].

Computationally [AIR83, Wil82c]. Computations [BOGW88, QSA88]. compute [Per85].

Computer [Ano78a, Ano82d, Boy88, BGK77, BCKS +83, Bur81, CR88b, Dav85, EK74, Fei73, Gai80a, Hig88a, IEE79, IEE81, IEE82a, IEE82b, IEE84, IEE85, IEE86b, IEE87a, IEE88, IEE93, Kol77, Kon89, Lau81, Lit87, MZS79, Mu88, NIS85, Nat85b, PK79, Ran82a, Ran86, Sny80, Sto89, Sum84, Uni78a, WTE +88].

Computerized [Cha85b]. Computers [Che73, GJ79, Goo79, Lev61a, ML87, NS78b, Ran82b, SE86, Van69, Bos82, Fey82, Hig83, Kah76, NS78a, Sch69, BWV +88].

Computing [ACM82, ACM83, ACM85, ACM86, ACM87, ACM88, ACM89a, ACM89c, BIB89, BMV85, Bur81, Den79a, Ass88, Cam87, EHG85c, Hog88, Odd87a, Pfe89, PH78, Sch84, Sch66].

conceal [BB79]. concealable [KL84]. concealed [Lea87]. concept [Des88].

Concepts [Hig88c, Ano84b]. Concerning [Hil31, Kar89b, WS79].

concinnatae [Hei76]. conclusion [Bra79].

course [Herm89]. Conditionals [BCKS +83]. Conference [Ano78a, CSB89, CM82, Fea83, HW76, IEE81, IEE82b, IEE87b, IEE88, Ker75, MZS79, RR86, SAW +81, San86, USE88c, USE89b, USE90, USE99, Ano87a, Ano88g, EKMN84, Had84, LLH89, Mor89, Rud82, Uni78a].

conferring [Bud29, Bud76]. confidentiality [Ple77]. confidentially [Ple75].

Confine [Lam73]. conglobatae [Hei76]. Congress [Gle87]. congruence [Phu82]. congruences [FKH +88].

congruential [Boy89a, Knu80, Knu85, Ree79, Ste87].

conjecture [BSW89, Mul89b].

conjugationes [Hei76]. Connection [Kol77, Win78]. Consensus [CMS89].

Consequences [IR89]. Considerations [KBD89, Mey73].

Constant [BI88, CMS89]. Constant-Time [CMS89].

Construct [GGM86, CS83, LR88b].

constructing [AB81, IM86]. contain [Lea87]. contained [Wal00]. containing [Bud76, du 44].

Continued [Por52, Sha48b]. Continuously [MM87]. contracts [GEL85]. Contribution [Gyl34].

Contributions [EKMN84].

Control [AT83, Bla83, Kar85, MTMA85, Pro85, Dat85, Dem88, Gra82, Kar86, O'S88, Sal73, San88].

Controlled [AWL +88, Gun88a, OM84].

Controlling [O'S88, Wei83].

Conventional [Bud82a, Mer88]. conversations [Shu82].

convoy [Roh77, Roh75]. coprocessing [Van86].

Coprocessor [SK97]. core [GL89].

Corporation [WTE +85]. Correcting [SBET85, Mor89].

Corrections [CC81, Kak85, Rao84].

Correctness [Ano81a]. correctness [Ga77, Gai80c, O'S88].

Correlated [Blu84].

Correlation [Sie84].

Correlation-Immunity [Sie84].

Correspondance [S.73].

Corrigendum [Vin72].


counterintelligence [Men89].

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

Covert [Giv78, Kon89, Ano82b, Gle57, GPW85, Gle86, Kob87a, Wol43a, Wol43b, Wol43c, Wol83].

Covert [Giv78, Kon89, Ano82b, Gle57, GPW85, Gle86, Kob87a, Wol43a, Wol43b, Wol43c, Wol83].

Crack [Giv78, Kon89, Ano82b, Gle57, GPW85, Gle86, Kob87a, Wol43a, Wol43b, Wol43c, Wol83].

Crime [DB89]. criteria
[BLS75]. **Criterion** [McC75]. **Critical** [Her78, Riv79, Roh77]. **critique** [DH76a]. 
**crittografia** [Sac36, Sac47]. **crossword** [SD86]. **crosswords** [WW79]. **crypt** [Pro80, RW84]. **crypt-ology** [Pro80].

**Cryptanalysis**
[And52, Ano60, Bar61, Bar75, Bar77, Bar79a, Bar84, Bee81, BO88, Can71, CE86, Daw85, DH77, Fos82, Gai44, Gai56, Kon85, Lev61b, Mac87, MN86, Nöb84, Nöb85, Nöb88, RRM78, SS84, Wil86c, dB88, And79, And80, Ano39, Ano76, Ano82b, Bla75, BB60, BB67, Bri86, Bri88, CR88b, Cun84, DK85, DDP85, Elv87, Fri35a, Fri35b, Fri39b, Fri41, Fri42, Fri76c, Fri76d, Fri87, Gai39, Gai40, Gai43, Gai83, Gyl36, Gyl38, HS89, Hit43, Hof55, Kul35, Kul38, Kul67, Kul76, Lev61c, Mil43a, Mil43b, Mil43c, Sim46, Sim66a, Sim66b, 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, Hei81].

**Cryptanalytical** [Cha86b]. **cryptanalysis** [CR88a]. **cryptic** [SD86, WW79].

**CRYPTO** [BC85, Bra90, Wil86b, CF88, F˚ak87, O'C81, Wil85, CRS83, CRY81, Ger82, Odl87b, Pom88]. **Crypto-ease** [O'C81]. **Crypto-Functions** [Wil85].

**Cryptogram** [Ano60]. **Cryptograms** [MM83, Nan36, Nan74]. **cryptography** [Bar77, Gyl36, Gyl38]. **Cryptographer** [Sca86, Wol70].

**Cryptographia** [Con39, Put27, Col64]. **Cryptographic** [ARS83, Agn87, Agn88, AT83, BIB89, BCI85, Bry67, CPS7, CP88, DLM82, DHM80, Dlf82b, EMMT78, Fei70, Gifs1, GJ82, GGM85, Gun88b, Gyl34, Ham71, Hen81, KV89, KMM*80, Len87, LT85, MTMA85, MM78, QV89, Ritxx, San88, Ser85, Sha83a, Sie84, Smi83, Uni88a, Van69, VA88, Ano86b, BOCS83, Bla79, Bur88, Com76, CF88, Coh87a, D*83, Erd86, Fei74, FNS75, FF57, FM76, GY85, Gro74, HS85, HFL*85, Her81, HCS88, IN89, Lau81, Lev83, LR86, Mas83, NY89b, NY89a, Odl85, Par85, Pic86, PH78, Sed88, Smi71a, Smi74, SB84, Uni82a, Uni82b, Wei83].

**Cryptographically** [BM82, BM84a, KM88, Sha83b, Ayo83, Ste87]. **Cryptographic** [vN83, S.73, Val92, Bau39, Bau46, Giv25, Giv32, Jos85, LS25, Sac51, dIS02, du 44].

**Cryptography**
[Ame81, Ano76, Ano88c, Ano88b, BBB*81, BP89, BB85, Bet83, BGK77, BE76, BE79, Bur84a, Bur84b, CG75, Cop87, CM79, Dav81, DB81, Den82, DH76b, Dlf88, ECW75, Fei73, Fis84, Fri76c, Gro82, Gud80, GL82, Hel79b, Hil29, Hsi31, Hul98, Kon81, LM22, Lan81, Len87, Lev85, Lev61a, Lev61b, Mau4, MM82, Mil86, Mor66, SP89, Sha87, Sha45, SE86, Smi43, Smi44, Smi71a, Smi83, Tur41a, Wil82a, dRHG*99, AS83, Are21, Are22, BCB88, Bau39, Bau46, BB89, BS82, Bra81, Bus82, Cho86, DK85, Des88, D76c, Fri76a, Fri76c, Fagg88b, Gai88, Ger82, Giv78, Gui76, HHL89, Hel76, Hit43, IL89, vN83, Kil88, Kob87a, Kra86, LS25, LS81, Lec89, Lev61c, MS76, Men39, Mey73, Mic88, Mil43a, Mil43b, Mil43c, ML67, NBS76, Nea75].

**cryptography** [Per85, Pie77, Pri83, Sac36, Sac47, Sac51, Sac77, Sch84, Sch86, SW61, Shu76, Shu82, SNO72, TP63, Uni42, VS41, Vd41, Vai00, We88b, Wei89, Wie87, Wil82b, Woo82, dIS02, BCKS*83, Col64, du 44, Kon89, Lei79a, Lei79b, Ano82a, ST89].

**Cryptologia** [Hig881]. **Cryptologic** [Ale45, Jou88, Sny79, Sny80]. **cryptologist** [Cla77b, FFW55]. **Cryptography**
[AM85, BC85, Boy86, Bra89b, Bra89a, Cal92, CRS83, CP87, Com87, DKKM87, DK*89, Fer87, Gir72, Kah66, Kah79, Kah84, Kon89, Las85, Len79, LP87, Mar70a, Mar70b, Mei83, Nai89, Por84, QV89, Rug85, She86, She87, ...
digitalized [Rab77]. Digits [Ran55, Ran01]. Digraphic [Bow59].
dimension [MM82]. Diophantine [Lag84a]. diplomacy [TP63]. Diplomatic
[Web79, Shu80a, Shu80b]. Direct [Bou85]. Directions [DH76b]. Directly [MO182].
Dirichlet [BD74]. disaster [Far67, Far69]. Discrete [COS86, EIG85a, Odl85, Adl79,
CEvGP87, DO86, EIG85a, EIG85c, Gm88, Her81, LW88, Odl87a, Per85, RR86].
Discretionary [Kar85, Kar86, Kar87]. discussion [BB88]. disk [Hig89].
Dispersal [Rab89]. dissertation [She86, She87]. distance [Vou80a, Vou80b]. Distributed
[ACM89a, BOGW88, Mil87b, RU88, Sat89, MT86]. Distributed-protocol
[Mil87b]. Distribution [BBF83, MM78, CM85, Eck85, Kar84, LLH89]. Dits
[BCKS+83]. Divergence [vTB86]. Divers [S.73]. Divi [Hei76]. Division [Mon85].
divisions [Bar75]. Dkr [Bro86]. Dn [Tri60b, Tri21b]. do [BB79, Kos83].
Document [Cop89]. documents [Lew78].
DOE [Bur88]. does [Bra79]. DOL [Tho86]. Donald [Hit43]. Door [IWA81, MH78].
Doorbell [Sto65]. Doran [AWL+88].
double [Cou86]. Dr. [Ano60]. Draft
[Bra75a, CR85]. Dual [NM88]. Duke
[Wal01]. Dupont [BBB+81]. durch [Sch20].
during [Bar79c, Bar79b, Men89]. Dutch
[BBW+88]. Dvorak [WTE+85]. Dynamic
[Pro85, Tsy89, WCWG86]. dzialan [Kos83].
E. [WTE+85]. Early
[BBW+88, Goo79, Zor87, BBW+88]. Eary
[Riv87]. ease [O’C81]. East [Str89]. Easy
[Gal78, Gor85, VV86]. Eavedropper
[RS84]. ECL [HR82]. écriture [S.73, Zaf63].
écritures [Per90]. ECS [Nen75]. ed
[AWL+88]. Edgar [Sau89]. Edited [CM82].
Editor [Den79b, Mul89]. Edmonton [ACM89a]. EDP [Ano84b]. eds [AWL88].

