Title word cross-reference

(modp) [Pol78], $1/2 + 1\text{Poly}(\log N)$
[ACGS84], $\textbf{13.95}$ [Hig83], $\textbf{16.95}$
[Ano84a], $\textbf{19.95}$ [HJH85], $25 \cdot 10^9$ [PSW80],
$2^m \pm 1$ [BLS75], $2^n \pm 1$ [BS76], $2n$ [QG89],
$\textbf{34.95}$ [Ano82a], $\textbf{35.00}$ [Lei79a, Lei79b],
$\textbf{49.95}$ [Shu80a, Shu80b], $B$ [CS83], $D$
[Kak85]. $F_q$ [SX89], $\frac{1}{2} + \frac{1}{\text{poly}(\log N)}$ [CG85].
GF($2^n$) [BMV85]. GF($p$) [COS86, PH78].
GF($p^2$) [EIG85c]. $l$ [VGT89]. $M^3$ [Wil86a].
GF($2^m$) [Mas89]. GF($p^n$) [MOVW89]. $N$
[Knu87, QG89, VGT89], $n = 2$ [Lev61a].
NC$^0$ [Has87]. $O(\log n)$ [LW88]. $O(\log n)$
[Bra87a].

- Bit [QG89]. - ciphered [Knu87]. - tree

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, Fée83, Had84]. 1984
[San86, BC85]. 1985 [Wil86b]. 1986
[ACM86, IEE86a]. 1987
\textbf{Mit76, NBS75a, Per85, PH78, PST88, Ree79, Roy86, Sha82, Sha84, Yas76, CA81, CA83a, Hun85, Kno79, Mar76, Wic87.} \textbf{Algorithms}\ [DS83, Has84, HM83, Knut69b, Knut69a, Knut73, QG89, Riv74b, She86, She87, AIR83, AG85, Eve98, Gam88, Mor89, OR5+87, PBGV89, Riv74a, SB84, She88]. \textbf{Alios}\ [Hei76]. \textbf{Alive}\ [Cha85a]. \textbf{Allied}\ [AWL+88, WTE+85]. \textbf{Allocation}\ [LB89a, LB89b]. \textbf{Alone}\ [RRM78]. \textbf{Alphabet}\ [Hil29]. \textbf{alphabétilques}\ [S.73]. \textbf{alphabets}\ [Fri35c, RF35]. \textbf{Alsbalden}\ [Sch20]. \textbf{also}\ [Wal00]. \textbf{Alternating}\ [CG75, Gun88a]. \textbf{Algorithmic}\ [DS83, Has84, HM83, Knu69b, Knu69a, Knu73, QG89, Riv74b, She86, She87, AIR83, AG85, Eve98, Gam88, Mor89, OR5+87, PBGV89, Riv74a, SB84, She88]. \textbf{Algorithms}\ [DS83, Has84, HM83, Knut69b, Knut69a, Knut73, QG89, Riv74b, She86, She87, AIR83, AG85, Eve98, Gam88, Mor89, OR5+87, PBGV89, Riv74a, SB84, She88].
[SK97]. **auffzulosen** [Sch20]. **August** [ACM89a, Gle87, USE88b, USE88a, Wil86b, Wal00]. **Austria** [CSB89, Pie86]. **aut** [Hei76]. **Authenticated** [DS83].

**Authenticating** [Sm87]. **Authentication** [Boo81, BAN89b, CV89, EKW74, GJ82, GL79, IW81, IL83, Kar85, Kar86, Lam81, MRW89, NIS85, Nat85b, NS78b, NS87, NS88, Pvl86, PW86b, PW87b, Lin93, Sid81, Sim85a, St.84, St.85, SNS88, Tsu89, WC81, ALN87b, Ano86a, Ano87c, Ano87d, Ano88j, BAN89a, Chr88, Den84b, Gi881, HHL89, Kaw87, Mer82b, Mi187b, NS78a, OR87, Lin87, Lin88, Lin89, SM83, Spe87, Tho74, Wan86].

**Authenticator** [Dav85]. **authenticators** [FVTS87]. **author** [FF57, Lea87]. **Authority** [MM87].

**Authorization** [GW76]. **Automata** [IEE74, KV89]. **Automated** [Gui76, CR88a]. **Automatic** [AWL88, Hig88f].

**automaton** [Gua87, TC85, TC86].

**Available** [MM87]. **avalanche** [DQD85]. **AVL** [Hol87]. **Award** [Ano82d, Ash87].

**Awards** [Bur81].

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

**Babbage**

[BCKS83, Bro86, SBET85, Vam85, Wor87, BWV88, Fra84, Fra85b, Fra86].

**Back** [Ano85a]. **background** [FM76]. **backup** [Ano87b]. **Bacon** [Lea87, Sar28].

**Bad** [AD81]. **Bahasa** [HS89]. **balance** [Sie83].

**Balancing** [Rab89]. **Ballistica** [Mer44].

**Baltimore** [USE89b, USE89a]. **Bamford** [Ano84a]. **band** [Bur88]. **bank** [Fei70].

**banking** [Per88]. **Banned** [SE86]. **Banquet** [SWT88]. **barbaris** [Hei76]. **bars** [Gyl38].

**baru** [Saw55]. **base** [We60].

**Based** [CR85, EIG85b, Gud80, Has84, HR82, IW81, Mer88, OSS85, Rub79, Sha85, WM85, Ale98, BR88, BS82, BS83, CF78, CR88c, CV89, Dem88, Drie79, EG85a, EIG85a, Gon89, Gro74, IL89, Jon86, Kar89a, Kar89b, KM88, Lan89, LB89a, LB89b, Lei80, Lew78, Lid85, MS76, Mi185, Mit76, MT86, MS83, Nie88, Noh88, PBGV89, Ron84, Sal85, SY86a, SY86b, Sal88, TIF88, YY89]. **Bases** [Ker75, MOV89, VGT88, VGT89].

**Basic** [UU89, Uni70, Dav79, Lag84b, Sha82, Sha84, vda88, Boy86, War82].

**Basic-plus** [War82]. **Batava** [Con39].

**Bateman** [Mul89b].

**battle** [Nor73, Roh77, Mac87, Roh75].

**battles** [Roh77].

**Be** [SE86, Hal79a, McC75, MT72, Nai89].

**Bearlagair** [MS76].

**been** [Bar79a].

**Behaviour** [QSA88].

**Belgium** [QV89, Van87].

**belief** [Gra82].

**Benchmarks** [Est80].

**Berkeley** [ACM86, Gle87].

**Bernardini** [Nis89].

**Bernstein** [WTE85].

**Berücksichtigung** [Kas63].

**besonderer** [Kas63].

**Best** [Fut73].

**Between** [Den86, Bar79b, Sie83, Win74b].

**Beyond** [Joh89, Boy88].

**Biased** [Bhu84].

**Bibliography**

[Lan46, VS41, Vol41, Gal45a, Gal45b, Gal45c, Gal70, Lei79a, Lei79b, Pri83, Shu76].

**Bidirectional** [Gul83].

**bifid** [Bow60a].

**Big** [Cha85b, Cha85c].

**Bijective** [Oka88].

**Binary** [PM78, Bou85, Er89, Vin71, Vin72].

**Biographical** [Kas63].

**Biographies** [Wei88].

**biology** [Sch84].

**bipolar** [Ano78b].

**Birkeroed** [Wor87].

**Birth** [Wel86].

**Birthday** [CN87, GCC88].

**BIT** [Riv79, QG89, Cho86, Per85, Roy86, Tex84].

**bit-slice** [Roy86].

**Bits** [ACGS84, BM82, BM84a, BOCS83, Boy89a, CG85, CG88, KLL88, LW88, BCKS83].

**Black** [Yar31, Yar40, Yar83, Fer87].

**Bletchley** [Goo79, MB86].

**Blind** [Cha83b].

**Block** [Fei74, QG89, Whe87, APW85, CE86, Hor85, Smi74].

**blockcipher** [PBGV89].

**Blocking** [Yun85a].

**board** [Ano78b].

**boat** [Bhe64].

**Bodyguard** [Bro75].

**Bog** [MS76].

**Bog-Latin** [MS76].

**Bombay** [Wel86].

**Book** [Ano82a, Ano84a, Ano85a, Bro86, Fil78, Gin70, HJ85, Dad84].

JL75]. Computational [Sim79b, Mei83].
Computationally [AIR83, Wil82c].
Computations [BOGW88, QSA88].
compute [Per85]. Computer
[Ano78a, Ano82d, Boy88, BK77, BCKS+83, 
Bur81, CR88b, Dav85, EKW74, Fei73, 
Gai80a, Hig88a, IEE79, IEE81, IEE82a, 
IEE82b, IEE84, IEE85, IEE86b, IEE87a, 
IEE88, IEE89, Kar85, Kol77, Kon89, Lau81, 
Lit87, MZS79, Muf88, NIS85, Nat85b, PK79, 
Ran82a, San86, Sny80, Sto89, Sum84, 
Un178a, WTE+85, WW79, Ano88j, Bea72, 
Boy86, Bra75b, CF88, D+83, Dif75, Dre79, 
Fis84, Fis87, GJ79, Goo79, Lev61a, ML87, 
NS78b, Ran82b, SE86, Van69, Bos82, Fey82, 
Hig85, Kah76, NS78a, Sch69, BWV+88].

Computing [ACM82, ACM83, ACM85, ACM86, ACM87, 
ACM88, ACM89a, ACM89c, BIB89, BMV85, 
Bur81, Den79a, Ass88, Cam87, EKG85c, 
Hog88, Odl87a, Pf89, PH78, Sch84, Sch86].
conceal [BB79]. concealability [KL84].
concealed [Lea87]. concept [Des88].
Concepts [Hig88c, Ano84b]. Concerning 
[Ano78a, CSB89, CM82, Fea83, HW76, IEE81, IEE82b, 
IEE87b, IEE88, Ker75, MZS79, RR86, 
SMT+81, San86, USE88c, USE89b, USE89a, 
USE99, Ano87a, Ano88g, EKM88, Had84, 
LLH89, Mor89, Rud82, Un178a]. conferring 
[Bud29, Bud76]. confidentiality [Ple77].
confidentially [Ple75]. Confinement 
[Lam73]. conglogateae [Hei76]. Congress 
[Gle87]. congruence [Plu82]. congruences 
[FHK+88]. congruential 
[Boy89a, Knu80, Knu85, Ree79, Ste87].
conjecture [BSW89, Mul89b].
conjunctions [Hei76]. Connection 
[Kol77, Win78]. Consensus [CMS89].
Consequences [IR89]. Considerations 
[KBD89, Mey73]. Constant 
[BIB89, CMS89]. Constant-Time [CMS89].
Construct [GGM86, CS83, LR88b].
constructing [AB81, IM86]. contain 
[Lea87]. contained [Wal00]. containing 
[Bud76, du44]. contenant [du44].
Continued [Por52, Sha48b]. Continuously 
[MM87]. contracts [EGL85]. Contribution 
[Gyl34]. Contributions [EKM84].
Control [AT83, Bla83, Kar85, MTMA85, 
Pro85, Dat85, Dem88, Gra82, Kar86, O’S88, 
Sal73, San88]. Controlled 
[AWL+88, Gun88a, OM84]. Controlling 
[O’S88, Wei83]. Conventional 
[Dif82a, Mer88]. conversations [Shu82].
convoy [Roh77, Roh75]. coprocessing 
[Van86]. Coprocessor [SK97]. core [GL89].
Corporation [WTE+85]. Correcting 
[SBET85, Mor89]. correction 
[CC81, Kak85, Rao84]. Corrections 
[Ano81a]. correctness 
[Gai77, Gai80c, O’S88]. Correlated [Blu84].
Correlation [Sie84].
Correlation-Immunity [Sie84].
correspondance [S.73]. Corrigendum 
[Vin72]. COST [Muf88, QSA88]. COST-11 
[Muf88]. Council [BBB+81]. counter 
[Wei82b]. counterintelligence [Men89].
coup [Win74b]. Cours [Giv25, Giv32].
Course [Giv78, Kon89, Ano82b, Gle57, 
GPW85, Gle86, Kob87a, Wol43a, Wol43b, 
Wol43c, Wol83]. Covert 
[Gir87, Men89, Mil87a]. crack 
[SW83, RU88]. cracked [MT72]. Cracking 
[Ree79, Hig87a, See89]. craft [Wol70].
creating [KS89]. crime [DB89]. criteria 
[BLS75]. Criterion [McC75]. Critical 
[Her78, Riv79, Roh77]. critique [DH76a].
crittografia [Sac36, Sac47]. crossword [SD86]. crossovers [WW79]. crypt [Pro80, RW84]. crypt-ology [Pro80]. Cryptanalysis [And52, Ano60, Bar61, Bar75, Bar77, Bar79a, Bar84, Bee81, BO88, Cam71, CE86, Daw85, DH77, Fos82, Gai44, Gai56, Kon85, Lev61b, Mac87, MN86, Nob84, Nob85, Nob88, RRM78, SS84, Wil86c, dBB88, And79, And80, Ano39, Ano76, Ano82b, Bia75, BB60, BB67, Bri86, Bri88, CR88b, Cou86, DK85, DDOP85, Elv87, Fri35a, Fri35b, Fri39b, Fri41, Fri42, Fri76c, Fri76b, Fri76d, Fri87, Gai39, Gai40, Gai43, Gai83, Gyl36, Gyl38, HS89, Hit43, Hol55, Kul35, Kul38, Kul67, Kul76, Lev61c, Mil43a, Mil43b, Mil43c, Sim40, Sim66, 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, HeI81]. Cryptanalytical [CR88a]. cryptanalysis [SD86, WW79]. CRYPTO [BC85, Bra90, Wil86b, CF88, Fak87, O'C81, Wil85, CRS83, CY81, 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, BC85, Bry67, CP87, CP88, DLM82, DH80, Dif82b, EMMT78, Fei70, Gif81, GJ82, GMM85, Gun88b, Gyl34, Ham71, Hen81, KV89, KMM+80, Lea87, LT85, MTMA85, MM78, QV89, Ritxx, San88, Ser85, Sha83a, Sie84, Sni83, Uni88a, Van69, VA88, Ano86b, BOCS83, Bla79, Bur88, Com76, CF88, Coh87a, D+83, Erd86, Fei74, FNS75, FF57, FM76, GY58, Gro74, HS85, HFL+85, Her81, HC88, 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, BGG77, BE76, BE79, Bur84a, Bur84b, CG75, Cop87, CM79, Dav81, DB81, Den82, DH76b, Dif88, ECW75, Fei73, Fis84, Fri76c, Gro82, Gud80, GL82, Hel79b, HlI29, HiI31, HuI98, Kon81, LM22, Lau81, Len78, Lev85, Lev86a, Lev86b, Mau14, MM82, Mil66, Mor66, SP89, Sha87, Sha45, SE86, Smi43, Smi44, Smi55, Smi71b, Smi83, Tur41a, Wil82a, dRH+99, AS83, Are21, Are22, BCB88, Bau39, Bau46, BB89, BS82, Bra81, Bus82, Choe86, DK85, Des88, DH76c, Fri76a, Fri76e, Gag88b, Gal88, Ger82, Giv78, Gui76, HHL89, HeI76, Hit43, IL89, vN83, Kil88, Korb87a, Kra86, LS25, LS81, Lee89, Lev61c, MS76, Men39, Mey73, Mic88, Mil43a, Mil43b, Mil43c, ML67, NBS76, Nea75]. cryptography [Per85, Pie77, Pri83, Sac36, Sac47, Sac51, Sac77, Sch84, Sch86, SW61, Shn66, Shn82, SNO72, TP63, Uni42, VS41, Vol41, Wal00, Wei88b, Wei98, Wil82b, Wuo82, dIS02, BCK83+83, Col64, du 44, Kon89, Lei79a, Lei79b, Ano82a, ST89]. Cryptologia [Hig88]. Cryptologist [Ale45, Jou84, Sny79, Sny80]. Cryptology [Cland77, BFW55]. Cryptology [AM85, BC85, Boy86, Bra89b, Bra89a, Cal92, CR83, CP87, Com87, DKMM87, DK+89, Fer87, Gir72, Kah66, Kah79, Kah84, Kon89, Las85, Lem79, LP87, Mars70a, Mar70b, Mei83, NaI89, Por84, QV89, Rug85, She86, She87, She88, Uni79a, Wor75, Bec88, BCI85, Boy88, Bra87b, Bra88, Bra90, CP88, Che73, CRY81,
D\textsuperscript{+83}, Fra89, Fri56, Fri63, Gal45a, Gal45b, Gal45c, Gal70, Gun88b, Jou88, Kah63, Kah82, Kah83, Oak78, Odl87b, Pat87, Pie86, Poma88, Sie83, Sim88, Sin77, Wil86b, van88, Ano82d, Bau82, Lan46, HJH85).
cryptology [Bec97]. cryptomenytics [Wal00]. cryptopak [Com76]. cryptoprocessor [MS83]. cryptoprotocols [Yun85a, Per85]. cryptosystem [CR85, ElG85b, Jun87, WM85, AM88, AM89, ABS1, CR88c, DO86, Eck83, EG85a, ElG85a, GC80, GM85, Gua87, Hel81, Hoo82, HM88, Jun88, Kar89a, Kar89b, Koy82a, Koy82b, Koy83, KM88, Lag84b, LLH89, LB88, LM80, Mei81, Nöb88, Odl84, Sal85, SY86a, SY86b, Sal88, SM83, Sha82, Sha84, SS86, SP79, SW83, SSA87, TC85, TC86, TIF\textsuperscript{+88}, VGT88, Web88, WS79, Yun85b].
cryptosystems [Bla88, BR88, Den84a, GS84, Koy82b, Koy83, LM88, MM83, N¨ob88, Odl84, Pat88, Pat89, SB82, Sim79a, Sim84, SY86a, SY86b, Sal88, SM83, Sha82, Sha84, SS86, SP79, SW83, SSA87, TC85, TC86, TIF\textsuperscript{+88}, VGT88, Web88, WS79, Yun85b].
CTTE [MPS02]. Cuckoo [Sto89]. curiosa [Shu82]. Current [Muf88]. Curve [Kob87b, CL88].
Curves [Mil86, Len87, SX89]. Curzon [Jef86]. custom [She86, She87, She88].
Cyber [LtW88a, LtW88b]. Cycle [MS87, Mas83]. Cyclic [PT89]. Cypher [Bro86, Den68, Fer87, Jef86, RRM78, Wor87, Fra84, Fra85b, Van85].
D [Bv82, Hit43, Cop89]. D. [WTE\textsuperscript{+85}]. DO\textsuperscript{L} [SSA87]. DO\textsuperscript{L}-TO\textsuperscript{L} [SSA87]. D1 [Hig88d]. D4 [Hig88d]. Dabbling [Ritxx]. Dalgarno [Shu82]. Dallas [USE88c]. das [Saw55].
dans [Zaf63]. Dante [Are21]. Data [Ano78a, Ano81b, Ano85b, Ano88d, Ano88e, Bis88b, Bis88d, Bran85a, Bur88, CA81, CA83b, Cia86, DM83, Den79b, DH77, Gai77, Gai80c, Gir71, Guh83, Hig87d, Int79, Int81b, Int84, Int87, Int88, IW81, Jun86, KBN88, Kat77, Ker75, Kra84, Lex76, Mar76, Nat77, NIS85, Nat85b, PT89, Pri80, SB82, Sim79a, Sim84, Tho86, Uni78a, Uni81, YY89, Am83, AL87, Ano80, Ano88i, Bar74, Ber80, Bra75b, Bra79, Cam88, Dat85, Den82, Diff5, Dron89, Fei70, FNS75, Fun78, Gef73, Gir72, Gru84, Hol87, Joh89, Kak83, MM82, Mit76, Mul81, NBS75a, Nat84, Nai89, NS89, O’C81, Pea80, Pri83, Sha88, Smi71a, SN072, Sor80, Tex84, Uni87, UNN83, Uni84, Van86, Wei80, Zef79, Ano78a, Ano88f, Bec82, Bis88a, Bis88c, CA83a, DH76a, EMMT78, Fra85a, Gai80a].
Data [Gai80b, Jue81, Man79, NBS75b, Nat84, Sup88, Uni78a, Uni78b, Uni82c, UNN83, UNN85, Uni84, Uni77, Uni83, Uni88b]. data-bank [Fei70]. data-flow [Sha88].
Database [Ano88f, Ano88e, DW81, GW76, Ano84b, Ano88c]. Datagram [Tsu89].
DBMS [Fai88]. DBS [IEE86a]. DC [BBB\textsuperscript{+81}, IEE82b]. Deavours [SE86].
Debate [BWV\textsuperscript{+88}]. Dec. [Uni79b]. December [Ano88c, IEE88]. deception [Men89]. déciffrissement [Per90, Za63].
Dechiffrierkunst [Kas63]. decifrar [Col64]. Decimal [BD74].
Decipherability [Ryt86, AG84].
Decipherable [BK80]. Deciphered [Ano81a, Rej81, Cla77a, Zor85].
Deciphering [Knu80, Knu85, Col86, Kas63, Zaf63].
Decipherment [Gel74, Man60, Bud76].
decision [Fis84]. deck [Her89]. decoder [Boy88]. decoders [MP86]. decree [Bud29, Bud76]. d’écriture [S.73].
Decrypting [Rub79, Sie85]. Decryption [Hen81, Beh54, Hen82, Per90, Sau99, Uni79b, Wil86c]. Dee [Shu82]. defeat [Lew82].
defies [S86]. Defined [BS86]. definitions [Kah63]. Degenerate [Ber99], degree [Has88]. Degrees [WTE85]. deinde [Hei76]. Demands [Fak87].
Demonstrating [CEvdGP87], demotic [Bud76, Bud29]. d'encres [S.73]. denies [Ano79]. Denmark [Bro86, Wor87].
Denning [Bv82]. Density [LO85].
denudata [Con99]. DEP [FMP85].
Dependence [DQD85], dependency [O'S88], deposits [GBS82], depth [Dat85]. description [Riv86], d'escrire [du 44]. desiderata [Hei76]. Design [Cha86, Flo83, Gud80, Mey73, PW86a, PR85a, SRC84, Sha88, Ayo83, Fak87, FLR77, HL88, KD78, KD97, MM82, MPS02, MT68, PR85b, Smi71a, WT86]. designed [Bur88]. designing [LLH89], designs [Mas89]. destination [Mit89]. destroyer [Uni88a]. Detecting [She86, She87, VV86, She88]. detection [Dem88]. detective [Fut73]. deterioration [Her89]. determination [Bou85].
deutschen [Kas63], developing [MPS02].
Development [AWL88, NS89, Ano78c, Bro81, Kah82, Uni78b]. Developments [Ano88h, AWL88, WTE85, Jur86].
Deviates [Ran55, Ran01]. device [Sha88, Smi71a, Tex84]. devices [Ano87d, Dat85, Spe87]. diagnostic [Sau89].
Dickson [MN86, Nöb88].
Diffusion [AWL88]. digest [Rub82]. Digital [AWL88, Den84a, FMP85, GMR88, Her89, Mat79, MA81, Mer88, Mer89, Oka88, Par85, Ran82b, RSA78, RSA83, Sim85b, Zei79, Ano80, Bar87, Cha79, Cha81, Dem88, Fun78, Lie81, RSA82, Sal78, Sch84, Sch86, Sny79, TC85, TC86, Bur81].
Digitalized [Rab77]. Digits [Ran55, Ran01]. Digraphic [Bow89].
Directions [DH76b]. Directly [MO82].
Dirichlet [BD74]. disaster [Far67, Far69].
Discrete [COS86, EIG85b, Adl87, CEvdGP87, D086, EIG85a, EIG85c, Gam88, Her81, LW88, Odl87a, Per85, RR86].
Discretionary [Kar85, Kar86, Kar87].
discussion [BBR88], disk [Hig89].
Dispersal [Rab89]. dissertation [She86, She87]. distance [Vou80a, Vou80b].
Distributed [ACM89a, BOGW88, Mil87b, RU88, Sat89, MT86]. Distributed-protocol [Mil87b]. Distribution [BBF83, MM78, CM85, Eee85, Kah84, LLH89]. Dits [BCKS83]. Divergence [vTB86]. Divers [S.73]. Divi [Hei76]. Division [Mon85].
divisions [Bar75]. Dkr [Bro86]. Dn [Tri06b, Tri21b], do [BB79, Kos83].
Document [Cop89]. documents [Lew78].
DOE [Bur88]. does [Bra79]. DOL [Tho86].
Donald [Hit83]. Door [IW81, MH78].
Doorbell [Sto65]. Doran [AWL88].
double [Cou86]. Dr. [Ano60]. Draft [Bra75a, CR85]. Dual [NM88]. Duke [Wa100]. Dupont [BBB81], durc [Sch20].
during [Bar79c, Bar79b, Men89]. Dutch [BWV88]. Dvorak [WTE85]. Dynamic [Pro85, Tsu86, WCG86].
dzialan [Kos83].

Editor [Den79b, Mul89b]. Edmonton [ACM89a]. EDP [Ano84b]. eds [AWL88].
Education [BBB+81, Mar70b]. Educators [Gra82]. Edwards [Bur81]. Effects [Beh54]. Efficient [BG58, DGD+85, HGD85, IN89, Kno79, KFB79, OSS85, OR87, Rab89, RT88, VV85, AIR83, ABS1, MI88]. efforts [Gra82].

EFTs [Van87]. Egg [Sto89]. Egyptian [Bud76]. Eighteenth [ACM86]. Eighth [ACM89a]. einem [Sch20]. einiger [Eck82]. Electrical [IEE82b]. Electronic [Ano85b, BW85, HFL+85, Per88, Lin93, Bau39, Bau46, Bau46]. Elliptic [Kob87b, Mil86, CL88, Len87, SX89].

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, Bau46].

Elliptic [Kob87b, Mil86, CL88, Len87, SX89]. Elsevier [Lit87, San86]. elucidation [Wal00]. elusa [Hei76]. Embedding [BCB88, Sha83a]. emc [Ano87a, Ano88g]. emc/rfi [Ano87a, Ano88g]. employed [Col64]. empregados [Col64]. emulates [Ano78a, Ano88g].

Enciphered [Bar79a, Lea87]. Enciphering [Kno79, KFB79, Tuc70]. Encipherment [BM75, BM76, FH74, Kon85, Bar79a, PR85b, Lin87, Lin88, Lin89]. Encrypted [VP888, ALN87a, Ano87b, Ano88i, SSDG81].

Encryption [Ano78a, Ano81b, Ano82c, Ano88f, Aylo68b, Aylo68a, Ayo81, Bar74, BM89, Bec82, Bet88, Bis88a, Bis88b, Bis88c, Bis88d, BG85, Boo81, Bra75a, Bra75b, Bur88, CA81, CA83b, CA83a, sC85, DWK81, Den79b, DB89, DH76a, DH77, EMMT78, FMP85, Fra85a, Gai77, Gai80a, Gai80b, Gai80c, GM84, Gui83, H887, Hig87c, Hig88e, Hoo80, IEE86a, Jue81, KJ77, Kak85, Kal85, Kat77, Kem88, KBD89, Kol77, Lex76, LS89, Ma79, Mar76, MH81, Mer88, Mit76, NBS75a, NBS75b, Nat77, Nat84, NS75b, 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, Ame83, AA80, Ano80, Ano84b, Ano85b, Ano87a, Ano88d, Ano88e, Ano88g, APW85].

encryption [Ayo83, Bar77, Ben88, Ber09, Bis88c, Bis89b, BM84b, Cam88, CF78, Chr88, Chu89, Dat85, Den84b, Die88, Dif75, Dret79, Dro89, Eck85, Fak86, Fal88, Gai78, GY87, Gam88, GMS2, Gol84, Gru87, Hig87b, Hig87d, Hig88a, Hig88f, Hua88, HW88, Int81a, Int79, Int81b, Int84, Int87, Int88, Joh89, Jon86, Kal84, KD78, KD79, KKM82, Kem89, Ker79, Knu80, Knu85, KS89, KL84, Kra84, Kic87, MO78, MS88, MS86, Mil85, Mil81, NM88, NS78a, NU88, NS89, O881, OMS4, ORS87, PP89, Pri80, Rao84, Rec79, RS83, Roy86, Ses81, Sim79b, Sim82b, Sor80, Sup88, Tex84, Van86, Vou80b, Wab87, Wan86, Wat89, Wel80, Wel82b, Wib87, Wil80, Wil86a, YY89, Zfi79, Gab82].