Education [BBB+81, Mar70b]. Educators [Gra82]. Edwards [Bur81]. Effects [Beh54].

Efficient [BG85, DDG+85, HGD85, IN89, Kno79, KFB79, OSS85, OR87, Rab89, RT88, VV85, ABR83, ABS81, MI88]. efforts [Gra82].

EFTs [Van87]. Egg [Sto89].

Egyptian [Cas76, Bud76]. Eighteenth [ACM86]. Eighth [ACM89a].

Electrical [IEE82b]. Electronic [Ano85b, BW85, HFL+85, Per88, Lin93, Cha79, Cha81, Kem88, Lin87, Lin88, Lin89]. Electronics [IEE82b, Hor85, SWT+81].

Elementary [Cam71, Fri76e, Gai39, Gai40, Gai43, Gle57, GPW85, Gle86, Lev61b, Mil43a, Mil43b, Mil43c, Sin66, Sin68a, Sin68b, Lev61c].

Elements [Fri76d, UG23, Uni24b, UU80, UU83, Uni24a, BE76, Fri76b, PR85a, Bau39, Bau46, Bau39, Bau46]. Elliptic [Kob87b, Mil86, CL88, Len87, SX89].

Elsevier [Lit87, San86]. elucidation [Wal00]. elusa [Hei76]. Embedding [BCB88, Sha83a]. emc [Ano87a, Ano88g]. emp [Ano87a, Ano88g]. employed [Col64].

empregados [Col64]. emulates [Ano78b]. enciphered [Bar79a, Lea87]. Enciphering [Kno79, KFB79, Tuc70]. Encipherment [BM75, BM76, FH74, Kon85, Bar79a, PR85b, Lin87, Lin88, Lin89]. Encrypted [VP88, ALN87a, Ano87b, Ano88, SSDG81].

Encryption [Ano78a, Ano81b, Ano82c, Ano88f, Ayo68b, Ayo68a, Ayo81, Bar74, BM89, Bec82, Bet88, Bis88a, Bis88b, Bis88c, Bis88d, BG85, Boo81, Bra75a, Bra75b, Bur88, CA81, CA83b, CA83a, cS85, DWK81, Den79b, DB89, DH76a, DH77, EMMT78, FMP85, Fra85a, Gai77, Gai80a, Gai80b, Gai80c, GM84, Gai83, HS87, Hig87c, Hig88e, Hoo80, IEE86a, Jue81, KJ77, Kuk85, Kal85, Kat77, Kem88, KBD89, Kol77, Lex76, LS89, Ma79, Mar76, MH81, Mer88, Mit76, NBS75a, NBS75b, Nat77, Nat84, NS78b, PM78, Pea80, Ple75, Ple77, Pon89, PK79, Lin93, SJ76, SB82, SBC85, Sim79c, TT84a, TT84b, Tho86, Uni78a, Uni78b, Uni87, Uni82c, UNN83, UNN85, Uni84, Uni77, Uni81, Uni83, Uni88b, Yas76, Am83, AA88, Ano80, Ano84b, Ano85b, Ano87a, Ano88d, Ano88e, Ano88g, APW85].

encryption [Ayo83, Bar87, Ben88, Ber09, Bis88e, Bis89b, BM84b, Cam88, CF78, Chr88, Chn89, Dat85, Den84b, Die88, Dif75, Dre79, Dro89, Eck85, Fak86, Fal88, Gai78, GY87, Gam88, GM82, Gol84, Gru84, Hig87b, Hig87d, Hig88a, Hig88f, Hua88, HW88, Int81a, Int79, Int81b, Int84, Int87, Int88, Joh89, Jon86, Kal84, KD78, KD79, KYM82, Kem89, Ker89, Knu80, Knu85, KSB98, Klu84, Kra84, Kuc87, MO182, MIS, Mei85, MP86, Mil85, Mul81, NM88, NS78a, NU88, NS89, OCS1, OMS4, ORS+87, PP89, Pri80, Rae84, Ren79, RS83, Roy86, Ses81, Sim79b, Sim82h, Sor80, Sup88, Tex84, Van86, Vou80b, Wab87, Wan86, Wat89, Wel80, Wel82b, Whe87, Wel85, Wel86a, YY89, Zef79, Gab82]. encryptions [RN89]. Encryptor [Cia86]. encryptors [Mor83]. Encyclopedia [BCKS+83]. End [SRC84, Ano84b, KYM82, LS89].

End-to-End [SRC84, KYM82, LS89].

enemy [Zor87]. enforcement [JL75]. engendered [Bla89]. Engine [BCKS+83].

Engineering [Ano88c, Ano88f, Ano88e, Sch75]. Engineers [IEE82b]. England [Mur87].

English [Bud76, MS76]. English-jargon [MS76].


Enigma [Ano81a, AWL+88, Dea88, WTE+85, Ber83, Hod83, Ale45, Ano86c, Ano87a, Ano88g, Ber73, Ber83, Elv87, Gaj89, Gar79, Gar80, Koz84a, Koz84b, Rej77, Rej81, Rejxx, Tur99, Wel82a]. enigmatic [Wal00]. énigme [Ber73]. Entities [NS88].

Entring [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, H˚as88, TIF88].
equidistribution [Koo86]. equipment
[F˚ak87, HFL85, Int81b, Int84, Ser85,
Uni82a, Uni82b, Uni88a, Uni82c, UNN85]. equivalent [Ayo83]. equivocation
[vTB86]. era [BB89, Men89]. Ernst
[Sch20]. eroffnen [Sch20]. Errata
[Ano88h]. 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
[Ano82d]. estimation [And79, And80].
Exchange [Blu83b, Ted85, Yao86, AS83, Rab81].
Execution [FH74], exercise [Bec82, Cal89].
Exhaustive [DH77], exercise [Bec82, Cal89].
Exhibite
[Bur81]. existence
[Lu79, Lu80]. Expanded [Ne87].
Expected [Bra87a]. Experimental
[BB89, SN072]. Experiments [HM83].
Experts [Jur86]. explicantur [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. [SBET85].
F.E.A.L [dB88]. fabrication [S.73].
facsimile [UNN85]. factor
[Gu76, Vou80a, Vou80b]. factored [Bac88].
Factoring [CD85, Len87, Odl87a, PST88,
LtW88a, LtW88b]. Factorization
[DH85b, Wi85, KLL88, Po74].
Factorizations [BS75, BL85, DH85a].
Factors [RM85, CE86]. Failure [CMS89].
Fair [Ted85]. Fall [IEE82b, WTE85].
family [Tex84]. Famous [Bon47]. Far
[Str89]. Fast [AM85, Bis88b, Bis88c, Bis88d,
Cop84, DDOP85, Hen81, Hen82, SM83,
AG84, Bis88a, Bis88e, Bis89b, HC88, Odl84].
Fault [BIB89, BOGW88, Rab89].
Fault-Tolerant [BIB89, BOGW88]. Faults
[CGMA85]. Fear [Hor85]. February
[Ano78a, BBB81, IEE86a, Mur87, Rud82,
Uni78a]. Federal [NBS75b]. feedback
[Nie88]. Fellowship [Bur81]. fernen [Sch20].
Feuerstein [Bet83]. Field [Den84b]. Fields
[CR85, CR88c, Cop84, Jur86, Lid85, Mas89,
Mul81, Odl85]. 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, CR88c, KV89, Lid85,
Mas83, Mas89, Odl85, TC86, TC85].
Finiteness [Blu85]. FIPS
[NI85, Nat85a, Nat85b, Uni83]. First
[ACM89c, Dif88, Faa83, 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 [Blu82, Blu83a, Sak89]. Flips
[Blu84]. Flops [Rub79]. Florence [CM82].
improvements [Sin85]. in-depth [Dat85].
incendiary [Uni88a]. including [APW85].
‘inda [MTA87]. Independent [Blu84].
Index [Pol78, Fri35a, Fri87]. indirect
[Fri35c, RF35]. Indoglottal [Nis89].
Indonesia [HS89]. industry
[Hor85, Rud82, WTE85]. Inferring
[Boy89b, Boy89a, Plu82, Plu83]. Infinite
[TT84a, TT84b]. Influence
[Sny79, Bee81, HT79, HH79]. influenced
[Uni79b]. inform
[Bv82, Hel81, Lu80, Mei81]. Informatics
[CM82]. Information
[Ano88c, Ano88f, Ano88e, Bla85, BG85,
CA83b, CA83a, Cha86a, Coh87b, CM79,
Gag88a, GJ82, Gra82, Len78, MH78, NBS75b,
Rab89, WTE85, Ame83, ALN87b, Bos82,
Gif81, GM82, Hig83, Ham80, Ham86, Hig83, Hor85,
JMS84, PR85b, Rud82, Sal73, Sch84, Sch86]. Initial
[BD74, Bel77]. Inmos
[AWL88]. Inn
[IEE81]. innovation
[AWL88, Gra82, SWT81]. input
[DQD85]. inquisitionis [Hei76]. Insatser
[Gyl31]. inscribed [Bud29, Bud76].
Insection [Sau89]. Insecure
[Den79a, Lam81, Mer78, NS88, Bea72,
Hel79a, Kaw87]. INSPEC
[Ano88f, Ano88c, Ano88e]. Installation
[Cha83a, MM78]. installing [MP86].
Institute [IEE82b]. institution [AA88].
Instrumenta [Sch20]. Instruments
[Ano88h, AWL88, WTE85]. Insure
[Sim79a, Sin84]. integer [DH85a, FHK88].
integers [Len87, Odl88, PST88]. Integrating
[Sat89]. Integration [She88].
Integrity [BS82, PT89, Coh87a]. intellecta
[Hei76]. intellectual [Ale98]. Intelligence
[And86, Jon78a, SBET85, Uni78b, Uni79b,
Bch54, Cal89, HT79, HH79, Hor85, Jon78b,
Men89, Nis89, Zor87]. Interactive
[BOKGW88, Fel87, GMR89, BFM88,
MP502]. interbank [FVT87]. Intercept
[Gar79]. interception [Hor85]. interface
[SSDG81]. interfaces [Ano85b]. internal
[Rou84]. International
[CSB89, CM82, Gle87, IEE82b, Kah63, Ker75,
Kra84, San86, ST89, Mor89, Rud82, Jou88]. Internet
[LS89, Lin87, Lin88, Lin89, Lin93, Tsu89]. Internetworks [IL83]. Interoperability
[Nat84, UNN83, UNN85, Uni84]. interpretation
[Nis89]. Intractability
[BOKGW88, GJ79]. Intractable [Wil85]. Intrepid [Ste76]. Introduction
[Bec88, Bec97, Bra87b, HW75, Sni83, Bos82,
HW79, Hig83, Nan36, Nan74, SP89, ST89,
Sta70, Sta78, War82, van88]. Introductory
[Ano39, Coh87b]. intruder [Fit89].
intruder-proof [Fit89]. invented [Pli98].
Inversen [Gab82]. Investigation [Gam88].
investigations [Fra85a]. involvement
[Uni78b]. Ioannis [Tri06b, Tri21b].
Iohannis [Tri06a, Tri21a]. IPS [KMM80].
Ireland [MS76]. ISBN [Bro86, ST89].
ISDN [PP89]. Island [ACM85, IEE84].
ISO [Cop89, Kra84]. ISO/CCITT [Cop89].
issue [Gal88, Gra82]. Issues
[Lit87, Cho86, Fra89, Mas83]. istikhraj
[MTA87]. Italian [Alb70, Sac36, Sac47].
Italica [Con39]. Italy
[AG85, CM82, Mor89]. item [Sch20].
Iterated [Bri85, BLO83, BLO84, Kar89b,
SY86a, SY86b]. IV
[BCK8+83, Fri41, Tuc79b]. J
[BSCK8+83, Mul89b, WTE85, Rub79].
J. [BCK8+83, Lan46, SWT81, WTE85,
WG82]. Jack [Rud82]. Jacobi [Hei76].
James [Ano84a]. January
[Ano88f, Ano88e, Ano88c, Ano88b, FM76].
Japan [IEE87b, Lew82]. Japanese
[Cla77a, Str87]. jargon [MS76]. Java
[Ale98]. Java-based [Ale98]. Jennifer
[ST89]. Johannes [Shu82, Wal00].
Johannis [Hei76]. John
[Ano82a, Hig88d, MS76, Man60, Shu82].
Joint [Rao84]. Josef [ST89]. Joseph
[Hig88a]. Journal [Jou88]. Jr [Mul89b].