 Ends [SRC84, Ano84b, KYM82, LS89]. End-to-End [SRC84, KYM82, LS89]. enemy [Zor87]. enforcement [LJ75].

engendered [Bla89]. Engine [BCKS+83]. Engineering [Ano88c, Ano88f, Ano88e, 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, WTE85, Ber83, Hod83, Ale45, Ano86c, Ano87a, Ano88g, Ber73, Ber83, Elv87, Gaj89, Gar79, Gar80, Koz84a, Koz84b, Rej77, Rej81, Rejxx, Tur99, WeI82a]. enigmatic [Wal00]. `enigme [Ber73]. Entities [NS88].

Entering [Mor92]. Entropy [EHMS00]. entry [Gai78]. Enumeration [PM78].

Environment [BW85, Bis89a, KS89, Nai89, Pon89, PK79, Lin93, SJ76, SB82, SBC85, Sim79c, TT84a, TT84b, Tho86, Uni78a, Uni78b, Uni87, Uni82c, UNN83, UNN85, Uni84, Uni77, Uni81, Uni83, Uni88b, Yas76, Ame83, AA80, Ano80, Ano84b, Ano85b, Ano87a, Ano88d, Ano88e, Ano88g, APW85].
France fractionating Fourth IEE87a, IEE89, Eck82]. Founding [Kil88].

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

Fourth [IEE88, Rud82]. Fraction [Por52].

fractionating [Fri41]. Fragmentation [Tsu89]. framework [Per85]. Framingham [Ker75]. France [BCI85]. Francis [Lea87].

Francisco [ACM82, Rud82]. Franken [BCKS+83, Bro86, SBET85, Vam85].

französischen [Kas63]. free [PBGV89].

freedom [Sie83]. French [Bau39, Bau46, Kas63, vN83, LS25, Per90, Sac51, Zaf93, diS02, du 44]. Friedman [Cla77a, Cla77b]. Führungsprobleme [Roh75].

Function [IW81, Mer88, Win83, Win84]. Functional [SS89]. Functions [ACGS88, GGM85, GGM86, MRW89, QG89, Sie84, WSC1, WSC2, Yao82b, BM89, GL89, IL89, Lev85, LR88b, NY89b, NY89a].

Fundamental [Knu73]. Funds [BW85, Ano85b, Kem88]. Further [RF35].

Futrelle [BCKS+83]. Future [Woo82, CSB89, Echk85, RIn85].

G [Ano82a, WG82]. G. [BCKS+83].

Gaithersburg [Ano78a, Uni78a]. Galland [lan46].

Gallica [Con39]. Galois [Mul81].

Game [GMW87, Yun85a, See89]. Games [Gar77].

Gardner [AWL+88]. Garland [Lei79a, Lei79b].

Gateways [Tsu89]. gase [Sau89].

Geheime [Sch20]. geheimer [Sch20].

Geheimschriften [Kas63].

Geleitzugschlachten [Roh75]. General [GMT45, Sid81, EKMN84, ISN87, NBWH78, Uni82c].

generalis [Tri90a, Tri21a].

Generalized [Kot85, Adi83, GCC88].

Generals [Bra87a, LSP82, Rei85, Win74b].

Generate [BM82, BM84a, Yao86, Bac88].

generated [Bar84, Plu82]. generating [Er89].

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

Generator [AM85, BE79, FMC85, Boy89a, KM88, Mit76, Par85].

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

gegene [Con39].

geometry [Mil85].

German [AWL+88, Elv87, Lec89, WTE+85, Ale45, Bau82, Cha86b, Eck82, Gab82, Ga89, Kas63, Koz84a, Koz84b, Rej85, Roh75, Uni79b, Win74b].

Germanica [Con39].

Germany [Bet83, Zor87]. get [Bet88].

gewisser [Sch20].

Gewiss [CN87].

Girolamo [Shu82].

Global [IEE87b, San86].

GLOBECOM [IEE87b]. glossary [SW61].

GMD [Bur81].

Godfather [Ran82a].

Godfather [Kah79, Lew78, Per88].

Goldstine [Ano81a, SWT+81].

Goldwasser [Mor88].

Goldwasser-Killian-Atkin [Mor88].

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

Gordon [DG57].

Government [Hig88a, Den86, Fer87, Jef86].

Governmental [Dav81].

Graecia [Con39].

Graecis [Hei76].

grand [Kah82].

grande [Ber73].

graph [NM88].

greater [Lu79, Lu80].

Greatest [Ber83, Cla77b, Lew87].

Greek [Bud29, Bud76].

Group [Bla85, sC85].

Gro74. Bv82, Buc82, DS81, DMS81, Des88, NBWH78, UNN85, Ame81, BB8+81, DB81].

Group-oriented [Des88].

Group-Theoretic [Bla85].

Groups [CG75, DG57, Mas83, SBET85].

Grubb

[Sar28].

Grundlagen [Eck82].

guerre [Ber73].

guess [VGT89].

GUIDE [HR82].

Guidance [Mur87].

Guide [GJ79, CF88, MP86, MM82, Tex64, Uni82b, Uni79b].

Guidelines [Ano81b, Uni81, Bra75a].

Gustavus [Wal00].

H [Ano81a, BCKS+83, SWT+81, SBET85, WG82].

H. [BCKS+83, SWT+81].
juxta [Hei76].


Kernel [LB89a, LB89b, Sch75, Sii83]. Key [AS83, BLP83, BW85, BG85, Boo81, Bur84a, Bur84b, Cha86a, Cha85a, Den84a, Di88, EMMT78, EIG85b, GS84, Hel79b, LS89, Oka88, RSA78, RSA83, SBC85, Smi83, TTT84a, TTT84b, WM85, Wil85, Yun85a, AM88, AM89, Adl83, Ano88d, Bar87, BB79, BM84b, BS83, CM85, Ch086, CR88c, DDOP85, DH76c, Dif82a, EG85a, ElG85a, ECW75, Fra89, Gag88a, GC80, GM85, GS88, Gua87, Gly83, HHL89, HL88, Her78, Hoo82, Hun85, HW88, Kak84, Kar89b, KYM82, KL84, Koy82a, Koy82b, Koy83, Kuc87, Lag84a, LL889, Lak83, LB88, Lom83, Lu79, Lu80, LP87, Mer80, Mer82a, Mer82b, Mic88, Mi85, MN81, Mi84, N888, Nib88, O85a, OR87, PR85a, RN87, RN89, RV79, RSA82, Roy86, Sal85, SY86a, SY86b, Sal88, SM83, Ses81, SS86, SSA87, TC85, TC86, TIF88]. key [Web88, Wie87, Wil82b, WS79, Wil80, Wil86a, Yas76, vTT86]. Key-Link-Pair [Cha86a]. keyless [AS83, Yun85b]. Keys [Blu83b, EHM800, MTA85, MM78, MS87, Ber09, Bla79, BV82, CS83, D88, DMS81, Hig87d, HM88, MM88, S86]. Killian [Mor88]. kind [Gar77]. kinds [SX89].


Lands [Gyl31]. language [MS76, Sal88, Slu82, Wri89]. languages [Kas63, MS76, SSA88, SWT81]. Lapid [Ano88]. Large [AWL88, Ker75, NS78b, Sat89, She88, Hoo80, N87, PST88].

Large-Scale [AWL88]. Lasers [Sch83]. late [MS76]. Latin [MS76]. Latina [Con39]. latter [Gyl38]. iattice [VGT88, VGT89].

Law [CM82]. Lawrence [Ano88].

Laxenburg [CSB89]. Layer [VK84, Nat84, UNN83, Uni84]. Lazy [LB89a, LB89b]. lead [Gra82]. leading [Dat85]. learning [KV89]. least [CG85].

Lecture [WG82]. lectures [Fri63, Ash87].

Lee [Bur81, SWT81, GC80]. Lessons [Ad87, Riv87]. Lett [BV82, Hei81, Mei81].

Letter [MB86, Mul89b]. Level [VK83, Gra82]. levels [Uni82]. Levy [WTE85].

Library [Lei79a, Lei79b, Com76, Sin77]. Libri [Tri18]. libros [Tri06a, Tri21a]. lies [Bro75].


Linear [Hil83, Kot85, Man60, RM85, Boy89a, CE86, FH88, Kmu80, Kmu85, NU88, Plus82, Ste87, Vog85, Zaf63]. linearly [HS85]. Lines [Gua04, Cher88, Kah82].

linguarum [Con39]. Link [CA83b, MOI82].

Linz [Pic86]. lists [Bar75]. Literature [AWL88, Lan46, DAW85, Gal45a, Gal45b, Gal45c, Gal70]. literis [Hei76]. Little [Fil78, Sim04]. Load [Rab89]. Local [IEE81, Kaw87, CV89, Wan86]. Location [Mur87]. Lock [Cha86a, WW84]. Log

Magica [Hei76], magische [Sch20, Sch33], Mail [Lin93, Cha79, Cha81, Mit89, Lin87, Lin88, Lin89, Tho74], Maine [Hau74].

Mainframe [Dav85]. Maintenance [Cha83a, Gai80b, Gai80a]. Majority [GMW87, RBO89], make [Cha85c]. Making [Coo83, Fis84]. Malaysia [HS89], Malcotti [Guo04]. Man [Fil78, Cha77a, Cla77b, Ste76].

Manageable [Fak87]. Management [BW85, EMMT78, LS89, Fak87, KYM82].

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

Manitoba [HW76], manner [du 44].

Manual [AWL+88, Cou86, Hit43, Sac77, Uni40, Uni82a, Wil86c, Sac36, Sac47, Sac51].

Manuale [Sac36, Sac47]. Manuel [Sac51].

Manuscripts [MS76], mapping [FO89, Gab82]. Maratea [AG85], March [Bet83, Roh75, Roh77]. Markers [BBF83].

Market [Per88], markets [Int87, Int88].

Markoff [Hig88d], Markov [Bli84]. Mary [Ano39]. Maryland [Ano78a, Uni78a, USE89b], Marz [Roh75]. Marzolla [Nis89]. Masani [AWL+88].

Maskhutah [Bud76], Massachusets [ACM83]. Massey [WW84]. Master [Bv82, DS81, DMS81, Koy82a, Koy82b, Koy83].

Match [Riv74a], matched [Sor80]. Matching [MM87, AG84]. Math [Mul89b].

Mathematica [Mer44], Mathematical [Ano88h, AWL+88, BD74, Cam71, Fra85a, Gar77, Kon89, Mar70b, Pat87, Por52, Sha45, Sha48a, Sha48b, WTE+85, Eck82, Hof55, Sin66, Sin68a, Sin68b, Wor75]. Mathematicians [Ano81a, Gle87, Rej81, Pat87, Kon89].

Mathematics [HW76, Hel79b, Mul84, RR86].

Mathematiken [Eck82], Matrices [PM78]. Matrix [Lev58, Bou85, Vou80b].

Matsumoto [DDOP85], matter [Ano85a].

Matyas [BCKS+83], Maverick [AWL+88].

Maximin [Bau82], maxims [Bau82].

Maximum [And79, And80], May [ACM82, ACM85, ACM86, ACM87, ACM88, ACM89c, Fëa83, Gun88b, RR86, Uni79b].

Maze [Sto89], McEliece [AM88, AM89, LB88].

McLean [AWL+88]. MD [USE89a]. measure [Hoo80].

Measurement [SB84], Measures [GS84, GS88].

MEBAS [KS89]. Mechanica [Mer44].

Mechanism [Cha86a, GW76].

Mechanisms [Mul88, VK83, VK84, CV89, O’S88].

Medieval [ML67]. Mediterranean [Ben89].

Meetings [WG82], members [Ano39].

Memorandum [Jef86]. Memories [WTE+85].

Memory [LB89a, LB89b].
VK83, Bur88, Dat85, KD78, Tho74].

Networks
[IEE81, Kar85, Mu88, NS78b, PW86a, PW87a, PK79, Ay83, CV89, KD79, Kar86, Mei85, NS78a, NBWH78, Wan86, Wel82b].

Neumann [Ano88]. Nevada [ACM89b].

Newbold [Sar28]. News
[Ano82d, Bur81, Hig88a, Kol77].

Nihil [Hei76].

Nine [Wal00].

Nineteenth [ACM87].

Niv [Ano88i].

Nj [Hig83].

No [Cha86b, Bv82, Hig88a, Ker89, Lu80, Mul89b, RM85, Tuc79a, Tuc79b].

Nominibus [Hei76].

Non [BIB89, BFMM88, Cun89, Dav81, Fel87, Bar75].

Non-Cryptographic [BIB89].

Non-Governmental [Dav81].

Non-homomorphic [Chu89].

Non-Interactive [Fel87, BFM88].

Non-pattern [Bar75].

Non-Cryptographic [BOGW88, Sak89].

Nonlinear [Sie84, TIF88, Web88].

Nonrandomness [KLL88].

Nonsingular [PM78].

Norbert [AWL+88]. Normal
[Ran55, Ran01, MOVW89].

Normandy [Ben80].

Norris [AWL+88].

Norse [ML67].

North [Had84].

North-Holland [Had84].

Notation [BCKS+83].

Note
[BD74, Lam81, Lam73, Wel88a, Vec87, Bv82, CM85, Lei80, Mei81, Mul84].

Notes
[BD74, Por52].

Notice [NSB75b, Uni83].

Notices [Ano82d, Bur81].

Notion
[MRS87, MRS88].

Nov [IEE87b].

Nova [Hei76, Sch20].

Novel [Sto65].

November
[ACM89b, IEE82a, IEE89].

NP
[GG79, VV86].

NP-Completeness [GJ79].

NSA [Ano84a, Un87b].

Number
[BI89, Boy89b, BE79, FM85, Kon89, Plu83, Scl84, Sch86, VV85, CE86, Guy76, Jac87, Kob87a, KM88, Mit76, Per85, Por84, RT88, Sta70, Sta78].

Numbers
[HW75, Bac88, HW79, KL88, Tip27, Vin71, Vin72].

Numerical
[Ano81a, HW76, SWT+81].

Nummis [Mer44].

O [Bro86].

O. [BCKS+83, SBET85].

Oakland [IEE80, IEE83, IEE87c].

Object
[GL79].

Objects
[Bla85].

Oblivious
[Kil88, Rab81].

Obscuras [Col64].

Obscure [Col64].

Observability
[PW86a, PW87a].

Observation
[LB88].

Observations
[Kar89b].

Obsolet [Sha5c].

Obtaining
[RSA78, RSA83, RSA82].

Occult
[Tri06c, Tri21c].

Occulte [Con39].

Oct
[IEE79].

October
[Ano88b, CSB89, HEE76, IEE77, IEE81, IEE84, IEE85, IEE86b, IEE87a, IEE89, MB86].

Off [Ste88].

Office
[IL83].

Official
[Lew78].

Ogham
[MS76].

Oh [Wei88].

Okamoto [VGT88].

Old [Wil82a].

Ole [Van85].

Ology
[Pro80].

Omura
[WW84].

One
[BBB91, Has87, IR89, IL89, IW81, Kno79, KFB79, Lev85, Sed88, Win83, Win84, AIR83, Are22, GL89, HC88, NY89b, NY89a, Sha88, Wal100].

One-Chip
[Ste88].

One-time
[AIR83].

One-Way
[Ir89, IW81, Kno79, KFB79, Win83, Win84, Has87, IL89, Lev85, GL89, NY89b, NY89a, Sha88].

Only
[Sie85].

Ontario
[San86].

Open
[CG87, SNS88].

OpenBSD
[dRHG+99].

Operating
[HUR76, Hoo80, MT86, SII83].

Operation
[AWL+88, CA83a, Nat80, Am83, Far67, Far69].

Operations
[Cal89, Erd86, Gyl81, HT79, HH79, Uni81].

Optimal
[MTMA85, MOVW89].

Optimization
[LTW88a, LTW88b].

Options
[PW86a].

Order
[Boy89a].

Ordered
[CS83].

Orderly
[PM78].

Orders
[Koo86].

Organization
[Kra84].

Organizational
[AWL+88].

Organizations
[Sny80, Sny79].

Organized
[DB89].

Oriented
[Des88].

Origin
[BCKS+83, An87c, Bro81, MS76].

Origins
[Ran82b, Kah84].

Orlando
[IEE88].

Orleans
[IEE74].

Ornithological
[Daw85].

Osborne
[WTE85].

Other
[AWL+88, Den84a, AB81, FF57].

Output
[DQD85].

Outputs
[SK97].

Outstanding
[Jur86].

Overflow
[NBWH78].

Overview
[Den79b, Mat79, Sun84, dRHG+99].
P [Mul89b, Hig88a]. package
[Bis88e, Bis89b, Gru84, Hig87c]. packet
[SSDG81]. Packings [SBET85]. pad
[AIR83]. pages
[Ano84a, Fil78, HJH85, Wor87]. Pair
[Cha86a]. palace
[Ano84a, Bam82]. palace

Palindromic [MS87]. Paper
[Ano82d, Fri35a, Fri35c, Kul83, RF35]. paper
[Ano84a, Bam82].

package

paperback [ST89]. Papers
[Ran82b, CM82, Rud82, AWL88].

papers/Componon [Rud82]. Paradoxical
[GM85]. paradoxical [Hei76]. Parallel
[QSA88, VPS88, PP89, RT88, Sal85].

Parameters [SI76]. Paris [BCI85]. Park
[Hig83, EIE89, MB86]. Part
[Are22, Bur84a, Bur84b, Fri35b, Fri41, Lin87, Lin88, Lin89, Lin93, Vol41, She86, She87].

Partial
[BG85, Cha85a, GM82, PP89, Riv74a].

partial-match [Riv74a]. participants
[Hei76]. Partitioned [GY87]. partitioning
[GY87]. partly [MS76]. Parts [ACGS88].

party [BO85c]. Pascal [APW85]. Pass
[Has84]. Pass-Algorithm [Has84]. passa
[Hei76]. passim [Hei76]. Password
[HHL89, Lam81, Nat85a, RU88, See89, BCW86, Gai78, Sin85]. past [Riv85].

past/future [Riv85]. patents
[Lev83]. Pattern [AG84, Bar75]. Patterson
[Kon89]. payments [Cha83b]. PC
[Bec97, Dea87]. Peapolitani [Hei76]. Pearl
[Far67, Far69]. Pegawai [Saw55]. Pennings
[AWL88]. perfectly [Por84].

Performance
[Lag84b, Beh54, Lom83].

Period
[BE79, Bar79b]. Permutation
[AM85, LM84, KD78, KD79, LR86, Mei85].

Permutations
[IR89, Ayo68b, Ayo68a, Ayo81, Ayo83, Hss87, LR88b, Rej77].

perniciousa [Hei76]. Personal [Ano87d, Den79a, EHMS80, Ste89, Boy86, Win69].

Peter [Hig88b]. Peters [BCKS83]. FGP
[Saw55]. phaenomena [Mer44]. Philippum
[Tri06b, Tri21b]. Physica [Mer44].

Physica-Mathematica [Mer44].

physical

[Nat84, UNN83, Uni84]. Physics
[Ano88c, Ano88f, Ano88e, Ano88h, AWL+88, WTE+85, Fey82, Sch84, Sch86]. Picking
[Hig88a]. picture [SSA88]. Pieprzyk
[ST89]. Pioneer [Ano82d]. Pioneered
[Sny80]. Pioneers [Wei88]. pipeline
[PST88]. placing [She86, She87, She88].

Plaintext
[Khah63, vdAvE86]. plane [Mil85].

platform [Ale98]. Play [GMW87, GM82].

Player [Yun85a]. Playfair [Bow59]. plays
[FF57, Loea87]. Pless [Hua88]. plus
[Ber73, War82]. PN [Von80b]. pneumatica
[Mer44]. Poe [Sau89]. poems [Lea87].

Point [Sin77, Gyl38]. points [HC88]. Poker
[FM85, Yun85a, GM82]. policies [JL75].

Polish
[Ano81a, Dea88, Rej81, Wei86].
polyalphabetic [CR88a, Fri35c, Mit76].

Polygraphia [Hei76]. Polygraphiae
[Tri18]. polygraphic [Cam88]. Polynomial
[KLL88, OSS85, Sll87, Kak83, LR88a, MI88, Sha82, Sha84]. polynomial-time [Sha84].
polynomial-tuples [MI88]. polynomials
[LM84, Ltid85, No88]. Pond [Hau74].

ponderibus [Mer44]. Portland
[IEE85, USE88b, USE88a]. Portrait
[AWL+88]. Portuguese [Col64]. position
[Fri35c, RF35]. Positions [Bur81].
possession [CEvG87]. post [Hei76].

postales [S.73]. potential [Kar87]. pour
[Per90, S.73]. Power [EG85b]. Powerful
[Smi83]. pp [Ano82a, Bro86, Hel81, Hig83, Hig88b, Hig88d, Lei79a, Lei79b, Mei81, Riv79, Shu80a, Shu80b]. practica [Mer44].

Practical
[Ano22, BB60, BB67, Fel87, FS87, Lit87, MP86]. Practice
[Bl83, Hu98, Ser85]. praecipue [Con39].

Pre [Ad87]. Pre-RSA [Ad87].

Precautions [Vin71, Vin72]. predicate
[GL89]. Preliminary [Dif75, CR85, OSS85].

Prentice [ST89]. Prentice-Hall [ST89].

prepared [BB+81]. Presence
[CGMA85]. present [Riv85]. presents
[Tuc79a, Tuc79b]. Press [Man60]. Prevent
[Cha85b]. Price [ST89]. Primality
prime [Kra86, Mor88, BLS75, Mil76, Pol74]. Primer [KP89, Per85, MB86]. Primes [BLS75, Mil76, Pol74]. Principles [Gro82, Kon81, Ano82a]. Principes [Tri06b, Tri21b].

printers [Sch83]. Privacy [Hei76]. Private [Tri06b, Tri21b]. Private-key [RN87, RN89, Mil85]. Private-key [RN87, RN89, Mi85]. prin [Hei76]. Principle [Smith83]. Printing [Ver26]. Pro [Hei76]. probabilistic [BG85, GM82, GM84, Gol84, CG88, Loi80, MRS87, MRS88]. Probability [Tur41a, Gle57, GPW85, Gle86, KP89, VT86]. Probable [McC75, KP89]. Probable-Word-Proof [McC75]. Problem [AT83, BCKS+83, Cal89, CN87, GMR85, LSP82, Lam73, Mau14, Ryt86, Sim83, WM85, Bar79a, Com87, Gai78, Gy78, Jon86, Rei85, Tho74, Vou80b, Wil83b]. Problems [BLS75, Mil76, Pol74]. Procedure [Nat85a, Nat85b, Uni83, NIS85]. Processes [Cal89, CN87, GMR85, LSP82, Lam73, Mau14, Ryt86, Sim83, WM85, Bar79a, Com87, Gai78, Gy78, Jon86, Rei85, Tho74, Vou80b, Wil83b]. 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, BC85, CR83, CS88, CSE88b, CR81, F68a, GM88b, Had84, Mor89, Odl87b, Pic86, Pom86, 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 [Pel60, SWT+81, Boy86, Ste88, War82, BCSK+83]. Programowa [Kos83]. Programs [FH74, KMM+80, Dea87]. Progressions [BD74]. Project [Mu83, Bla75]. projections [Gyl38]. promissa [Hei76]. Proof [BM84b, GMR89, MC75, Fit89]. Proofs [BOGKW88]. Propagation [Pro85]. properties [Chu89]. property [Ale98]. proposal [Rou84]. Proposed [NBS75b, Dif75, DH76a, Mc87]. propositional [Kar89a]. Prospective [Ano88h, AWL+88, WTE+85]. protect [Gef73]. Protecting [EHMS00]. Protection [Chu86a, Coh87b, HUR76, HP87, Hog88, Sal73, Wei88a, Ale98, Ano86b, BP82, Ben80, Bra75b, CF78, CF88, Coh87a, Dif75, NBS75a, SB84, Uni87, Wei89, vAd86]. protein [GY58]. Protocol [BBF83, Blu82, Blu83a, Bra87a, St.93, VT84, E85, Mi87b, Sak89]. Protocols [CCD88, CMS89, DM83, FM85, GMW87, Mer80, Mer82a, Sid81, VK83, Yao82a, BO85a, BO85b, BO85c, Cam87, DL82, D+83, Eve85, Kerm89, RBO89]. Prototype [SBC85, BB89]. Provabel [IR89]. provably [IN89, Sha86]. prove [FS87]. proven [Lea87]. Prover [BOGKW88]. provided [Gyl38]. Providence [ACM85]. provides [Uni87]. Proving [FLR77]. Pseudo [AM85, BM82, BM84a, Boy89b, FHJ+84, Gar82, LR86, Pru83, VV85, Mit76]. Pseudo-Inversen [Gar82]. Pseudo-Random [BM82, BM84a, Boy89b, Pru83, VV85, HJ+84, LR86, Mit76]. pseudoinverses [Gar82]. pseudonym [Ano60]. pseudonyms [Cha79, Cha81]. Pseudoprimes [PSW80]. Pseudorandom [MT72, Por84, Shad83, KM88, Lev85, LR88b, RT88]. Ptolemy [Bud29, Bud76]. PUB [Nat85a, Nat85b, Uni83, NIS85]. Public [BG85, Boo81, Bur84a, Bur84b, CR85, Den84a, DH76c, Di88, El85b, ECW75, GS84, Hei79b, HP87, Kuc87, LP87, Pseudoprimes [PSW80]. Pseudorandom [MT72, Por84, Shad83, KM88, Lev85, LR88b, RT88]. Ptolemy [Bud29, Bud76]. PUB [Nat85a, Nat85b, Uni83, NIS85]. Public [BG85, Boo81, Bur84a, Bur84b, CR85, Den84a, DH76c, Di88, El85b, ECW75, GS84, Hei79b, HP87, Kuc87, LP87,
Public-Key

Publication [Uni83, Wei83]. Publications [Lan46, Oak78, Pri83]. Publishers [Lit87]. Publishing [HJJ85, Had84a, Den84a, Dif88, GS84, Hel79b, Oka88, RSA83, WM85, Wil85, ECW75, LP87, AM88, AM89, Bar87, EG85a, GC80, GS88, Gua87, HHL89, HL88, Her78, Her81, Hoo82, HW88, Kahl79, Kar89b, KL84, Koy82b, Koy83, Lag84a, Lak83, LB88, Mer80, Mer82a, Mer82b, MN81, Mul84, Nöb88, 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].

Publications [Lan46, Oak78, Pri83]. Publishers [Lit87]. Publishing [HJJ85, Had84a, Den84a, Dif88, GS84, Hel79b, Oka88, RSA83, WM85, Wil85, ECW75, LP87, AM88, AM89, Bar87, EG85a, GC80, GS88, Gua87, HHL89, HL88, Her78, Her81, Hoo82, HW88, Kahl79, Kar89b, KL84, Koy82b, Koy83, Lag84a, Lak83, LB88, Mer80, Mer82a, Mer82b, MN81, Mul84, Nöb88, 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].


Ramp [BM85]. Random
Request [Bur81]. requests [NBS75a].

Requirements [FH74, Ano85b, Nat84, Uni7a, UNN83, UNN85, Uni84]. Requiring [EKW74]. Research [Dav81, IEE89, Bla75, Gir71, Jou88].

resource [Ano88j]. Restera [Lec89]. Restraints [Dav81]. Results [BO88, BS67, CM79, Kal85, Muf88, DH85a, JM84, Per85]. Retail [BW85]. Retrieval [CM79, KBD89, Riv74b, Riv74a].