Logarithms [BMV85, ElG85b, Mas83, Cop84, COS86, EG85a, ElG85a, ElG85c, OdI85, OdI87a, PH88]. Logic [BAN89b, HR82, BAN89a, Kar89a, Lei80, CM82]. London [Lei79a, Lei79b, Mur87]. Long [BE79]. Long-Period [BE79]. looks [FFW55]. loop [Tuc70]. Lord [Jef86]. Low [LO85, Boy89a, H˚as88]. Low-Density [LO85]. low-order [Boy89a]. LPC [SJ76].


Mathematicians [Ano81a, Gle87, Rej81, Pat87, Kon89].

medieval [ML67], Mediterraneo [Ben89]. Meetings [WG82], members [Ano39]. Memorandum [Je86], Memories [WTE+85], Memory [LB89a, LB89b]. mensuris [Mer44], Mental [GMW87, Yun85a, GM82]. Mercury [Wil41], merit [VA88], Merkle [Lag84b, Sha82, Sha84], Mersenne [Mul89b, BSW89]. Message [Ano87c, Chr88, Dav85, GMR88, LHM84, MRW89, Lin87, Lin88, Lin93, Lu79, Lu80, MI88, Lin89]. Messages [Rus27, AA88, BB79, FVTS87, KL84, SP79]. Messenger [Wil41], metamodel [Nis89], metatheory [Nis89]. Meteor [Cam88]. Method [ARS83, Bla75, DHM80, Mor66, O’N86, Rejxx, RSA78, RSA83, Bar79a, CM85, Hig88a, Kak84, Lom83, NM88, RSA82]. Methods [Cam88, Gaj89, Pol78, DK89, Dem88, IM86, Ku35, Ku38, KU67, KU76, de 53]. Meyer [BCKS+83], microcomputer [Ano75b, Hig87e, Ste89, Tex84]. Microcomputers [Ano88a, Ano89, Fos82]. Microelectronics [AWL+88]. microprocessor [CV89, MS83]. microprocessor-based [CV89, MS83]. Microsoft [vdAV86], Midway [Mac87]. Mifflin [Ano84a]. Migration [GL79]. Militaire [vN83, Jos85]. Military [Cha86b, Fri35b, Fri39b, Fri41, Fri42, LHM84, Sin77, Fri76a, Fri76c, Hit43, Men89, Zor87, vN83]. Millikin [Hit43]. Million [Ban55, Ran01]. millions [Gar77], Mind [AWL+88], mini [Ano78b], mini- [Ano78b]. Minister [MB86]. Minneapolis [IEE81], Minnesota [IE81]. Mirror [Cla12], missing [Boy89a]. Model [LHM84, Gly36]. Models [CMS89, D83, MPSO2]. Modern [Ano86a, Bra88, Kah66, SE86, Bla75, Bra87b, Com87, DK85, Lec89]. moderne [Lec89]. Modes [CA83a, Nat80, Ame83]. modification [Wil80]. Modular
Networks
[IEE81, Kar85, Mu88, NS78b, PW86a, PW87a, PK79, Ayo83, CV89, KD79, Kar86, Me85, NS78a, NBWH78, Wan86, Wel82b].

Neumann [Ano88i].

Nevada [ACM89b].

Newbold [Sar28].

News [Ano82d, Bur81, Hig88a, Kol77].

Nine [Hei76].

Nine [Wal00].

Ninth [ACM87].

Niv [Ano88i].

NJ [Hig83].

No [Cha86b, BV82, Hig88a, Ker89, Lu80, Mul89b, RM85, Tac79a, Tac79b].

Non [BIB89, BFM88, Chu89, Dav81, Fe87, Bar75].

Non-Cryptographic [BIB89].

Non-Governmental [Dav81].

Non-homomorphic [Chu89].

Non-Interactive [Fe87, BFM88].

Non-pattern [Bar75].

Noncryptographic [BOGW88, Sak89].

Nonlinear [Sie84, TIF88, Web88].

Nonrandomness [KLL88].

Nonsingular [PM78].

Norbert [AWL88].

Normal [Ran55, Ran01, MOVW89].

Normalcy [Ben80].

Norris [AWL88].

Norse [ML67].

North [Had84].

North-Holland [Had84].

Notation [BCKS+83].

Note [BD74, Lam81, Lam73, Wel88a, Wic87, BV82, CM85, Lei80, Mei81, Mul84].

Notes [BD74, Por52].

Notice [NBS75b, Uni83].

Notices [Ano82d, Bur81].

Notion [MRS88, MRS88].

Nov [IEE87b].

Novel [Sto65].

November [ACM89b, IEE82a, IEE89].

NP [GJ79, VV86].

NP-Completeness [GJ79].

NSA [Ano84a, Uni78b].

Number [BIB89, Boy89b, BE79, FMC85, Kon89, Plu83, Sch84, Sch86, VV85, CE86, Guy76, Jac87, Kob87a, KM88, Mit76, Per85, Por84, RT88, Sta70, Sta78].

Numbers [HW75, Bac88, HW79, KLL88, Tip27, Vin71, Vin72].

Numerical [Ano81a, HW76, SWT+81].

Nummis [Mer44].

Nunc [Hei76].

O [Bro86].

Oakland [IEE80, IEE83, IEE87c].

Object [GL79].

Objection [Bl85].

Oblivious [Kil88, Rab81].

Obscuras [Col84].

Obscure [Col84].

Observability [PW86a, PW87a].

Observation [LB88].

Observations [Kar89b].

Obtaining [RSA78, RSA83, RSA82].

Occultam [Tr106c, Tr121c].

Occulte [Con39].

Oct [IEE79].

October [Ano88b, CSB89, HW76, IEE74, IEE81, IEE84, IEE85, IEE86b, IEE87a, IEE89, MB86].

off [Ste88].

Office [IL83].

Official [Lew78].

Ohio [Wei88].

Okamoto [VGT88].

Old [Wil82a].

Ole [Vam85].

Ology [Pro80].

Omura [WW84].

One [BBB+81, Hä87, IR89, IL89, IW81, Kn87, KFB79, Lev85, Sed88, Win83, Win84, AIR83, Acc2, GL89, HC88, NY89b, NY89a, Sha88, Sha88, Wal00].

One-Chip [Ste88].

One-time [AIR83].

One-Way [IR89, IW81, Kn87, KFB79, Win83, Win84, Hä87, IL89, Lev85, GL89, NY89b, NY89a, Sha88].

Only [Sie85].

Ontario [San86].

Op [CG87, SNS88].

OpenBSD [dRHG99].

Operating [HRU76, Hoo80, MTS6, Sii83].

Operation [AWL88, CA83a, Nat80, Ame83, Far67, Far69].

Operations [Cal89, Er86, Gyl31, HT79, HH79, Uni81].

Optimal [MTMA85, MOVW89].

Optimization [LtW88a, LtW88b].

Options [PW86a].

order [Boy89a].

ordered [CS83].

Orderly [PM78].

Ordered [CS83].

Order [AWL88].

Organizations [Sny80, Sny79].

organized [DB89].

organized [DB89].

organized [Des88].

Origin [BCKS+83, Ano78c, Bro81, MS76].

Origins [Ran82b, Kals84].

Orlando [IEE88].

Orleans [IEE74].

oral [Daw85].

Osborne [WTE85].

Other [AWL88, Den84a, AB81, FF57].

output
prepared [BBB+81]. Presence [CGMA85].
present [Riv85]. presents
[Kra86, Mor88, BLS75, Mil76, Pol74]. prime
[KP89, Per85, MB86]. Primer
[Gro82, Kon81, Ano82a]. Primes
[BD74, Gor85, HW88]. primo
[Hei76]. Principem
[Tri06b, Tri21b]. Principles
[ACM89a, Jev74, Fri35c, GS78, Hul98, RF35].
printers
[Sch83]. Printing [Ver26]. Prisoner
[Sim83]. Privacy
[BBR88, Drc79, Fei73, IEE80, IEE83, IEE87c, Lin87, Lin88, Lin89, Lin93, Uni87, Fei70, Gir71, Gir72, Pie77, Wil83b]. Private
[RN87, RN89, Mil85, Ste89]. Private-key
[RN87, RN89, Mil85]. pro [Hei76].
Probabilistic [BG85, GM82, GM84, Gol84, CG88, Lei80, MRS87, MRS88].
Probability
[Tur41a, Gle57, GPW85, Gle86, KP89, vTB86]. Probable
[Mc75, KP89].
Probable-Word-Proof
[McC75]. Problem
[AT83, BCKS+83, Cal89, CN87, GMR85, LSP82, Lam73, Mau14, Ryt86, Sim83, WM85, Bar79a, Com87, Gai78, GF87, Jon86, Rei85, Tho74, Vou80b, Wil83b].
Problems
[BS86, Blu82, Blu83a, BO85d, CG87, LO85, Eve85, FS87, Fri76b, Jur86, MP86, Roh75, Rou84, Sca81, Wil82c].
procédés [S.73]. Procedure
[Bir85, Pur74, Wil80]. Procedures
[Lin93, Bau82, Lin87, Lin88, Lin89, Uni88a].
Proceedings
[ACM82, ACM83, ACM95, ACM97, ACM98a, ACM99b, ACM99c, BC85, CP87, EKM84, Gle87, HW76, IEE80, IEE82b, IEE83, IEE87c, Ker75, KV89, RR86, San86, USE88b, USE88c, USE88a, USE89b, USE89a, Ano78a, Ano78b, Bet83, BCI85, CRS83, CP88, CSB89, CRY81, Fé8a3, Gou88b, Had84, Mor89, Odl87b, Pic86, Poo88, Uni78a, Wil86b, ACM86, ACM88, AWL+88, Bra90].
Process [Bv82, Hei81, Mei81]. Processing
[ALN87a, Ano88i, NBS75b, Ben88].
Processor
[FMP85, Sed88, Bar87]. Produced
[Boy89b, Plu83, Boy89a]. Producing
[Win83]. product
[Ano78b]. products
[Ano89]. program
[Ben88]. Programming
[Pe860, SWT+81, Boy86, Ste88, War82, BCKS+83]. Programowa
[Kos83]. Programs
[FH74, KMM+80, Dea87]. Progressions
[BD74]. Project
[Mu88, Bla75].
projections
[Gy38]. promissa
[Hei76]. Proof
[BM84b, GM89, Mc75, Fe89]. Proofs
[BOGKW88]. Propagation
[Pro85]. properties
[Chu89]. property
[Ale98]. proposal
[Rou84]. Proposed
[NBS75b, Di87, DH76a, Mc75].
propositional
[Kar89a]. Prospective
[Ano88h, AWL+88, WTE+85].
protect
[Gef73]. Protecting
[EHM800]. Protection
[Cha86a, Coh87b, HR76, HPE87, Hog88, Sal73, Wel88a, Ale89, Ano86b, BP82, Ber80, Bra75b, CF78, CF88, Coh87a, Di87, NBS75a, SB84, Uni87, Wel80, vdAvE86].
protein
[GY85]. Protocol
[BBF83, Blu82, Blu83a, Bra87a, St.93, VK84, EGL85, Mil87b, Sak89]. Protocols
[CDD88, CMS89, DM83, FM85, GM87, Mer80, Mer82a, Sid81, VK83, Yao82a, BO85a, BO85b, BO85c, Cam87, DLM82, D+83, Eve85, Kem89, RBO89]. Prototype
[BSC85, BB89]. Provably
[IR89]. provably
[IN89, Sha86]. prove
[FS87]. proven
[Lea87]. Prover
[BOGKW88]. provided
[Gy38]. Providence
[AC85]. provides
[Un87]. Proving
[FLR77]. Pseudo
[AM85, BM82, BM84a, Boy89b, FH1+84, Gab82, LR86, Plu83, VV85, Mit76].
Pseudo-Inversen
[Gab82]. Pseudo-Random
[BM82, BM84a, Boy89b, Plu83, VV85, FH1+84, LR86, Mit76]. pseudoinverses
[Gab82]. pseudonym
[Ano60]. pseudonyms
[Cha79, Cha81].
Pseudoprimes
[PS80]. Pseudorandom
[MT72, Por84, Sha83b, KM88, Lev85, LR88b, RT88]. Ptolemys
[Bud29, Bud76].
scripta [Con39]. scripti [Put27]. scripturam [Tri39c, Tri21c]. sea [Bee81].

Seal [Far67, Far69]. Sealing [GJ82, Gif81]. Search [BM75, BM76, BCKS83, Jue81, Gul83, Sha86, Sie83]. Seattle [ACM89c].

Seberry [ST89]. Sec'83 [Fea83, Had84]. Sec'84 [San86]. Secondary [San86, SBET85, HT79, HH79].

Secondary [Fri35c, NBWH78, BM76, BCKS83, Jue81, Gul83, Sha86, Sie83]. Seattle [ACM89c].

Secrecy [EKW74, Mer82b, Sha49, Gif81]. Secret [Ano80]. Secr`ete [S.73]. Secr`etement [du 44]. Secr`etes [Per90].

Secrets [HJH85, MM87, SDV83, Ted85, Yao86, Hig88a, Kah83, MS81, Rab81]. Section [Den79b, Sim88]. Sector [Ano80].

Secret-key [NU88]. Secretedisk [Hig88f].

Self-Synchronizing [Pro85]. Selfcipher [Pel60]. Selfridge [Mul89b]. Semigroups [Eck83].

Seminar [Mar70b, Mar70a]. Seminumerical [Knu69b, Knu69a]. Senate [Uni78b].

Sententiam [Hei76]. Sentinel [Sup88]. September [BGK77, Ker75, San86].

Sequence [AWL+88, LT85, KM88, Plu82]. Sequences [BM82, BM84a, Boy89b, BE79, Gol67, Gol82, Gun88a, MS87, Plu83, Sha83b, Boy89a, CE86, Kak85, Koo86, Nie88, Por84, Vog85, Vou80b].

Serenissimum [Tri06b, Tri21b]. Service [St.85].

Set [Nai89]. Set [Nea75, WC81, SX89]. seventeenth [ACM85]. Sex [Tri88].

Shakespeare [Are22, FF55, FF57, Lea87]. Shakespearean [FF57]. Shamir [BB79, SP79, Bar78, Lag84b, Odl84].

Shaped [WTE+85]. Share [Sha79]. Shared [IW81, Fra89]. Sharing [CGMA85, FE87, BV82, DS81, DMS81, IS87, MS81, RBO89, Sal73, Wil68a, Wil68b, Wil72, Wil75].