Resource [Ano85b]. Resulting [DEK74]. Requiring [EKW74]. Research [Dav81, IEE89, Bla75, Gir71, Jou88].

reserata [Hei76]. resource [Ano88j]. Restera [Lec89]. Restraints [Dav81]. Results [BO88, BS67, CM79, Kal85, Muf88, DH85a, JM84, Per85]. Retail [BW85]. Retrieval [CM79, KBD89, Riv74b, Riv74a].

Requirements [FH74, Ano85b, Nat84, Uni7a, UNN83, UNN85, Uni84]. Requiring [EKW74]. Research [Dav81, IEE89, Bla75, Gir71, Jou88].


Rune [Hau74]. runic [ML67]. running [Ste88].

S [BCKS83, Lan46, Mul89b, Gu83, WT86]. S-box [Gu83]. S-boxes [WT86]. S.


Science [AWL88, BCKS83, IEE79, IEE82a, IEE84, IEE85, IEE86b, IEE87a, IEE89, Jev74, Lit87, Mil86b, Odl84, OM84, Wil86a].

Schemes [BM85, OSS85, Sha85, Chu89, DO86, IN89, ISN87, MA81, Ple75, Ple77, Rao84, Sha86].

Schimpp [Sch20]. Schlicht [Roh75]. Schneider [Bv82]. School [Den86, Fer87, Jef86]. Schreiben [Sch20, Sch20]. Schreibkunst [Sch20, Sch33]. Schriften [Sch20]. Science [AWL88, BCKS83, IEE79, IEE82a, IEE84, IEE85, IEE86b, IEE87a, IE89, Jev74, Lit87, Mil86b, Odl84, Sha86].

scripta [Con39]. scripti [Put27]. scripturam [Tri06c, Tri21c]. sea [Bee81].

Seal [Far67, Far69]. Sealing [GJ82, Gif81]. Search [BM75, BM76, BCKS83, Jue81, Gu83, Sha86, Sie83]. Seattle [ACM89c].
Seberry [ST89]. Sec’83 [Féa83, Had84]. Sec’84 [San86]. Second [San86, SBET85, HT79, HH79]. secondary [Fri85c, NBWH78, RF35]. Secrecy [EKW74, Sha49, Gif81]. Secret [Ano22, Blu83b, Cha85a, Cha85b, CGMA85, Cla12, Dro89, EHMS00, Fin87, Gin70, Has84, Hig89, Hon19, ISN87, Nan36, Nan74, Nor73, Pie77, Pra39, Ric74, Sea86, Sea56, Sha79, Ste87, TP63, Ver61, Win69, Wol70, Yar40, Yun85a, Ano84a, Ano88a, Bam82, Bro86, Cal80, Fra84, Fra85b, Fra86, GM82, Hig88c, Hig88d, Jac87, Jon78b, Ker89, Laf64, Lan81, Lew78, MS76, Mic88, NU88, Per90, RBO89, Smi43, Smi44, Smi71b, Ste76, Vam85, Win74a, Win74b, Win75, Wor87, Win85, Zim48, Zor87, du 44, Kas63, SBET85]. secret-key [NU88]. Secretdisk [Hig88f]. secr`ete [S.73]. secr`etement [du 44]. secretes [Per90]. Secrets [HJH85, MM87, SDV83, Ted85, Yao86, Hig88a, Ker89, MS81, Rab81]. Section [Den79b, Sin88]. sector [Ano80]. secundum [Hei76]. Secure [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 [ADD891, AM88, AM89, Ano78c, Ber80, BM85, BGK77, Bro81, Cha85c, DM83, Fea83, GJ82, IEE80, IEE83, IEE87c, IEE88, Kol77, Lan89, LHM84, Len78, Lit87, MHS1, Muf88, Pfi89, Pur74, Rab89, RW84, San86, Sat89, Sch83, SS89, Sum84, USE88b, USE88a, VK83, VK84, Ano78a, Ano82c, Ano84b, Ano89, Bar74, Bec97, BOC83, BCW86, Bis89a, BO85a, Bo85b, Bos82, BS82, Cho86, D’83, Den82, Dre79, Dro89, Eve85, Fal88, FLR77, Fis84, GS78, Gon89, HS85, HAd84, HL88, Hef76, Hoo88, Hoo80, JL75, Kak83, KVM82, Ker89, Koc89, LB88, MM82, MRS87, MRS88, Mit76, NBS76, Nat84, Nai89, Pri83, Rou84, Sch75, SP89, Ser85, Sie83, Sil83, Sin85, Ste89, Uni78a, Uni82c, UNN83, UNN85, Uni84, Uni81, Van87, dC87, Ano79, Féa83, Had84, Hig83]. security [ST89]. Security-related [AM88, AM89]. sed [Hei76]. seed [Bou85]. seen [Uni79b]. Seev [Ano88i]. seejao [Col64]. Select [Uni78b]. Selected [Ran82b, CM82]. Selemus [Wal00]. Self [Pro85, Sch86]. self-similarity [Sch86]. Self-Synchronizing [Pro85]. Selfcipher [Pel60]. Selfridge [Mul89b]. semigroups [Eck83]. Seminar [Mar70b, Mar70a]. Seminumerical [Knu69b, Knu69a]. Senate [Uni78b]. Senior [Mar70b, Mar70a]. 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, Vam85, Vou80b]. Serenissimum [Tri06b, Tri21b]. server [St.85]. Service [SS89, SNS88, NBWH78, St.84]. Service [Ano88c, Ano88f, Ano88e, Bur88]. ses [Jos85]. Set [Nea75, WC81, SX89]. seventeenth [ACM85]. Sex [Tri88]. Shakespeare [Are22, FFW55, FF57, Lea87]. Shakespearean [FF57]. Shamir [BB79, SP79, Bar87, Lag84b, Odl84]. Shaped [WTE+85]. Share [Sha79]. Shared [IW81, Fra89]. Sharing [CGMA85, Fin87, BV82, DS81, DMS81, ISN87, MS81, RBO89, Sal73, Wil68a, Wil68b, Wil72, Wil75]. Shelta [MS76]. Shift [Gol67, Gol82, Bar84, Nie88]. shift-register [Bar84]. short [Bud76]. shortcut [Tuc79a, Tuc79b]. Should [SE86, Nai89]. shuffling [NS89]. Shulman [Lei79a, Lei79b]. SIAM [RR86]. sic [Ple75]. Sieve [Sil87, PST88]. signal [Ano82c, Bar87, Eck85]. Signaling [Cla12]. signalling [Hol87]. Signals
Signature
[And86, sC85, Win74b].
Signatures
[Boo81, Den84a, Mat79, MH78, Rab77, RSA78, RSA83, Sim85b, Cha83b, Lie81, RSA82, Sal78, TC85, TC86, dC86, dC87].
signs [S.73].
significant [CG85]. significantibus [Hei76].
signing [EGL85].
similarity [Sch86].

Simoneita [Per90]. Simple
[CMS89, HM83, SBET85, Bar75, Hor85].
simplification [Gui83]. Simplified [RB82].
Simulate [QSA88]. Simulating [Fey82].
Simulation [Ham71, Kal85, KS89, Lau81].
simultaneity [CGMA85, GY87].
simultaneous [Has88]. Singer [IEE84].
Sign [Ano78b, Bar61, BOCS83, Gyl38, Riv80, Tuc70]. Single-board [Ano78b].
single-chip [Riv80]. Singular [MM83].
Sinkov [Cam71]. sive [Con39, Put27]. Six
[BCKS83, Fri63, Gyl38, Wel82a]. size
[Yas76]. skil[l [Uni82a]. skonczonych
[Kos83]. slice [Roy86]. slide [Gyl38]. Small
[DQD85]. Smart [CSB89, McI85]. Society
[Des88, IEE82b, Rud82, Ano82d]. sofic
[Bla89]. Software
[Fak86, HP87, SK97, BE76, DDG+85, Erd86, Gru84, Hig87e, OM84, Rou84].
software-based [Rou84]. Soldier [Uni82a].
Solomon [MS81]. Solution
[AT83, Cha86b, GMR85, Man14, Sed88, Dea88, Fri35c, Gai39, Gai40, Gai43, Gai44, Gai56, Hit43, ReI85, Von80b]. solutions
[Com87, FS87, Tuc79a, Tuc79b, VV86].
solver [Fri76b]. solves [Rou84]. Solving
[Blu82, Blu83a, Has88, LO85, MP86, Rejxx, TIF+88]. solvuntur [Hei76]. Some
[BS86, BS67, FNS75, Gag88b, GS78, HC88, JM84, Lev61a, Lev61b, Lev61c, MN81, Nie88, WS79, Wil85, dC87, DO86, Ecks2, Eve85, FF57, Her78, Hog88, KLL88, Koo86, Riv79, dC86]. sonderlichen [Sch20]. Sons
[Ano82a]. sophisticated [Hor85]. Sorting
[DG57]. Sound [Hon19]. Source
[Blu84, Wil82c]. Sources
[Ano87, Agn88, CG88]. South [RR86].
Space [Ryt86]. Spanheimensis
[Hei76, Tri21b, Tri06b]. spawned [Hor85].
Speaks [Burr]. Special
[Den79b, DB81, Gal88, Sim88, Kas63, MS76]. spécialement [S.73]. specialist [HFL+85]. specialties [Jur86]. Specification [SS89]. Spectral
[Chr78, Gut3]. Spectroscope
[Ano22]. spectrum [Kah84]. Speech
[KJ77, SJ76, BP85, HL87]. Speed
[Lev61a, Sed88, Ano87b, PP89]. Sphere
[SBET85]. Spirit [Hau74]. spirituum
[Hei76]. Sprache [Kas63]. spread [Kah84].

ing [Rud82]. Spy [Sto89, Win89]. spying [Hor85]. square [Bov59, Per85].
staff [Uni78b]. stamp [BO85a, BO85b].
Standard [Ano78a, Ano81b, Ano88f, Bis88b, Bis88d, Bur88, CA81, CA83b, CA83a, Kat77, Nat77, Nat85a, Nat85b, SB82, Uni78a, Ano88e, Bar87, Bet88, Dif75, Hig87b, Ame83, Ano78a, Bec82, Bis88a, Bis88c, Bra75a, DH76a, DH77, EMMT78, Fra85a, Gai77, Gai80a, Gai80b, Gai80c, Gu83, Jue81, Lex76, Ma79, NBS75b, Nat84, Uni78a, Uni78b, Uni87, Uni82c, UNN83, UNN85, Uni84, Uni87, Uni81, Uni83, Uni88b].
Standardization [Kra84]. Standards
[Ano78a, BGK77, Mar76, Uni78a, BS82, Dif75]. Stars [Rus27]. State [Blu84, Sha78].
Statement [Hei76]. States
[Shu80a, Shu80b, Sin77, Uni78b, 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 [Fèa83]. Stokes [BCKS+83]. Stone [Bud22, Bud29, Bud76].
Stones [Hau74]. Storage [CM79, Ano87b]. storage/backup [Ano87b]. Stored [TS88].
Symmetric [AQ98, Sim79c, Sim82b]. symmetry [Fri35c, RF35]. sympathiques [S.73].
Symposium [ACM82, ACM83, ACM85, ACM86, ACM87, ACM88, ACM89a, ACM89c, AWL+88, IEE74, IEE79, IEE80, IEE82a, IEE83, IEE84, IEE85, IEE86b, IEE87a, IEE87c, IEE89].
Synchronizing [Pro85]. Synthese [SB82].
synthesis [GY58]. System [AT&T86, ?]. ARS83, Bur84a, Bur84b, Bur85, DWK81, GW76, Guid80, Hen81, HR82, IL83, LHM84, LB89a, LB89b, Pro85, QSA88, RW84, SRC84, Sat89, SBC85, Smi83, TS88, TT84a, TT84b, ALN87b, BCB88, BCW86, Cho86, Dro89, FLR77, Fei74, Fra89, Fun78, Her81, Lan89, Lei80, Mii85, MPS02, Mul81, MT66, Si83, SNO72, Smi74, Sor80, TIF+88, Van87, Van86, ADDS91, Ber80, KBN88].
System/38 [Ber80]. systèmes [S.73].
Systems [Agn87, Agn88, Cha86a, Cha85a, GMR89, HRU76, KBD89, Kon85, LT85, Mur87, Sha83a, Sha49, SNS88, Ass88, Ver26, Ame83, Bar84, BP82, Bla89, Cha85c, CF88, Dre79, Fri35b, Fri41, FF57, Gen89, Gro74, Hoo80, HW88, La81, Mer82b, MM82, NBW78, Pea80, PR85b, Ses81, Tuc70, Wil68a, Wil68b, Wil72, Wil75, CA83b, CA83a].

T [Mul89b, WG82]. T. [BCKS+83, SBET85]. T0L [SSA87].
Täfelfungen [Gab82]. take [Gar77].
tale [Bro86, Fra84, Fra85b, Van85, Wor87]. Talk [Fil77, Ano39].
Tall [Bud76]. ta’miyah [MTA87]. tampering [Ano79]. tandem [Hei76].
Tanis [Bud76]. tap [OW84].
Tapping [Kah76]. Tar [Rud82]. task [MPS02]. Tassiana [Put27]. Teaching [Fil77].
Technical [Lam81, USE99, Fri35a, Fri35c, Kui35, RF35].
technic [Kos83]. technique [Hol87, NS89].