shuffling [NS89]. Shulman [Lei79a, Lei79b].
SIAM [RR86]. sic [Ple75]. Sieve
[Sil87, PST88]. signal
[Ano82c, Bar87, Eck85]. Signaling [Cla12].
signalling [Hol87]. signal [Ano82c, Bar87, Eck85]. Signaling [Cla12].
signatures [MI88]. Signatures
[Boo81, Den84a, Mat79, MH78, Rab77, RSA78, RSA83, Sim85b, Cha83b, Lie81, RSA82, Sal78, TC85, TC86, dC86, dC87].
signes [S.73]. significance [Odl85, PH78].
significant [CG85]. significantibus [Hei76].
signing [EGL85]. similarity [Sch86].
Simonsen [Per90]. Simple
[CMS89, HM83, SBET85, Bar75, Hol85].
simplification [Gyu83]. Simplified [RB82].
Simulate [QSA88]. Simulating [Fey82].
Simulation [Ham71, Kal85, Kla89, Lau81].
Simultaneity [CGMA85, GY87].
simultaneous [Has88]. Singer [IEE84].
Single [Ano78b, Bar61, BOCS83, Gy83, Riv80, Tuc70]. Single-board [Ano78b].
single-chip [Riv80]. Singular [MM83].
Sinkov [Cam71]. sive [Con39, Put27]. Six
[BCKS+83, Fri63, Gy83, Vel82a]. size
[Vas76]. skill [Un82a]. skonczonych
[Kos83]. slice [Roy86]. slide [Gyu83]. Small
[DQD85]. Smart [CBB89, Mic85]. Society
[Des88, IEE82b, Rud82, Ano82d]. sofic
[Bl89]. Software
[Fak86, HP87, SK97, BE76, DDG+85, Er86, Gr84, Hig876, OM84, Ron84].
software-based [Rou84]. Soldier [Un82a].
Solomon [MS81]. Solution
[AT83, Cha86b, GMR85, Man14, Sed88, Dea88, Fri35c, Gai39, Gai40, Gai43, Gai44, Gai56, Htt43, Rei85, Von80b]. solutions
[Com87, FS87, Tuc79a, Tuc79b, VV86].
solver [Fri76b]. solves [Rou84]. Solving
[Blu82, Blu83a, Has88, LO85, MP86, Rejxx, TF+88]. solvuntur [Hei76]. Some
[BS86, BS76, FNS75, Gag88b, GS78, HC88, JM84, Lev61a, Lev61b, Lev61c, MN81, Nie88, WS79, Wil85, dC87, DO86, Eck82, Eve85, FF57, Her78, Hog88, KL88, Koo86, Riv79, dC87].
sonderlichen [Sch20]. Sons
[Ano82a]. sophisticated [Hor85]. Sorting
[DG57]. Sound [Hon19]. Source
[Blu84, Wil82c]. Sources
[An87, An88, CG88]. South [RR86].
Space [Ryt86]. Spanheimensis
[Hei76, Tri21b, Tri06b]. spawned [Hor85].
Speaks [Bur81]. Special
[Den79b, DB81, Gal88, Sim88, Kas63, MS76].
spector [S.73]. specialist [HFL+85]. specialties [Jur86]. Specification [SS89].
Spectr [Chr78, G83]. Spectroscope
[An22]. spectrum [Kab84]. Speech
[KJ77, SJ76, BP85, Hol87]. Speed
[Lev61a, Sed88, Ano87b, PP89]. Sphere
[SBET85]. Spirit [Hau74]. spiritum
[Hei76]. Sprache [Kas63]. spread [Kab84].
spring [Rud82]. Spy [Sto89, Win89].
spying [Hor85]. square [Bow59, Per85].
staff [Un87]. stamp [BO85a, BO85b].
Standard [Ano78a, Ano81b, Ano88f, Bis88b, Bis88d, Bur88, CBA1, CBA3b, CBA3a, Kat77, Nat77, Nat85a, Nat85b, SB82, Un87a, Ano88e, Bar77, Bet88, Diff75, Hig87b, Ame83, Ano78a, Bec82, Bis88a, Bis88c, Bra75a, DH76a, DH77, EMMT78, Fra85a, Gai77, Gai80a, Gai80b, Gai80c, Gu83, Jue81, Lex76, Ma79, NBS75b, Nat84, Un78a, Un78b, Un87, Un82c, UNN83, UNN85, Un84, Un77, Un81, Un83, Un88b].
Standardization [Kra84]. Standards
[Ano78a, BGK77, Mar76, Un78a, BR82, Diff75]. Stars [Rus27]. State
[Blu84, Sha87].
Statement [Hei76]. States
[Shu80a, Shu80b, Sin77, Un78b, Bar79c, Bar79b, Lev83, Web79]. Statistical
[Kul35, Kul38, Kul87, Kul76, de 53]. statistically [Sor80]. Statistics
Steganographia
[Tri06c, Tri21c, Sch20, Sch33, Hei76, Wal00].
Steganographiae [Tri21b, Tri06b].
Steganographica [Hei76].
Steganographicos [Tri06a, Tri21a].
Steganologia [Sch20, Sch33, Hei76, Wal00].
Stego [Hei76].
Stelae [Bud76].
Step [Gun88a].
Stockholm [Fea83].
Stokes [BCKS+83].
Stone [Bud22, Bud29, Bud76].
Stories [Hau74].
Storage [CM79, Ano87b].
Storage/backup [Ano87b].
Stored [TS88].
Stories [Bon47, Fut73].
Story [KBD89].
Stories [Hau74].
Stock [Buck86].
Strategy [Ben89, HT79, HH79].
Stream [Rub79, Sie85, Bar84].
Structured [MS87, Wil83a].
Structured [KD79, KD78, War82].
Subcategories [Uni81].
Subexponential [Adl79, ElG85c].
Subexponential-time [ElG85c].
Substring [Wil83a].
Subkeys [DWK81].
Subroutine [Com76].
Subsequences [Koo86].
Subset [LO85, IN89].
Substitution [HM83, Lev58, PR79, Bar75, Bow59, Fri35b, Fri35c, KD78, KD79, L581, Mit76].
Substitution-permutation [KD78, KD79].
Substitutions [SY86a, SY86b].
Subtle [du 44].
Subtle [du 44].
Subtractive [Mor83].
Sui [Tri06c, Tri21c].
Suitable [Dav85].
Sum [LO85, IN89].
Summary [Uni78b].
Summer [Bur81, Ass88, USE89b, USE89a].
Sunt [Con39].
Supercomputing [ACM89b, Bis89a].
Superincreasing [Wil83a].
Support [BGK77, Bra79, Mail76, KWD78, War82].
Supers [Sch20, Sch33].
Superscript [Hei76].
Superscript [Hei76].
Sur [Wil83a].
Survey [BO88, Cha86b, Tho86, PV85, Pop89].
Sweden [Fea83].
Swedish [Gly89].
Swift [Wil41].
Switzerland [Gun88b].
SX [LW88a, LT88b].
SX-2 [LT88a, LT88b].
Symmetric [QG89, Sim79c, Sim82b].
Symmetry [QG89, Sim79c, Sim82b].
Symposium [ACM82, ACM84, ACM86, ACM87, ACM88, ACM89a, ACM89c, AM1+88, IEE74, IEE79, IEE80, IEE82a, IEE83, IEE84, IEE85, IEE86b, IEE87a, IEE87c, IEE88].
Synchronizing [Pro85].
Synthesis [SB82].
synthesis [Gly89].
System [AT&T86, ?, ARS83, Bur84a, Bur84b, Bur85, DWK81, GW76, Gud80, Hen81, HR82, IL83, LHM84, LB89a, LB89b, Pr85, QSA88, RW84, SRC84, Sat89, SBC85, SMI83, TS88, TT84a, TT84b, ALN87b, BCB88, BCW86, Ch80, D80, FLR77, Fei74, Fra89, Fun87, Her81, Lan89, Lei80, Mil85, MP802, M81, MT86, S80, SNO72, SM87, Sor80, TIF+88, Van87, Van86, ADD891, Ber80, KBBN88].
System/38 [Ber80].
systèmes [S.73].
Systems [Ag87, Ag88, Cha86a, Cha85a, GMR89, H876, K88D9, K88E5, LT85, Mur87, Sha83a, Sha49, SNS88, Ass88, Ver26, Am83e, Bar84, BP82, Bls89, Cha85c, CF88, Dre79, F88, Fri35b, Fri41, FF85, Gon89, Gro74, H80, HW88, L888, L881, M82, MB82, NBW87, Pea80, P85b, S81, T840, Wil85, Wil85b, Wil72, Wil75, CA83b, CA83a].
T [Mul89b, WG82].
T. [BCKS+83, SBET85].
TOL [SSA87].
Täfelungen [Gab82].
Tale [Gar77].
Tale [Bro86, Fra84, Fra85b, Van85, Wor87].
Talk [Fil77, Ano39].
Talk [Bud76].
ta‘miyih [MTA87].
tampering [Ano79].
tandem [Hei76].
Tanis [Bud76].
tap [OW84].
Tapping [Kah76].
Tar [Rud82].
task
Techniques
[BCI85, CP87, CP88, Gun88b, QV89, Van69, FNS75, Kem89, Pic86, RS83, Wil86c].
technologies [DB89].

Telecommunications [IEE87b, Uni82c].

Telecryptograph [Ga64].
telegraph [FM76, Tuc66].

Telegraphic [Ver26].

Telegaphing [Ga64].
teleinformatics [GL82].

Telephone
[Blu82, Blu83a, Gua04, Hon19, NBW78].
telephones [Wab87].

Teletrus [Rih87].
television [Eck85].
telix [FVT87].

Templars [GB82].

Ten [Dif88, Hel79a].

term [Mur88].

Terminal [BD74].

terrorism [DB89].

Test
[HR82, LT85, AG84].

Testing
[Mor88, Eve85, Gai80a, Gai80b, Pol74].

tests [Mil76].

Text [KBD89, PM78, DO86, Int81b, Int84, Int87, Int88].

texts
[Bud29, Bud76, Knu87].

th [VGT89].

TH1 [Uni88a].

TH4 [Uni88a].

Their
[Ano88b, AWL88b, WC81, WTE85, Edw15, Fri35c, Gai39, Gai40, Gai43, Gai44, Gai56, G78, Jur86, NY89b, NY89a, Odl85, dC87].

Theorem
[GMW78, Chu89].

Theorems
[BOGW88, Pol74].

Theoretic
[Bla85, Gro74, JM84].

there [Mer44].

theories [Rug85].

Theory
[ACM82, ACM83, ACM85, ACM86, ACM87, ACM88, ACM89c, BCI85, Bla83, Bla85, CP87, CP88, GJ79, Gun88b, HW75, IEE74, Kon89, Lu80, QV89, Sha45, Sha48a, Sha48b, Sha49, Sim85a, Yao82b, Gag88a, Gag88b, Gol84, Ham80, Ham86, HW79, Jac87, Kob87a, Lak83, Nie86, Per85, Pic86, Rej77, Sal88, Sch84, Sch86, Sta70, Sta78].

Theory/Coding
[Sim85a].

there [Fak86].

thieves [Hor85].

thing [Yas76].

Thinking
[BCKS83, Fut73].

Third [Kah63, RR86].

Thomas [Sea56].

Thompson [SBET85].

Thousands [Fil77].

threat [Ano88a].

Three [Per85, Pon89, WTE85].

Threshold
[Cha85a, Kot85, LLH89].

throughout [Win74b].

Thwarting [Hor85].

tilings [Gab82].

Till [Gyl81].

time [CMS89, FH74, QSA88, Wil68a, Wil68b, Wil72, Wil75, AIR83, Bra81, EIG5c, Hig88a, Sha82, Sha84, Wal00, YY89].

time-luck [Bra81].

Time-sharing
[Wil68a, Wil68b, Wil72, Wil75].

timely
[OR87].

Times [Hig88d, NBW78].

tips
[MP86].

tissue [Fun78].

titles [Sim77].

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].

tradeoff
[Bra81].

traduzir
[Col64].

Traffic
[Cal89, Hol87, Uni79b, Wct82b].

trails
[Cam87].

Trainer
[Uni82b].

Traité
[LS25, dLS02].

Trans
[Lu80].

transaction
[Cha85c, ADDS91].

Transactional
[O’N86].

transcendental
[KLL88].

Transfer
[BW85, Ano85b, Gra82, Kem88, Kii88, Rab81].

Transformation
[Hil31, Com76, NM88].

transformations
[YY89].

transformed
[MOI82].

Transition
[Len79].

translating
[Col64].

translations
[Bud76].

transmission
[Ano88d].

transparent
[Hig88f].

Transport
[VK84].

Transposition
[Fr141, Bar61, Cou86].

Trap
[IW81, MH78].

Trap-Door
[IW81].

Trapdoor
[Wil83a, Yao82b, GM85, SM83].
verification
[KYM82, Kem89, MI88, Sil83, WCWG86].
verified [SSDG81].
Verify [Sim79a, Sim84].
Verifying [ALN87b]. Vernam [Tuc70].
Verschlüsselungsabbildungen [Gab82].
version [OSS85]. versions [CM82]. versus [Dif82a, Fák86].
Verify [Sim79a, Sim84].
Verifying [ALN87b]. Vernam [Tuc70].
Verschlüsselungsabbildungen [Gab82].
version [OSS85]. versions [CM82]. versus [Dif82a, Fák86].
Verify [Sim79a, Sim84].
Verifying [ALN87b]. Vernam [Tuc70].
Verschlüsselungsabbildungen [Gab82].
version [OSS85]. versions [CM82]. versus [Dif82a, Fák86].
Verify [Sim79a, Sim84].
Verifying [ALN87b]. Vernam [Tuc70].
References


[ACGS84] W. Alexi, B. Chor, O. Goldreich, and C. P. Schnorr. RSA/Rabin bits are 1/2 + 1Poly(log N) secure. In IEEE [IEE84], pages 449-457. CO-


[ACM85] ACM, editor. Proceedings of the seventeenth annual ACM Sym-

ACM:1986:PEA


ACM:1987:PNA


ACM:1988:PTA


ACM:1989:PEA


ACM:1989:PSN


ACM:1989:PTF


ACM:1989:PTA


ACM:1989:PEA

REFERENCES


C. H. O’D. Alexander. Cryptologic history of the German
REFERENCES


REFERENCES


ACE:1981:RPC


ANSI:1983:ANS


Andrew:1986:TCB


Andree:1952:C


Andelman:1979:MLE


Andelman:1980:MLE


Anonymous:1922:PUS


Anonymous:1939:ITM

[And52] Anonymous. Introductory talk to members of the William and Mary College cryptanalysis.