Techniques
[BCI85, CP87, CP88, Gun88b, QV89, Van69, FNS75, Kem89, Pic86, RS83, Wil86c].
technologies [DB89]. Technology [Ano87d, AWL+88, Gra82, Ano86a, Cam87, Di82b, Gai80a, Rud82, BCKS+83].
Telecommunications [IEE87b, Uni82c].
Telecryptograph [Gua04]. telegram [FM76, Tuc66]. Telegraph [Ver26].
Telegraphic [Gua04]. teleinformatics [GL82].
Telephone [Blu82, Blu83a, Gua04, Hon19, NBWH78].
itelephones [Wab87]. Telephoning [Mea20].
Teletrust [Rih87]. television [Eck85].
telex [FVTS87]. Templars [GB82]. Tem[pl]ars [GB82]. Ten [Dif88, Hel79a]. ter [Muf88].
Terminal [BD74]. terrorism [DB89]. Test [HR82, LT85, AG84]. Testing [Mor88, Eve85, Gai80a, Pol74].
tests [Mil76]. Text [KBD89, PM78, DO86, Int81b, Int84, Int87, Int88]. texts [Bud29, Bud76, Knu87].
Their [Ano88h, AWL+88, WC81, WTE+85, Edw15, Fri35c, Gai39, Gai40, Gai43, Gai44, Gai56, GS78, Jur86, NY89b, NY89a, Odl85, dC87].
Theorem [GMW87, Chu89]. Theorems [BOGW88, Pol74]. Theoretic [Bla85, Gro74, JM84].
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 [Føk86]. thieves [Hor85]. thing [Yas76]. Thinking [BCKS+83, Fut73]. Third [Kah63, RR86].
Thomas [Sea56]. Thompson [SBET85]. Thousands [Fil77]. threat [Ano88a].
Three [Per85, Pon89, WTE+85]. Threshold [Cha85a, Kot85, LLH89]. throughout [Win74b]. Thwarting [Hor85].
tilings [Gab82]. Till [Gyl81]. Time [CMS89, FH74, QSA88, Wil68a, Wil68b, Wil72, Wil75, AIR83, Bra81, EIG85c, Hig88a, Sha82, Sha84, Wal00, YY89].
time-luck [Bra81]. Time-sharing [Wil68a, Wil68b, Wil72, Wil75].
timely [OR87]. Times [Hig88d, NBWH78]. tips [MP86]. tissue [Fun78]. titles [Sin77]. TLP [Bék79]. TMS7500 [Tex84]. TMS75C00 [Tex84]. today [DKKM87, Føk86].
tokens [Spe87]. Tokyo [IEE87b]. Tolerance [Rab89]. Tolerant [BIB89, BOGW88].
tomorrow [DKKM87]. tool [Mic88].
Toolbox [Sac86]. Tools [Die88, Ano86a, DB89].
top [Cal80, Hig88d, Hig88c, Zor87].
top-secret [Zor87]. Topic [Mar70b, Mar70a]. Tore [Riv79].
Toronto [IEE86b, Sen86].
totally [Hel79a]. Tracking [Sto89]. tract [Sim80].
Tractatus [Mer44]. tradeoff [Bra81].
traduzir [Col64]. Traffic [Cal89, Hol87, Uni79b, Wel82b]. trails [Cam87].
Trainer [Uni82b]. Traité [LS25, dLS82].
trans. [LS25, dLS82]. transaction [Cha85c, ADS91]. Transactional [O’N86].
transcendental [KLL88]. Transfer [BW85, Ano85b, Gra82, Kem88, Kil88, Rab81].
Transformation [Hil31, Con76, NM88]. transformations [YY89]. transformed [MOI82].
Translation [Lem79]. translating [Col64]. translations [Bud76].
transmission [Ano88d]. transparent [Hig88f]. Transport [VK84].
Transposition [Fri41, Bar61, Con86]. Trap [IW81, MH78]. Trap-Door [IW81].
Trapdoor [Wil83a, Yao82b, GM85, SM83].
trapdoor-knapsack [SM83]. Trapdoors [Sha83a]. TRASEX [Van87].
Trattati [Alb70]. Treatise [LS81, Tur99, LS25, dLS82]. Treatises [Alb70].
Treaty [Sim79a, Sim84]. tree
[CS83, San88]. Trees
[BM75, BM76, Er89, FHK+84]. trend
[Nai89]. tres [du 44]. tres-subtile [du 44].
Trial [Mon85]. Triangle [IEE89]. trifid
[Bow60b]. Triple [Cla12]. triplex
[Tri06a, Tri21a]. Trithemii [Hei76, Hei76].
Trithemij [Tri06a, Tri06b, Tri21a, Tri21b).
Trithemio [Hei76]. Trithemius
[Shu82, Wal00]. Trojan [Kar87]. Troubled
[Lit87]. truly [Vin71, Vin72]. truncated
[FK+88, HS85]. Trust [Tho84, Tho87].
Trusted [MM87, SK97, BCB88]. Trusting
[Tho84, Tho87]. Trustworthy
[Sim79a, Sim86]. U-boat
[Beh54]. U.S.
[Gr82, Sy79]. ubi [Hei76]. ue [Hei76].
ultimate [Wii86c]. ultra
[Cal80, Mul89a, Be77, Ben78, Ben79, Lew78, Wle86, Win74a, Win74b, Win75, Win89].
ultrasound [Fun78]. unabridged [Kah63].
Unbiased [Bli84, CG88]. Unclassified
[Un87b]. Unconditionally [CC88].
Undergraduate [An82d]. Uniform
[Lie81]. Unique
[LR88a, Ryt86, AG84, VV86]. Uniquely
[BK80]. United
[ST89, Uni78b, Bar79c, Bar79b, Lev83, Sni77, 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, USE90]. Usage
[Nat85a, S.73]. Use [IW81, Sni83, Sor80, WC81, Hit43, K89, Nat84, UNN83, UNN85, Uni84, Wel80, Wel82b]. used
[Bar79a, Ben88, FF57, SX89]. useful
[Yun85b]. Usenix [USE99]. User [EKW74, Has84, PW86a, PW87a, ALN87b, An84b, An86a, CF88, O'S88, OM84, Tex84].
user-controlled [OM84]. users
[An88a, Sni87, Spe87]. Uses
[An22, Edw15, Mii86, An80]. Using
[BBF83, Bir85, Boo81, CM79, KJ77, NS78a, NS78b, PR79, QG89, SK97, SBC85, Sie85, Wan86, AS83, An81b, An87c, Ayo83, Bar75, BM89, Bra75a, BE76, CF78, DG57, Dre79, Er89, HS87, HHL89, HW88, Kak85, Kem89, Koy82a, Mul81, NS89, Ok88, PR85a, PP89, Uni82c, Uni81, Vou80b]. ut
[Hei76]. utility [Sup88].
V [Bud29, Bud76, Bra79]. vacuum [Zor87].
vacuum-tube [Zor87]. Validating
[Gail77, Gai80c]. Validation [Has84].
valuable [Uni87]. Value [MM83, Eve98].
value-adding [Eve98]. Valves [BCKS+83].
Variable [Lev58]. variables
[FK+88, HS85]. Variants [IS84].
variations [An87a, An88, dC87].
varieties [TC86]. V¨arldskriget [Gyl31].
Vehicle [Mur87]. verbis [Hei76].
verbogene [Sch20]. verborgens [Sch20].
Verfahren [Bau82]. verifiability [BO85c].
Verifiable [CGMA85, Fel87, RBO89].
verification
[KYM82, Kem89, MI88, Sili83, WCGW86]. verified [SSDG81]. Verify [Sim79a, Sim84].
Verifying [ALN87b]. Vernam [Tuc70].
Verschlüsselungsabbildungen [Gab82].
version [OSS85]. versions [CM82]. versus [Dif82a, Fak86]. verwandter [SB82]. Very [Ker75, She88, du 44]. via [Cam87]. Vienna [EKM84]. view [Bel77, Gyl38]. viewpoint [Gra2, Gyl36]. Vigenère [Tuc70]. VILL [Ric74, HJH85, Hig83]. vindicata [Hei76].

vindicato [Hei76]. viruses [Ano88a]. Visible [Hon19]. VLSI [Mas89, ORS+87, She86, She87, She88, Wat89]. vnd [Sch20]. vne [du 44]. vnd [Sch20, Sch33].


Vol [Lei79a, Lei79b]. voluntatem [Tri06c, Tri21c]. vs [Jue81]. vulnerable [Hig88d].

W [BCKS+83, WTE+85, Kos83]. W. [SE86, WTE+85]. wa [MTA87].

wa-istikhrjaj [MTA87]. Wagstaff [Mul89b].

War [AWL+88, Bar79a, Cla77a, Elv87, Jon78a, Koz84a, Koz4b, Men89, WTE+85, Win74h, Bee81, Ber83, Gar79, Gar80, Jon78a, Lew78, Ste76, Uni79b, Gyl31, Gyl34, HT79, HH79, SBET85]. warfare [Men89, Nor73]. Wars [Bar79b, Den86].

Was [AWL+88, Koz84b, WTE+85, Koz84a].

Washington [ACM89c, BBB81, IEE82b]. watch [Ano87d]. Waterman [BCKS+83].

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

watermarks [Est80]. Waveform [KJ77].


weaknesses [She86, She87, She88]. weapon [Bel77]. Web [Ale98].

Weber [Shu80a, Shu80b]. Webster [Kah63].

Wednesday [IEE86a, Mur87]. Weiss [Ano88]. Welchman [BCKS+83]. West [Sin77, Ben80]. Wexelblat [SWT+81]. WG [CS89]. whatever [Col64]. wheels [Gyl38].

where [Bar79a]. wherein [Lea87, Wal00].

Who [Fil78, Cla77a, Cla77b]. Whoes [Hor85]. Wide [Ale98, Bur88]. and [Sch20].

Wiener [AWL+88]. Wiley [Ano82a]. will [Hei79a]. William [Bar28, Ano39, FF57, Lea87]. Williams [KL84]. Wire [OW84, Ver62]. Wire-tap [OW84]. within [Hei79a]. Without [Mon85, PW86a, PW87a, Bla85, Cha85c, CEvdGP87, SDV83, Wil83]. with [See89].

Wizard [Jon78a]. Wolfe [Sto66]. woln [Sch20]. Word [BS86, BO85d, McC75, WM85, Bar75, Ben88, Eve85, Smi87].

WordPerfect [Ben88]. words [AG85]. Work [Goo79]. working [BB89].

Works [AWL+88]. Workshop [Bet83, BCI85, BG77, CP87, CP88, Gun88b, QV89, USE88a, USE88b, Hei76, NBS76, Pie66].

Workstations [NS88]. World [AWL+88, HT79, HH79, Ritxx, SBET85, WTE+85, Cla77a, Ale98, Bar79c, Bar79b, Cla77a, Elv87, Gyl31, Gyl34, Koz84a, Koz84b, Lew78, Lit87, Men89, Win74b].

worldwide [Int87, Int88]. Worthy [AWL+88]. would [Gar77]. Writing [Gel74, Hul98, Kah67a, Kah96, Kas63, Laf64, Nan36, Nan74, Ric74, Sea86, Smi43, Smi44, Smi55, Smi71b, Wol70, Zim48, du 44, Gin70]. writings [Col64, Lan81, Per90]. wrong [HM88].

wrote [FF57]. WW [Pli98]. Wyner [Kal84, Kal85].

X.509 [Cop89]. X3 [ML87]. X.9.23 [AA88].

xiv [Ano82a]. xvi [Lei79a, Lei79b]. xviii [Shu80a, Shu80b].

year [Dif82b, Hei79a]. Years [BCKS+83, Dif88, Ash87, Gar77]. Yehezkel [Ano88]. yesterday [DKK88].

York [ACM87, Ano82a, HJH85, Hig88d, Lea79a, Lei79b, MZS79, Sin77]. York/London [Lei79a, Lei79b]. yourself [FS87].
REFERENCES


References


REFERENCES


REFERENCES


REFERENCES


REFERENCES

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


Anonymous:1960:CNH


Anonymous:1976:CCA


Anonymous:1978:CSD


Anonymous:1978:NPAd


Anonymous:1978:ODA


Anonymous:1979:SSA


Anonymous:1980:ACS


Anonymous:1981:CHP

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


Anonymous:1985:BM


Anonymous:1987:TWP


Anonymous:1988:BRCb


Anonymous:1988:CCJc


Anonymous:1988:CCJb


Anonymous:1988:DEK


Anonymous:1988:DESb


Anonymous:1988:DESf

REFERENCES


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


REFERENCES


REFERENCES


Birnbaum:1986:VPS


Beardsley:1972:YCI


Becker:1982:EDE

REFERENCES

Beckett:1988:IC


Beckett:1997:ICP


Beesly:1981:CIW


Behrens:1954:EUP


Bell:1977:IVU

[Bel77] Ernest L. Bell. *An initial view of Ultra as an American weapon*.

Bennett:1980:UWN


Bennett:1988:AEA


Bennett:1989:UMS


Bertrand:1973:EOP


Berstis:1980:SPD

[Ber80] Viktors Berstis. Security and protection of data in the IBM
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

Bishop:1989:FEP


Book:1980:UDC


Blatman:1975:MMC


Blakley:1979:SCK


Blakley:1985:ITF


Blandman:1989:CSS


Blahut:1983:TPE


Blinch:1989:CSS


Brickell:1983:EAA
REFERENCES


REFERENCES

Blum:1982:HGC


Blum:1984:HGC


Boyer:1984:PCR


Blakley:1985:SRS


Beale:1989:EUR


Blake:1985:CLG

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.


Brickell:1988:CSR


Ben-Or:1983:CSS


Ben-Or:1988:MIP


Ben-Or:1988:CTN

REFERENCES

Bond:1947:FSC

Booth:1981:ASU

Bosworth:1982:CCC

Bounas:1985:DDS

Bowers:1959:DSP

Bowers:1960:BC

Bowers:1960:TC

Boyd:1986:CPC

Boyd:1988:CCB

Boyar:1989:ISPb
REFERENCES


REFERENCES


Brickell:1985:BIK


Brickell:1986:CKC


Brickell:1988:CKC


Brown:1975:BL


Brownell:1981:ODN


Brooke:1986:BRB

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. 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**
REFERENCES


Burnham:1988:DES


Brouwer:1982:NMK


Beker:1985:KMS


Buchholz:1988:CQDc


CBEMA:1981:ANS

REFERENCES

CBEMA:1983:ANSb


CBEMA:1983:ANSa


Calvocoressi:1980:TSU


Callimahos:1992:HC


Campagne:1971:REC


Campbell:1987:MBC


Cammack:1988:MDE

REFERENCES

Clark:1981:ECC


Chaum:1988:MUS


Coppersmith:1985:AF


Chaum:1986:CRN


Chaum:1987:DPD


Chaum:1978:ICP


Christoffersson:1988:CUH


Coppersmith:1975:GCA


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

REFERENCES

Chang:1986:DKL


Chapman:1986:NFS


Chesson:1973:CC


Chor:1986:TIP


Christoffersson:1988:MAE


Chuang:1989:NES


Ciarcia:1986:BHD


Chan:1988:IEC


Claudy:1912:TMS


REFERENCES


Cohen:1987:CCI


Cohen:1987:IIP


Colaco:1864:CRO

[Col64] F. N. Colaço. A cryptographia revelada, ou, Arte de traduzir e decifrar as escrituras obscuras, quases que sejão 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.

CPI:1976:CMS


Cominsky:1987:CAP


Conradi:1739:CDS


Coombs:1983:MC


Coppersmith:1984:FEL

[Cop84] D. Coppersmith. Fast evaluations of logarithms in fields of characteristic two. IEEE Transactions on Information Theory,
Coppersmith:1987:C


Coppersmith:1989:AID


Coppersmith:1986:DL


Courville:1986:MCC


Chaum:1987:ACE


Chor:1985:KTP

Benny Chor and Ronald L. Rivest. A knapsack type public key cryptosystem based on arithmetic in finite fields (preliminary draft). In Blakley and Chaum [BC85], pages 54–65.
REFERENCES


Carroll:1988:ACP


Carroll:1988:CC


Chor:1988:KTP


Chaum:1983:ACP


Crypto:1981:ACP


Cesarini:1983:ACC


Chaum:1989:SCF

Ciminiera:1989:AMM


DeMillo:1983:ACC


David:1985:MMA


Davida:1979:IHS


Davida:1981:CAR

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

Davies:1985:MAA

REFERENCES


REFERENCES


REFERENCES


REFERENCES


[Dre] Felix F. Dreher. Privacy and security in computer based systems using encryption. Pittsburgh State University. School of Business monograph series 7, Pittsburgh State University. Gladys A. Kelce School of
REFERENCES


Robert Scott Elvin. A crypt-
analysis of the World War II German Enigma cipher machine. Thesis (M.Sc.C.S.), University of New Brunswick, Ottawa, ON, Canada, 1987. 2 microfiches (104 fr.).


REFERENCES


REFERENCES


org/download/cryptolog_38/cryptolog_38.pdf. Reprint of [Fil77].

**Fisher:1984:CCS**


**Fitzgerald:1989:QIP**


**Flowers:1983:DC**


**Feiertag:1977:PMS**


**Friedman:1976:ZTJ**


**Fortune:1985:PP**


**Fairfield:1985:LRN**

R. C. Fairfield, R. L. Mortenson, and K. B. Coulthart. An LSI random number generator (RNG). In Blakley and Chaum
REFERENCES


[FNS75]


[Fla89]


[Fos82]


[Fra84]

Ole Immanuel Franksen. Mr. Babbage’s secret: the tale of a cypher and APL. Strandberg, Birkerod, Denmark, 1984. ISBN
REFERENCES


Franklin:1985:MID

Franksen:1985:MBS

Franksen:1986:SHM

Frankel:1989:TIC

Friedman:1935:ICA

Friedman:1935:MCP

Friedman:1935:PIS

Friedman:1939:CAC
William F. (William Frederick) Friedman. The cryptanalyst accepts a challenge. War Department, Office of the Chief Signal Officer, Washington, DC, USA, 1939. 24–36 pp. LCCN ????.

Friedman:1939:MC
REFERENCES

Friedman:1941:MCP

Friedman:1942:MC

Friedman:1956:CCC

Friedman:1963:SLC

Friedman:1976:AMC

Friedman:1976:CEC

Friedman:1976:CCA

Friedman:1976:EC

Friedman:1976:EMC

Friedman:1987:ICA
William F. (William Frederick) Friedman. The index of coincidence and its applications in...
REFERENCES


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


REFERENCES


Gaines:1939: ECS


Gaines:1940: ECS


Gaines:1943: ECS


Gaines:1944:CSC


Gaines:1956:CSC


Gait:1977:VCH


Gait:1978:EEP


Gait:1980:CST


Gait:1980:MTD

[Gai80b] Jason Gait. Maintenance testing for the Data Encryption
REFERENCES


[GB82] 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


**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**

**Gifford:1981:CSI**
David K. Gifford. Cryptographic scaling for information...
REFERENCES


**[Gin70]**


**[Gir71]**


**[Gir72]**


**[Gir87]**


**[Gij25]**


**[Giv32]**


**[Giv78]**


**[Garey:1979:CIG]**


**[Gifford:1982:CSI]**


**[Gligor:1979:OMA]**

V. D. Gligor and B. G. Lindsay. Object migration and authentication. *IEEE Transactions on
REFERENCES


Guillou:1982:CT


Goldreich:1989:HCP


Gleason:1986:ECP


Gleason:1987:PIC


Goldwasser:1982:PEH


Goldwasser:1984:PE


Goodman:1985:NTK

R. M. F. Goodman and A. J. McAuley. A new trapdoor knap-


REFERENCES

QA267.5.S4 G6 1982. Portions co-authored with Lloyd R.
Welch, Richard M. Goldstein,
and Alfred W. Hales.

Goldwasser:1984:PET

Shafrira Goldwasser. Probabilistic encryption: theory and
applications. Thesis (Ph. D.
in Computer Science), Depart-
ment of Computer Science, Uni-
versity of California, Berkeley,
Berkeley, CA, USA, December

Gong:1989:SCB

Li Gong. On security in
capability-based systems. Op-
erating Systems Review, 23(2):
56–60, April 1989. CODEN OS-
RED8. ISSN 0163-5980.

Good:1979:EWC

I. J. Good. Early work
on computers at Bletchley:
Annals of the History of
Computing, 1(1):38–48, July/
September 1979. CODEN AH-
COE5. ISSN 0164-1239. URL
http://dlib.computer.org/
an/books/an1979/pdf/a1038.
pdf; http://www.computer.
org/annals/an1979/a1038abs.
htm.

Gordon:1985:SPE

John A. Gordon. Strong primes
are easy to find. In Beth et al.
[BCI85], pages 216–223. CO-
DEN LNCSD9. ISBN 0-387-
16076-0 (USA). ISSN 0302-
9743 (print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
E951 1984. URL http://
link.springer-ny.com/link/
service/series/0558/tocs/
t0209.htm; http://www.springerlink.
com/openurl.asp?genre=issue&
issn=0302-9743&volume=209.
Held at the University of Paris,
Sorbonne.

Gleason:1985:ECP

Andrew M. Gleason, Walter F.
Penney, and Ronald E. Wyllys.
Elementary course in probabil-
ity for the cryptanalyst, vol-
ume 41 of A Cryptographic se-
ries. Aegean Park Press, La-
guna Hills, CA, USA, revised
072-7. ??? pp. LCCN Z104

Gray:1982:ICT

P. E. Gray. Information control
I: Technology transfer at issue:
The academic viewpoint: Edu-
cators believe efforts to limit
transfer of knowledge at the
university level are likely to
weaken the U.S. lead in inno-
vation. IEEE Spectrum, 19
(5):64–68, May 1982. CO-
DEN IEESAM. ISSN 0018-9235
(print), 1939-9340 (electronic).

Grossman:1974:GTR

E. Grossman. Group theoretic
remarks on cryptographic sys-
tems based on two types of addi-
tion. Research Report RC-4742,
IBM T. J. Watson Research
Center, Yorktown Heights, NY,
USA, February 26, 1974.
REFERENCES

ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://
comjnl.oxfordjournals.org/content/25/3/400-c.full.pdf+
hmtl.

data encryption hardware software
package. Project (M.S.), California State University,


(print), 1095-7111 (electronic). Special issue on cryptography.


ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1702757.

REFERENCES

SCNEBK. ISSN 0036-8423 (print), 1943-0930 (electronic).

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 protein synthesis. In Das Universum. Unser Bild vom Weltall. (German) [The Universe. Our picture of the Universe], page 442-450, Wiesbaden, Germany, 1958.

Galil:1987:PEA
Zvi Galil and Moti Yung. Partitioned encryption and achie-

**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 Gyldén. *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**


**Haskett:1984:PAU**

James A. Haskett. Pass-algorithms: a user validation

Haastad:1987:OWP


Haastad:1988:SSM


Haugen:1974:RSS


Huang:1988:SWP


Heidel:1676:JTP

[Wolfgang Erneuto Heidel. Johannes Trithemii 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 explicantur conjurationes spirituum ex Arabicis, Hebraicis, Chaldaicis & Graecis spirituum nominibus juxta quosdam conglobatae, aut secundum alios ex barbaris & nihil significantibus verbis concinnatae: deinde solvuntur & exhibentur artificia nova steganographica a Trithemio in literis ad Arnoldum Bostium & Polygraphia promissa, in hunc diem a nemine capta, sed pro para
REFERENCES


REFERENCES

Hersch:1989:DSA


Hardy:1985:ECC


Hoornaert:1985:EHI


Hinsley:1979:BISb


Harn:1989:PAU


Higenbottam:1973:CC


Highland:1983:BRCb

[Hig83] Harold Joseph Highland. Book review: Codes, ciphers and


Highland:1987:CC

Highland:1987:DES


[High87a]


[Hig87e]

Highland:1987:HEM

[High87b]


[Hig88a]

Highland:1988:PEM

[High87c]


[Hig88b]

Highland:1988:RRC

Esther H. Highland. A redundancy reducing cipher: Pe-
REFERENCES

Highland:1988:TSC


Highland:1988:TSV


Highland:1988:EAE


Highland:1988:SIT


Highland:1989:SDI


Hill:1929:CAA


Hill:1931:CCL

REFERENCES

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

**Hitt:1943:MSM**


**HJH:1985:BRK**


**He:1988:SDK**


**Hunter:1983:ERA**


**Hode:1988:RCW**


**Hodges:1983:ATE**


**Hoffer:1955:MAC**


**Hogan:1988:PIS**


**Hollis:1987:TCA**

REFERENCES

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

proceedings/stoc/22145/p356-
 hastad/p356-hastad.pdf;
http://www.acm.org/pubs/citations/
proceedings/stoc/22145/p356-
 hastad/. ACM order no. 508850.

Hammer:1987:EUM


Hardjono:1989:TCE


Hinsley:1979:BISa


Huang:1988:APE


Hulme:1898:CHP


Hunter:1985:ARK

REFERENCES


[IEEE82a] IEEE, editor. *23rd annual Symposium on Foundations of Com-
REFERENCES


REFERENCES


Imai:1986:AMC


Impagliazzo:1989:ECS


IRD:1981:DVE


IRD:1984:DTV


IRD:1987:DTV


IRD:1988:DTV


Impagliazzo:1989:LPC

[IR89] R. Impagliazzo and S. Rudich. Limits on the provable consequences of one-way permu-
REFERENCES

Ito:1987:SSS

Jurbensen:1984:SRI

Johnson:1989:BDC

Jones:1975:ESP

Jones:1978:WWB

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


Jon86    John W. Jones. Data encryption based on the logarithm problem. Thesis (M.A.Sc.), University of Ottawa, Ottawa, ON, Canada, 1986. 2 microfiches (103 fr.).

Josse:1885:CSA

Josse:1885:CSA


JCryptology:1988:JCI


Juenemann:1981:DES


Jung:1987:IRC


Jung:1988:IRC


Jurgen:1986:SEI


Kahn:1966:MC

REFERENCES

Kahn:1967:CSSa


Kahn:1967:CSSb


Kahn:1974:C


Kahn:1976:TC


Kahn:1979:CGP


Kahn:1982:GLC


Kahn:1983:KCS


Kahn:1984:COS


Kahn:1996:CSS


Kak:1983:EMP

REFERENCES

346, October 1983. CODEN IJ-CIAH. ISSN 0091-7036.


REFERENCES


[Kasiski:1863:GDG] Friedrich Wilhelm Kasiski. *Die Geheimschriften und die Dechiffrierkunst, 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 ????


REFERENCES

Kam:1979:SDS


Kemp:1988:EEF


Kemmerer:1989:AEP


Kerr:1989:SNM


KFB79]


Kil88]


Kak:1977:SEU

Kothari:1984:CMW


Kannan:1988:PFN


Kurosawa:1988:CSP


Konheim:1980:ICP


Knuth:1979:AEO


Knuth:1969:SNM


Knuth:1969:SA


Knuth:1973:FA

REFERENCES

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

[Knuth:1985:DLC]

[Knuth:1987:CT]

[Koblitz:1987:CNT]

[Koblitz:1987:ECC]

[Kochanski:1989:HSI]

[Kolata:1977:NCC]


[Konheim:1985:CAE]
REFERENCES

339. 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.

Konheim:1989:RMC


Koopman:1986:OES


Koscielny:1983:PRD


Kothari:1985:GLT


Koyama:1982:CUM

[Koy82a] Kenji Koyama. A cryptosystem using the master key for multi-address communication.
REFERENCES


Koyama:1982:MKR


Koyama:1983:MKR


Kozaczuk:1984:EHGa


Kozaczuk:1984:EHGb


Kim:1989:PRP


Krause:1984:DEI


Kranakis:1986:PC


Kordes:1989:UMC

F. L. G. Kordes and J. J. Schuurman. The use of MEBAS in creating a simulation environment for compression and encryption. Report NLR


REFERENCES


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

[Lau81] Rudolph F. Lauer. Computer simulation of classical substitution cryptographic systems, vol-
REFERENCES


REFERENCES

Leiss:1980:NSS


Lempel:1979:CT


Lennon:1978:CAI


Lenstra:1987:FIE


Levine:1958:VMS


Levine:1961:SAH


Levine:1961:SECa


Levine:1961:SECb


Levine:1983:USC


Levin:1985:OWF

REFERENCES

76.6 A13 1985. URL http://www.acm.org/pubs/articles/proceedings/stoc/22145/p363-
lemi/p363-lemi.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/22145/p363-
lemi/. ACM order no. 508850.

Lewin:1978:UGW


Lewin:1982:AMC


Lexar:1976:END


Landwehr:1984:SMM


Lidl:1985:CBP


Lieberherr:1981:UCD


RFC0989


RFC1040

J. Linn. RFC 1040: Privacy enhancement for Internet electronic mail: Part I:


REFERENCES

Luccio:1980:CMC


Lidl:1984:PPR


Leighton:1985:HBC


Lagarias:1985:SLD


Lomet:1983:HPU


Luciano:1987:CCC


Luby:1986:PRP


Lange:1981:TC

Lu:1989:SCI

Lamport:1982:BGP
Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, July 1982. CO-DEN 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 unforge-
able 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.


Mandelbrot:1960:BRJa


Marsh:1970:CSS


Marsh:1970:MEC


Marion:1976:ANB


Massey:1983:LFC


Mastrovito:1989:VDM

REFERENCES

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

Matyas:1979:DSO

Mauborgne:1914:APC

Milner-Barry:1986:ADL

McCarty:1975:AFP

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

Meijer:1985:MEN
Henk Meijer. Multiplication-permutation encryption net-

**Mendelsohn:1939:CC**


**Mendelsohn:1989:CWI**


**Mersenne:1644:CPM**

[Mer44] Marin Mersenne. *Cogitata Physica-Mathematica ... Tractatus de mensuris ponderibus atque nummis ... Hydraulica pneumatica; arsque navigandi. Harmonia theorica, practica. Et Mechanica phaenomena. Ballistica et acontismologia*. Antonii Bertier, Paris, France, April 1, 1644. [30], 40 [24], 41–370, [16], 96, [8], 138, [34] + 40 pp. URL http://www.mersenne.org/prime.htm; http://www.mersenne.org/status.htm. Three volumes. This is the book that introduced the conjecture that numbers of the form $M(n) = 2^n - 1$ are prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127,$ and 257, but could not test this claim. Euler showed in 1750 that $M(31)$ is prime. Lucas showed in 1876 that $M(127)$ is prime. Pervouchine showed in 1883 that $M(61)$ is prime, finally disproving the Mersenne conjecture. Powers in the early 1900s showed that $M(89)$ and $M(107)$ are prime, both missed by Mersenne. By 1947, it was known that the correct list is $2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$ and 127, so Mersenne had five errors in his list: 67 and 257 should have been removed, and 61, 89, and 107 added. By late 2001, 39 Mersenne primes were known, the five largest having been found by 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:1982:SAP


Merkle:1988:DSB


Merkle:1989:CDS


Meyer:1973:DCC


Merkle:1978:HIS


Merkle:1981:SME


Matsumoto:1988:PQP

REFERENCES


**Michener:1988:TSK**


**[Mil85]**

**Millikin:1943:ECCa**


**[Mil86]**

**Millikin:1943:ECCb**


**[Mil87a]**

**Millikin:1943:ECCc**


**[Mil76]**

**Miller:1976:RHT**


**[Mil85]**

**Millen:1987:CCC**


**[Mil86]**


**[Mil87a]**

REFERENCES


Monge:1967:NMC

Maulucci:1987:HAC

Matyas:1978:GDI

Meyer:1982:CND
REFERENCES

Moler:1983:SVA

Meadows:1987:MSA

Muller:1981:SRP

Muller:1986:CDS

Matsumoto:1982:DTL

Montgomery:1985:MMT

Morland:1666:NMC

Morrice:1692:EB

Morrison:1983:SEA
D. R. Morrison. Subtractive encryptors: alternatives to the
REFERENCES


Silvio Micali, Charles Rackoff, and Bob Sloan. The notion of security for probabilistic cryptosystems. SIAM Jour-
REFERENCES


REFERENCES


REFERENCES

[102x681] 140


Mulligan:1989:UMA


Mullin:1989:LEN


Muraszko:1987:CVR


Merwin:1979:NCC


Naik:1989:CDS


Nanovic:1936:SWI


Nanovic:1974:SWI

REFERENCES

NBS:1977:DES

Data Encryption Standard. 
U. S. Department of Commerce, 

NBS:1980:MO

DES Modes of Operation. 
U. S. Department of Commerce, 

NCSOTS:1984:ISR


NIST:1985:FPSa


NIST:1985:FPSb


NBS:1975:EAC

[ NBS75a ] NBS. Encryption algorithm for computer data protection: requests for comments. Federal Register, 40(?):12134–??, March 17, 1975. CODEN FEREAC. ISSN 0097-6326.

NBS:1975:NPF

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

NBS:1976:NWC


Nilsson:1978:OST

REFERENCES


REFERENCES


REFERENCES

Oakley:1978:RPC


O'Connell:1981:CDE


Odlyzko:1984:CAM


Odlyzko:1987:CCD


Odlyzko:1987:ACC

REFERENCES


H. Ong, C. P. Schnorr, and A. Shamir. Efficient signature schemes based on polynomial equations (preliminary version). In Blakley and Chaum
REFERENCES


Ozarow:1984:WTC


Parthasarathy:1985:DSG


Patterson:1987:MCC


Preneel:1989:CHB


Pearcey:1980:EDS


Pelta:1960:SP


Perret:1890:RCS

[P. M. Perret. Les règles de Cicco Simonetta pour le déchiffrement des écritures secrètes (4 juillet 1474). (French) [the rules
REFERENCES


Peralta:1985:TRN


Perry:1988:EBG


Pfleeger:1989:SC


Pohlig:1978:IAC


Pichler:1986:ACE


Pierce:1977:SSP


Popek:1979:ESC

Pless:1975:ESC


Pless:1977:ESC


Plimmer:1998:MIW


Plumstead:1982:ISG


Plumstead:1983:ISP


Payne:1978:OEN


Pollard:1974:TFP


Pollard:1978:MCM


Pomerance:1988:ACC

Carl Pomerance, editor. Advances in cryptology — CRYPTO
REFERENCES


REFERENCES


REFERENCES

Pomerance:1988:PAF


Pomerance:1980:P


Purdy:1974:HSL


Puteanus:1627:EPC


Pluimakers:1986:ACS


Pfitzmann:1986:NUO


**Power:1986:AHE**


**Fitzmann:1987:NUO**


**Power:1987:AHE**


**Quisquater:1989:BHF**


**Qin:1988:RSS**


**Quisquater:1989:ACE**


**Rabin:1977:DS**

M. O. Rabin. Digitalized signatures. In Richard A. De-

Rabin:1981:HES


Rabin:1989:EDI


Randell:1982:CGC


Randell:1982:ODC


Rand:2001:MRD


Rao:1984:JEE

Rhodes-Burke:1982:RSA


Rabin:1989:VSS


Reeds:1979:CMC


Reischuk:1985:NSB


Rejewski:1979:EMH


Rejewski:19xx:EMH


Rowlett:1935:FAP

REFERENCES

[Ric74] Sheila R. Richards. Secret writing in the public records: Henry VIII–George II. London, 1974. x + 173 + 4 plates pp. UK£4.50. Contains one hundred documents, all but one of which are written wholly or partially in cipher and are now deciphered and printed in full for the first time. Includes letters in French or Italian, with a summary in English.


Rivest:1985:RCP


Rivest:1987:EDR


Reeds:1985:NPR


Rao:1987:PKA


Rao:1989:PKA


Rohwer:1975:GIM


Rohwer:1977:CCB

Jürgen Rohwer. The critical convoy battles of March 1943: the battle for HX.229/SC122.
REFERENCES


*Routh:1984:PAA*


*Roy:1986:CBI*

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.).

*Ringeisen:1986:ADM*


*Reeds:1978:HCM*


*Rivest:1983:RET*


*Rivest:1984:HEE*


*Rivest:1978:MOD*

The basics of trap-door functions and the famous RSA public key cryptosystem are presented in this paper.

[Rivest:1982:MOD]


[Rivest:1983:MOD]


[Reif:1988:EPP]


[Raleigh:1988:CDP]


[Rubin:1979:DSC]


[Rudolph:1982:HTI]


[Ruggiu:1985:CCT]

REFERENCES

Russell:1927:CMS


Reeds:1984:FSU


Rytter:1986:SCU


S:1873:COD


Sacco:1936:MC


Sacco:1947:MC


Sacco:1951:MCF


Sacco:1977:MC


Saks:1989:RNP

REFERENCES


Saltzer:1973:PCI

Saltzer:1978:DS

Salomaa:1985:PKC

Salomaa:1988:PKC

Sansom:1986:BRC

Sandhu:1988:CIT

Sarton:1928:BRBn

Satyanarayanan:1989:ISL
Saunders:1989:IDE


Sawirudin:1955:PND


Schaumuller-Bichl:1982:ADE


Sorkin:1984:MCC


Serpell:1985:PES


Smillie:1985:RFM


Chen:1985:RGE

Su shing Chen. On rotation

Scacchetti:1986:CT


Schwenter:1620:SSN


Schroeder:1969:IC


Schroeder:1975:ESK


Schell:1983:SPA

K. J. Schell. Security printers application of lasers. Pro-
REFERENCES


Schroeder:1984:NTS


Schroeder:1986:NTS


Smith:1986:GCC


Sicherman:1983:AQR


Smillie:1986:RWA


Seaton:1956:THS

[E. Seaton. Thomas Hariot’s secret script. Ambix: Jour-


[Shannon48] Claude Shannon. A mathematical theory of communica-
REFERENCES

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

Shannon:1948:MTCb

Shannon:1949:CTS

Shamir:1979:HSS

Shamir:1982:PTA

Shamir:1983:ECT

Shamir:1983:GCS

Shamir:1984:PTA
Adi Shamir. A polynomial-time algorithm for breaking the basic Merkle–Hellman cryptosystem. *IEEE Transactions on
REFERENCES


[She88] A. T. Sherman. Cryptology and VLSI (Very Large Scale Integration). I. Detecting and exploiting algebraic weaknesses in
REFERENCES


REFERENCES


Simmons:1982:SAE


Simmons:1983:PPS


Simmons:1984:HID


Simmons:1985:ATC


Simmons:1985:SCD


Simmons:1988:SSC


Sinkov:1966:ECM

REFERENCES


Sinkov:1968:ECMa


Sinkov:1968:ECMb


Sinnott:1977:CTC


Singh:1985:IPS


Sambur:1976:SEM


Schneier:1997:RAS


Schobi:1983:FAT


Smith:1943:CSS


Smith:1944:CSS

Laurence Dwight Smith. *Cryptography: the science of secret writing*. G. Allen and Unwin,
REFERENCES


[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.


[Sny79] 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


[SW83] J. W. Smith and S. S. Wagstaff, Jr. How to crack an RSA cryp-


[SW+81] Herbert E. Salzer, Eric A. Weiss, Henry S. Tropp, Jane Smith, and Robert W. Rec
tor. Reviews: H. H. Goldst

THAO. ISSN 0490-6756.

Salomaa:1986:PKC


Tao:1985:FAP


Tao:1986:TVF


Tedrick:1985:FES


Thomason:1974:RPS


Thompson:1984:RTT

REFERENCES

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
...; praefixa est huic operi sua clauis, seu vera introductio ab ipso authore concinnata ... nunc vero in gratiam secretioris philosophiae studiorum publici iuris facta. Francofurti. Ex officina typographica Matthiae Beckeri, sumptibus Ioannis Berneri, anno 1606.

**Trithemius:1621:CGT**


**Trithemius:1621:CSI**


**Trithemius:1621:SHE**


**Trithemius:1621:SHE**

**Terry:1988:MSV**


**Tsudik:1989:DAI**


**Thersites:1984:IKE**

REFERENCES

Thomas:1984:IKE


Tuchman:1966:ZT


Tuckerman:1970:SVV


Tuchman:1979:HPN


Tuchman:1979:IHP


Turing:1941:APC


Turing:1941:SR


Turing:1999:TTE

[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.

**USASC:1923:EC**


**USWarDept:1924:EC**


**USWD:1924:EC**


**USASC:1940:CML**


**USASC:1942:ACC**


**USDOS:1970:BC**


**USNBS:1977:DES**


**USCSC:1978:CSD**


**USCSSC:1978:USN**

**[Uni78b]** United States Congress Senate. Select Committee on Intelligence. *Unclassified summary — involvement of NSA in the development of the Data Encryption Standard: staff report of the
REFERENCES

Senate Select Committee on Intelligence, United States Senate. United States Government Printing Office, Washing-
ton, DC, USA, April 1978. ii + 4 pp.


REFERENCES


USGAOPEMD:1987:PDD


USDA:1988:CED


USNBS:1988:DES


USGSA:1983:ISR


USGSA:1985:ISR

cessing standards publication, FIPS PUB 141.


[UU89] United States.Dept.of the Army and United States Army Intelli-

**VanderBank:1988:CFM**


**Valerio:1892:C**


**Vamos:1985:BRB**


**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

REFERENCES


REFERENCES

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


[Wat89] Miguel Watler. VLSI architectures and circuits for RSA encryption. Thesis (M.Sc.),
Queen’s University, Ottawa, ON, Canada, 1989. 137 pp.


REFERENCES


REFERENCES


Willett:1983:TKS


[Wil86a]

Williams:1983:PAP


[Wil86b]

Williams:1985:SPK

REFERENCES

192

Winterbotham:1969:SP

Winterbotham:1974:US

Winterbotham:1974:USF

Winterbotham:1975:US

Winterbotham:1978:NC

Winternitz:1983:POW

Winternitz:1984:SOH

Wagner:1985:PKC
REFERENCES

Wolfe:1943:FCCa

Wolfe:1943:FCCb

Wolfe:1943:FCCc

Wolfe:1970:SWC

Wolfe:1983:FCC

Wood:1982:FAC

Worth:1975:CMA

Wortmann:1987:BRB
Wrixon:1989:CCS

Williams:1979:SRC

Webster:1986:DB

Weiss:1985:RCM

Williams:1979:CAA
REFERENCES

Wah:1984:RAM


Yao:1982:PSC


Yao:1982:TAT


Yao:1986:HGE


Yardley:1931:ABC


Yardley:1940:SSA


Yardley:1983:CBC


Yasaki:1976:EAK

[Yas76] E. K. Yasaki. Encryption algorithm: key size is the
REFERENCES


### Yung:1985:CSP


### Yung:1985:SUK


### Yu:1989:DEB


### Zafiropulo:1963:RAD


### Zeidler:1979:DDE


### Zim:1948:CSW


### Zorpette:1987:BEC