Anonymous:1981:GIU


Anonymous:1982:BRCa


Anonymous:1982:CC


Anonymous:1982:ESS

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

Anonymous:1982:NNPa


Anonymous:1984:BRP


Anonymous:1984:ESC

REFERENCES

Anonymous:1985:BM


Anonymous:1985:DEA


Anonymous:1986:MTC


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:DEK


Anonymous:1988:DESb

Anonymous:1988:DESa

Anonymous:1988:EVE

Anonymous:1988:ERH

Anonymous:1988:PED

Anonymous:1988:RIA

Anonymous:1989:SZS

Arensberg:1921:CD
REFERENCES

Arensberg:1922:CSP

Adleman:1983:CCS

Alpern:1983:KEU

Ashenhurst:1987:ATA

USENIX:1988:CSSb

Akl:1983:CSP

ATT:1986:AUS

Aspray:1988:RCD


REFERENCES


REFERENCES


REFERENCES


Held at the University of Paris, Sorbonne.

REFERENCES


REFERENCES


REFERENCES


Bertrand:1983:EGE


Bergmann:2009:DKR


Beth:1983:CPW


Betts:1988:ESG


Blum:1988:NIZ


Blum:1985:EPP

REFERENCES

by the International Association for Cryptologic Research.

**Branstad:1977:RWC**


**Bar-Ilan:1989:NFC**


**Birrell:1985:SCU**


**Bishop:1988:AFDa**


**Bishop:1988:FEP**


**Bishop:1989:USS**

REFERENCES


REFERENCES


Blum:1982:HGC


Blum:1984:HGC


Boyer:1984:PCR


Blakley:1985:SRS


Beale:1989:EUR


Blake:1985:CLG

REFERENCES

0&page=73. 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.


REFERENCES


REFERENCES


Branstad:1979:VHD


Brassard:1981:TLT


Bracha:1987:ERR


Brassard:1987:IMC


Brassard:1988:MCT


Brassard:1989:CCb


Brassard:1989:CCa


Brassard:1990:ACC

REFERENCES


REFERENCES


Bryan:1967:CA


Brillhart:1967:SFR


Branstad:1982:ISS


Brickell:1983:SRK


Benois:1986:CSE


Bateman:1989:NMC

P. T. Bateman, J. L. Selfridge, and S. S. Wagstauff, 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) $p = 2^k - 1$ or $p = 4^k - 3$. (b) $M_p (= 2^p - 1)$ is prime. (c) $(2^p+1)/3$ is prime.

Buck:1982:PCS

REFERENCES


REFERENCES

CBEMA:1983:ANSb


CBEMA:1983:ANSa


Calvocoressi:1980:TSU


Callimahos:1989:TAZ


Callimahos:1992:HC


Campagne:1971:REC


Campbell:1987:MBC


Cammack:1988:MDE


[CF88] Per Christoffersson and Viiveke Fak. *Crypto users’ handbook: a guide for implementors of crypt-
REFERENCES


Coppersmith:1975:GCA


Chor:1985:RRL


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.
REFERENCES


Chandler:1983:IMC


Chaum:1983:BSU


Chaum:1985:HKS


Chaum:1985:NSC


Chaum:1985:SIT

[Cha85c] David Chaum. Security with-


Chang:1986:DKL


Chapman:1986:NFS


Chesson:1973:CC


Chor:1986:TIP


Christiansen:1978:SL


Christoffersson:1988:MAE


Chuang:1989:NES


Ciarcia:1986:BHD

REFERENCES


[CMS89] Benny Chor, Michael Merritt, and David B. Shmoys. Simple constant-time consensus protocols in realistic failure models.
REFERENCES


[Col64] F. N. Calâo. A cryptographia revelada, ou, Arte de traduzir e desifrar as escrituras obscuras, quaecunque quae 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.


Coppersmith:1984:FEL


Coppersmith:1987:C


Coppersmith:1989:AID


Coppersmith:1986:DL


Courville:1986:MCC


Chaum:1987:ACE


Chaum:1988:ACE

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Demirdogen:1988:FDM


Denning:1979:SPC


Denning:1979:EOS


Denning:1982:CDS


Denning:1984:DSR


Denning:1984:FEA


Denniston:1986:GCC


Desmedt:1988:SGC

REFERENCES

issn=0302-9743&volume=293.
CRYPTO '87, a Conference on the Theory and Applications of Cryptographic Techniques, held at the University of California, Santa Barbara ... August 16–20, 1987.


REFERENCES

114. 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.


[Deavours:1987:CYT] Cipher A. Deavours, David Kahn, Louis Kruh, and Greg...

**DeMillo:1982:CP**


**delaStelle:1902:TCF**


**Desmedt:1985:DOI**

REFERENCES

Dreher:1979:PSC


Dolev:1983:AAB


duCarlet:1644:CCV


Davida:1981:DES

Ecker:1982:MGE


Ecker:1983:FSR


Ecker:1985:STS


Ellis:1975:PKC


Edwards:1915:CCT


Epstein:1956:FBC


El-Gamal:1985:PCS


Even:1985:PCC

EVEN:1985:RPS


ELLIson:2000:PSK


Eigenthaler:1984:CGA


Evans:1974:UAS


ElGamal:1985:PKCa


ElGamal:1985:PKCb

ElGamal:1985:STA


Elvin:1987:CWW


Ehrsam:1978:CKM


Er:1989:NAG


Erdem:1986:HCO


Estell:1980:BW


Even:1985:CSW


Even:1998:FVA

DEN IEEASAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Faak:1986:SVH


Faak:1987:CMM


Falk:1988:DST


Farago:1967:BSS


Farago:1969:BSS


Feistel:1970:CCD


Feistel:1973:CCP


Feistel:1974:BCC


Feldman:1987:PSN

P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In IEEE [IEE87a],
REFERENCES


[Fey82]


[FH74]


[FHJ+84]


[FHK+88]

REFERENCES


REFERENCES

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.

Fairfield:1985:LRN


Fairfield:1985:LDE


Feistel:1975:SCT


Flajolet:1989:RMS

REFERENCES

Germany / London, UK / etc., 1989.

Foster:1982:CM

Franksen:1984:MBS

Franklin:1985:MID

Franksen:1985:MBS

Franksen:1986:SHM

Frankel:1989:TIC

Friedman:1935:ICA

Friedman:1935:MCP

Friedman:1935:PIS
Friedman:1939:CAC


Friedman:1939:MC


Friedman:1941:MCP


Friedman:1942:MC


Friedman:1956:CCC


Friedman:1963:SLC


Friedman:1976:AMC


Friedman:1976:CEC


Friedman:1976:CCA


Friedman:1976:EC

REFERENCES


Gaglione:1988:ITP


Gaglione:1988:SCT


Gaines:1939:ECS


Gaines:1940:ECS


Gaines:1943:ECS


Gaines:1944:CSC


Gaines:1956:CSC


Gait:1977:VCH


Gait:1978:EEP

REFERENCES


[Gal88] Zvi Galil, editor. Special issue on cryptography, volume 17(2)


REFERENCES


[Gam88]


[Gar77]


[Gar79]


[A Gilmour-Bryson:1982:CDT]

A. Gilmour-Bryson. Coding of the depositions of the Templars. In Ciampi and Martino [CM82], pages 451–467. ISBN 0-444-86414-8 (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

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].

Gelb:1974:RWD

Gersho:1982:ACR

Goldreich:1985:CAR

Goldreich:1986:HCR
Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How

**Gifford:1981:CSI**


**Gingerich:1970:BRB**


**Girdansky:1971:DPC**


**Girdansky:1972:CCD**


**Girling:1987:CCL**


**Givierge:1925:CC**


**Givierge:1932:CC**


**Givierge:1978:CC**


**Garey:1979:CIG**

REFERENCES


Goldwasser:1984:PE


Goldwasser:1985:PSS


Goldwasser:1988:DSS


Goldwasser:1989:KCI


Good:1945:GRT


Goldreich:1987:HPM

REFERENCES


[95] Golomb:1984:PET


[95] Good:1979:EWC


[95] Gleason:1985:ECP

P. E. Gray. Information control I: Technology transfer at issue: The academic viewpoint: Educators believe efforts to limit transfer of knowledge at the university level are likely to

Grossman:1974:GTR

Grover:1982:CP

Grundler:1984:DEH

Gaines:1978:SSP


Grollmann:1988:CMP

Guarini:1904:MTT

Guan:1987:CAP
REFERENCES

**Gudes:1980:DCB**


**Guillen:1976:AC**


**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**


REFERENCES


Gamow:1958:CAP
George Gamow and Martynas Ycas. The cryptographic approach to the problem of protein 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
Haugen:1974:RSS


Hasset:1984:PAU


Hastad:1987:OWP


Hastad:1988:SSM


Huang:1988:SWP


Heidel:1676:JTP

Wolfgang Ernesto Heidel. Johannes Trithemius primo Spanheimensis deinde Divi Jacobi Peapolitani abbatis Steganographia: quae hucusque a nemine intellecta sed passim ut supposititia, perniciosa, magica & necromantica rejecta, elusa, damnata & sententiam inquisitionis passa, nunc tandem vindicata, reserata et illustrata ubi post vindicias Trithemii clarissime explicatur conjurationes spirituum ex Arabicis, Hebraicis, Chaldæicis & Graecis spirituum nominibus juxta quosdam conglobatae, aut secundum alios ex barbaris & nihil significantibus verbis concin-
REFERENCES


**Hellman:1976:SPN**


**Hellman:1979:WTI**


**Hellman:1979:MPK**


**Herlestam:1978:CRS**


**Hellman:1981:ACA**


**Henry:1981:BJB**


**Henry:1982:FDA**

REFERENCES


Hershey:1981:DLP


Hersch:1989:DSA


Hardy:1985:ECC


Hoornaert:1985:EHI


Hinsley:1979:BISb


Harn:1989:PAU

L. Harn, D. Huang, and C. S. Laih. Password authentication using public-key cryptography. Computers and Math-
REFERENCES


REFERENCES

Highland:1988:PEM


Highland:1988:RRC


Highland:1988:TSC


Highland:1988:TSV


Highland:1988:EAE


Highland:1988:SIT


Highland:1989:SDI

REFERENCES

Hill:1929:CAA


He:1988:SDK


Hill:1931:CCL


Hunter:1983:ERA


Hitt:1943:MSM


Hule:1988:RCW


Hodges:1983:ATE


Hoffer:1955:MAC

REFERENCES

Hogan:1988:PIS

Hollis:1987:TCA

Honore:1919:STS

Hood:1980:EFS

Hoogendoorn:1982:SPK

Horgan:1985:TIT

Herzberg:1987:PPS

Holland:1982:GSA

Harrison:1976:POS
Michael A. Harrison, Walter L. Ruzzo, and Jeffrey D. Ullman. Protection in operating

**Haastad:1985:CST**


**Hammer:1987:EUH**


**Hardjono:1989:TCB**


**Hinsley:1979:BISa**


**Huang:1988:APE**


**Hulme:1898:CHP**


**Hunter:1985:ARK**

REFERENCES

107


See note [Wic87].

Hardy:1975:ITN


Hartnell:1976:PFM


Hardy:1979:ITN


Huthnance:1988:UPP


IEEE:1974:ASS

IEEE, editor. 15th Annual Symposium on Switching and Automata Theory, October 14–16, 1974, the University of New Orleans. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1974.

IEEE:1979:ASF


IEEE:1980:PSS

REFERENCES


REFERENCES

IEEE:1986:CEC


IEEE:1986:ASF


IEEE:1987:ASF


IEEE:1987:IIG


IEEE:1987:PIS


IEEE:1988:FAC


IEEE:1989:ASF

REFERENCES


Israel:1983:AOS


Impagliazzo:1989:OWF


Imai:1986:AMC


Impagliazzo:1989:ECS


IRD:1979:DVE


IDC:1981:DE


IRD:1981:DTV


IRD:1984:DTV


IRD:1987:DTV

REFERENCES

Report 727, International Resource Development, 6 Prowitt St., Norwalk, CT 06855, USA, February 1987. vii + 197 pp. [Jac87]


M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structures. In IEEE [IEE87b], pages 99–102. Three volumes. IEEE catalog no. 87CH2520-5. [JL75]


W. Stanley Jevons. The Principles of Science. ???? .????, 1874. ??–?? pp. [Jev74]


Michael Paul Johnson. Beyond DES: data compression
REFERENCES


[Jur86] R. K. Jurgen. The specialties: Experts identify the most outstanding developments or the most difficult problems in their fields. IEEE Spectrum, 23(1):
REFERENCES


[102x318] Kahn:1967:CSSa


[102x204] Kahn:1967:CSSb


[102x180] Kahn:1974:C


[102x84] Kahn:1983:KCS


REFERENCES


REFERENCES

Karger:1986:ADA


Karger:1987:LDP


Kari:1989:CBP


Kari:1989:OCP


Kasiski:1863:GDG

Friedrich Wilhelm Kasiski. *Die Geheimschriften und die Dechiffirkunst, 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

ATISET. ISSN 1046-8188. URL http://www.acm.org:80. Special Issue on Research and Development in Information Retrieval.


Kilian:1988:FCO


Kak:1977:SEU


Kothari:1984:CMW


Kurosawa:1988:CSP


Konheim:1980:ICP


Knoble:1979:AEO


Knuth:1969:SNM

Donald E. Knuth. Seminumerical Algorithms, volume 2 of The Art of Computer Programming. Addison-Wesley, Reading, MA,
REFERENCES


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


Koyama:1982:CUM


Koyama:1982:MKR


Koyama:1983:MKR


Kozaczuk:1984:EHGa


Kozaczuk:1984:EHGb


Kim:1989:PRP


Krause:1984:DEI

[Lothar Krause. Data encryption in ISO, the international organization for standardization.]
REFERENCES

Computers and Security, 3(3): 234–236, August 1984. CO-
DEN CPSEDU. ISSN 0167-
4048 (print), 1872-6208 (elec-
sciencedirect.com/science/
article/pii/0167404884900452

Kranakis:1986:PC

Evangelos Kranakis. Primality and cryptography. Wiley-
Teubner series in computer sci-
tence. John Wiley and Sons, Inc.,
New York, NY, USA, 1986.
pp. LCCN TK5102.5: K661
1986. US$33.00.

Kordes:1989:UMC

F. L. G. Kordes and J. J. Schu-
urman. The use of MEBAS
in creating a simulation envi-
nornment for compression and
encryption. Report NLR
TP 89130 U, National Lucht-
en Ruimtevaartlaboratorium,
Amsterdam, The Netherlands,

Kuchlin:1987:PKE

W. Küchlin. Public key encryp-
tion. SIGSAM Bulletin (ACM
Special Interest Group on Sym-

dbolic and Algebraic Manipula-
CODEN SIGSBZ. ISSN 0163-
5824 (print), 1557-9492 (elec-
tronic).

Kullback:1935:SMC

Solomon Kullback. Statistical
methods in cryptanalysis: tech-
nical paper. War Dept., Office
of the Chief Signal Officer: U.S.
G.P.O., Washington, DC, USA,
1935. various pp.

Kullback:1938:SMC

Solomon Kullback. Statistical
methods in cryptanalysis. War
Department, Office of the Chief
Signal Officer, Washington, DC,
USA, revised edition, 1938. 194
pp.

Kullback:1967:SMC

Solomon Kullback. Statistical
methods in cryptanalysis. Number
14 in Technical literature se-
ries monograph. National Ar-
chives, Washington, DC, USA,

Kullback:1976:SMC

Solomon Kullback. Statistical
methods in cryptanalysis, vol-
ume 4 of A Cryptographic se-
ries. Aegean Park Press, La-
guna Hills, CA, USA, revised
LCCN Z104: K84.

Kears:1989:CLL

M. Kearns and L. G. Valiant.
Cryptographic limitations on learn-
ing Boolean formulae and
finite automata. In ACM-
TOC’89 [ACM89c], pages 433–
LCCN QA 76.6 A13 1989.
URL http://www.acm.org/
pubs/articles/proceedings/
stoc/73007/p433-kears/p433-
kears.pdf; http://www.
acm.org/pubs/citations/proceedings/
stoc/73007/p433-kears/.
Kasami:1982:KMS


Laffin:1964:CCS


Lagarias:1984:KPK


Lagarias:1984:PAS


Lampson:1973:NCP


Lampport:1981:TNP


Landers:1946:RPR


Langie:1981:CSS


Landau:1989:SSC


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


Lee:1989:WLB


Leary:1987:CSM


Leclerc:1989:CRM


REFERENCES


Leighton:1979:BRA


Leighton:1979:BRB


Leiss:1980:NSS


Lempel:1979:CT


Lennon:1978:CAI


Lenstra:1987:FIE


Levine:1958:VMS


Levine:1961:SAH

REFERENCES

PAF. ISSN 0025-5718 (paper), 1088-6842 (electronic).

Levine:1961:SECa

Levine:1961:SECb

Levine:1983:USC

Levine:1985:OWF

Lewin:1978:UGW

Lewin:1982:AMC

Lexar:1976:END

Landwehr:1984:SMM

Lidl:1985:CBP
REFERENCES

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

[102x681]Lieberherr:1981:UCD


[190x602]RFC0989


[251x491]RFC1040


[446x289]RFC1113


[460x235]RFC1421

REFERENCES


REFERENCES


of Traite de cryptographie / par Andrée Lange et E.-A. Soudart. “Plus many problems in French for the solver”.


[LSP82] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine generals problem. ACM Transactions on Programming Languages and Systems, 4(3):382–401, July 1982. CODEN ATPSDT. ISSN 0164-0925 (print), 1558-4593 (electronic). 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.


REFERENCES

Lu:1980:AEG


Long:1988:DLH


Ma:1979:RAD


Meijer:1981:DSS


MacPherson:1987:CUN


Mandelbrot:1960:BRJa


Marsh:1970:CSS


Marsh:1970:MEC

ISSN 0002-9890 (print), 1930-0972 (electronic).

Marion:1976:ANB

Massey:1983:LFC

Mastrovito:1989:VDM
E. D. Mastrovito. VLSI designs for multiplication over finite fields $GF(2^m)$. Lecture Notes in Computer Science, 357:397–309, 1989. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Matyas:1979:DSO

Mauborgne:1914:APC

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
J. E. D. Meador. Keeping the camera on an even keel, tele-


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


[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 $2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$, 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


Merkle:1988:DSB


Merkle:1989:CDS


Meyer:1973:DCC

REFERENCES

Merkle:1978:HIS


Merkle:1981:SME


Matsumoto:1988:PQP


Michener:1988:TSK


Millikin:1943:ECCa


Millikin:1943:ECCb


Millikin:1943:ECCc


Miller:1976:RHT


Miller:1985:PES

REFERENCES

[135]

[102x681] REFERENCES

[102x681] 135


[102x395] [ML87] Ruth A. Maulucci and J. A. N. Lee. Happenings: The

**Matyas:1978:GDI**


**Meyer:1982:CND**


**Moler:1983:SVA**


**Meadows:1987:MSA**


**Muller:1981:SRP**


**Muller:1986:CDS**


**Matsumoto:1982:DTL**


**Montgomery:1985:MMT**

REFERENCES

137


Morland:1666:NMC


Morrice:1692:EB


Morrison:1983:SEA


Morain:1988:IGP


Mora:1989:AAA


Mullin:1988:ONB


Mevis:1986:SCP

REFERENCES


Mullender:1986:DCD


Marayati:1987:AWA


Mackinnon:1985:OAA


Muftic:1988:SMC

Mulherin:1981:FDE

Mullin:1989:LEN
Albert A. Mullin. Letter to the editor: “The new Mersenne conjecture” [Amer. Math. Monthly 96 (1989), no. 2, 125–128, MR 90c:11009] by P. T. Bateman, J. L. Selfridge and S. S. Wagstaff, Jr. American Mathematical Monthly, 96(6): 511, ????. 1989. CODEN AMYYAE. ISSN 0002-9890 (print), 1930-0972 (electronic). See [BSW89]. Conjectures that \(M_n(= 2^n – 1)\) 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, vis. \(M_q\).

Muraszko:1987:CVR

Merwin:1979:NCC
REFERENCES

Naik:1989:CDS


Nanovic:1936:SWI


Nanovic:1974:SWI


NBS:1977:DES


NBS:1980:MO


NCSOTS:1984:ISR


NIST:1985:FPSa


NIST:1985:FPSb


NBS:1975:EAC

REFERENCES

[NBS75b] NBS. Notice of a proposed federal information processing Data Encryption Standard. Federal Register, 40(??):12607–??, August 12, 1975. CODEN FEREAC. ISSN 0097-6326.


[Nöb84] Rupert Nöbauer. Cryptanalysis of the Rédei-scheme. In Eigenthaler et al. [EKMN84], pages
REFERENCES


T. Nemetz and J. Ureczky. A random linear secret-key encryption. In Probability theory and mathematical statistics with applications (Visegrád,
REFERENCES


Naor:1989:UOW


Naor:1989:UOH


Oakley:1978:RPC


O’Connell:1981:CDE


Odlyzko:1984:CAM


Odlyzko:1985:DLF


Odlyzko:1987:CCD

REFERENCES


ORS+87 G. A. Orton, M. P. Roy, P. A. Scott, L. E. Peppard, and
REFERENCES


REFERENCES


Pierce:1977:SSP

Popek:1979:ESC

Pless:1975:ESC

Pless:1977:ESC

Plimmer:1998:MIW

Plumstead:1982:ISG

Plumstead:1983:ISP

Payne:1978:OEN
W. H. Payne and K. L. McMillen. Orderly enumeration of nonsingular binary matrices applied to text encryption. Communications of the Association for Computing Machin-
REFERENCES


REFERENCES

Posch:1989:AEA


Peleg:1979:BSC


Pieprzyk:1985:DPK


Pieprzyk:1985:MDI


Pratt:1939:SUS


Pritchard:1980:DE


Price:1983:ABR


Pronzini:1980:MCC

REFERENCES


REFERENCES


Puteanus:1627:EPC


Pluimakers:1986:ACS


Pfitzmann:1986:NUO


Power:1987:AHE


Quisquater:1989:BHF

Qin:1988:RSS


Quisquater:1989:ACE


Rabin:1981:HES


Rabin:1989:EDI


Rand:1955:MRD


Randell:1982:CGC


Randell:1982:ODC

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

REFERENCES

A. Deavours and I. J. Good. This article was entitled “Jak matematycy polscy rozsyfrowz Enigmgę” in the Annals of the Polish Mathematical Society, Series II, Wiadomości Matematyczne, Volume 23, 1980, 1-28, translated by Joan Stepenoke. 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. £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.

Rihaczek:1987:T


Ritchie:19xx:DCW


Rivest:1974:HCA


Rivest:1974:AAR

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


REFERENCES


[San88] Ravinderpal S. Sandhu. Cryptographic implementation of a...
REFERENCES

CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Sarton:1928:BRBn


Satyanarayanan:1989:ISL


Saunders:1989:IDE


Sawirudin:1955:PND


Schaumuller-Bichl:1982:ADE


Sorkin:1984:MCC


Serpell:1985:PES

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**

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


Schroeder:1969:IC


Schroeder:1975:ESK


Schell:1983:SPA


Schroeder:1984:NTS


Schroeder:1986:NTS


Smith:1986:GCC


Sicherman:1983:AQR

REFERENCES


Smillie:1986:RWA


Seaton:1956:THS


Sedlak:1988:RCP


Seeley:1989:PCG

REFERENCES

[165]


Serpell:1985:CES

Seshadri:1981:KPP

Shannon:1945:MTC

Shannon:1948:MTCa
[Sha48a] 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
[Sha82] Adi Shamir. A polynomial time algorithm for breaking the basic Merkle–Hellman cryptosystem. In 23rd annual symposium
REFERENCES


[She86] Alan T. Sherman. Cryptology and VLSI (a two-part disserta-
REFERENCES

167


[102x681]Sherman:1988:CVV


[102x681]Sherman:1980:BRB


[102x681]Sherman:1980:BRU


[102x681]Sherman:1982:RCJ

[She82] Wayne Shumaker. Renaissance curiosa: 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

Sidhu:1981:APG


Siegenthaler:1984:CIN


Siegenthaler:1985:DCS


Silverman:1983:RVS


Silverman:1987:MPQ


Simonetta:1404:LTC

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


[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


Simmons:1988:SSC

Sinkov:1966:ECM

Sinkov:1968:ECMa

Sinkov:1968:ECMb

Sinkov:1966:ECM

Sinkov:1968:ECMa

Sinkov:1968:ECMb

Sinkov:1966:ECM

Sinkov:1968:ECMa

Sinkov:1968:ECMb

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.


[SMi83] 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.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
</table>
| [SRC84]   | J. H. Saltzer, D. P. Reed, and D. D. Clark. End-to-end argu-

**Shamir:1984:CCV**


**Siromoney:1986:PKC**


**Shepherd:1989:CSS**


**Subramanian:1987:DTP**


**Siromoney:1988:CPL**


**Smith:1981:VEP**


**StJohns:1984:RAS**

REFERENCES

StJohns:1985:RAS


Shawe-Taylor:1989:BRB


StJohns:1993:RIP


Stark:1970:INT


Stark:1978:INT


Stevenson:1976:MCI


Stern:1987:SLC


Stevens:1988:CPR

REFERENCES


**Stephenson:1989:PPM**


**Stout:1965:DRN**


**Stoll:1989:CET**


**Stripp:1987:BJC**


**Stripp:1989:CFE**


**Summers:1984:OCS**


**SuperMacSoftware:1988:SDE**


**Shulman:1961:GC**


**Smith:1983:HCR**


**Salzer:1981:RHH**

REFERENCES

Sun:1989:TKE

Salomaa:1986:PCB

Salomaa:1986:PKC

Tao:1985:FAP

Tao:1986:TVF

Tedrick:1985:FES

TI:1984:TTU
Texas Instruments Inc. *TMS7500 TMS75C00 user’s guide, data encryption device: 8-bit microcomputer family*. Texas Instruments, Dallas, TX, USA, 1984. various pp.
<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Tri06a]</td>
<td>Johannes Trithemius. Clausis generalis triplex in libros steganographicos Iohannis Trithemij .... Iohannis Berneri, Frankfurt, Germany, 1606. 7 + 1 pp. LCCN Z103.T84 S 1606. Ab ipso authore conscripta ... Darmbstadji: Excudebat Balthasar Hofmann,</td>
</tr>
</tbody>
</table>
REFERENCES

impensis Iohannis Berneri, bibliop. Francof., anno 1606.

**Trithemius:1606:CSI**


**Trithemius:1606:SHE**


**Trithemius:1621:CGT**


**Trithemius:1621:CSI**


**Trithemius:1621:SHE**


**Terry:1988:MSV**


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

Gaithersburg, MD, USA, 1977. 18 pp. LCCN JK468.A8 A31 no.46.


[Uni82c] United States.General Services Administration. Telecommunications: general security requirements for equipment us-
REFERENCES


[Uni82] 182

USNBS:1983:FPD


[Uni83] 182

USGSAOIRM:1984:ISR


[Uni84] 182

USGSAOPEMD:1987:PDD


[Uni87] 182

USDA:1988:CED


[Uni88a] 182

USNBS:1988:DES


[Uni88b] 182

USGSA:1983:ISR

REFERENCES


[UU80] United States. War Dept and United States. Adjutant-General's
REFERENCES


Philippe Van Heurck. TRA-SEX: national security system for EFTs in Belgium. *Computer Networks and ISDN Systems,* 14
REFERENCES


vanTilborg:1988:IC

[van88]

vandenAssem:1986:CPA

[vdAvE86]

Vernam:1926:CPT

[Ver26]

Vallee:1988:HBO

[VGT88]

Vallee:1989:HGR

[VGT89]

Vincent:1971:PAG

[Vin71]

Vincent:1972:CPA

[Vin72]

Voydock:1983:SMH
Victor L. Voydock and Stephen T. Kent. Security mechanisms in high-level network pro-
REFERENCES


**Voydock:1984:SMT**


**Kerckhoffs:1883:CMF**


**Vogel:1985:LCC**


Held at the University of Paris, Sorbonne.

**Volts:1941:BCP**


**Voukalis:1980:DFC**


**Voukalis:1980:GSE**


**Vassiliadis:1988:PEA**

REFERENCES

Volts:1941:BC


vanTilburg:1986:DBK


Vazirani:1985:ESP


Valiant:1986:NED


Waber:1987:VEC


Wagner:1983:F


Walden:1900:ADB

wherein is also contained a most clear elucidation of the Steganographia, a book at one time composed in magic and enigmatic form by Johannes Trithemius. ????, ????, 1900. LCCN Z103 .A95 1900.

Wang:1986:UEA


Warren:1982:BTC


Watler:1989:VAC


Wegman:1981:NHF


Worthington:1986:IDS


Weber:1979:USD


Webb:1988:NPK


Weingarten:1983:CCP


Weiss:1988:BOP

REFERENCES

- Wells:1980:ADB

- Welchman:1982:HSS

- Wells:1982:USE
  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, Southern Methodist University, Dallas, TX, USA, February 1982. 24 pp.

- Welchman:1986:PBB


- Welchman:1988:CC

- Welsh:1989:CC

- Wilkes:1982:MRJ
Wheeler:1987:BE


Wichmann:1987:NAR


Wiedemann:1986:QC


Wilkins:1641:MSS


Wilkes:1968:TSCa


Wilkes:1968:TSCb


Wilkes:1972:TSC


Wilkes:1975:TSC


Williams:1980:MRP


Willett:1982:CON

[Wil82a] Michael Willett. Cryptography old and new. Computers and Se-
REFERENCES


REFERENCES


[Win84] Robert S. Winternitz. Secure one-way hash function built from DES. *Proceedings of the
REFERENCES


Winterbotham:1989:US


Wagner:1985:PKC


Wolfe:1943:FCCb


Wolfe:1943:FCCc


Wolfe:1970:SWC


Wolfe:1983:FCC


Wood:1982:FAC

REFERENCES

Worth:1975:CMA


Wortmann:1987:BRB


Wrixon:1989:CCS


Williams:1979:SRC


Weiss:1985:RCM


[WTE+85]


REFERENCES

+ 264 + 1 pp. LCCN D639.S7 Y3 1940. The history and work of the Cryptographic bureau, officially known as section 8 of the Military intelligence division (MI-8).

Yardley:1983:CBC


Yasaki:1976:EAK


Yung:1985:CSP


Yu:1989:DEB


Zafíropulo:1963:RAD


Zei79

Howard M. Zeidler. Digital data encryption. SRI International, 333 Ravenswood Avenue, Menlo Park, CA 94025-3493, USA, Tel:
