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/

02 November 2023
Version 4.114

Title word cross-reference

(mod$p$) [Pol78]. $1/2 + 1$**Poly**$(\log N)$ [ACGS84]. **$13.95** [Hig83]. **$16.95** [Ano84a]. **$19.95** [HJH85]. $25 \cdot 10^9$ [PSW80]. $2^m \pm 1$ [BLS75]. $2^n \pm 1$ [BS67]. $2n$ [QG89]. **$34.95** [Ano82a]. **$35.00** [Lei79a, Lei79b]. **$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) [ElG85c]. l [VGT89]. M^3 [Wil86a]. GF(2^{m}) [Mas89]. GF(p^{n}) [MOVW89]. N [Knu87, QG89, VGT89]. $n = 2$ [Lev61a]. NC^0 [Hås87]. $O(\log n)$ [LW88]. $O(\log n)$ [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]. **1976** [BGK77]. **1977** [Uni78a]. **1981** [BBB+81]. **1982** [IEE82b]. **1983** [Bur81, Fêa83, Had84]. **1984}** [San86, BCI85]. **1985** [Wil86b]. **1986** [ACM86, IEE86a]. **1987**

[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, Cam71, 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, Cou86, DK85, DDOP85, Elv87, Fri35a, Fri35b, Fri39b, Fri41, Fri42, Fri76c, Fri76b, Fri76d, Fri87, Gai39, Gai40, Gai43, Gul83, Gyl36, Gyl38, HS89, Hit43, Hof55, Kul35, Kul38, Kul67, Kul76, Lev61c, Mil43a, Mil43b, Mil43c, Sim04, Sin66, Sin68a, Sin68b, SS86, UG23, Uni42, UU89, Uni70, Uni24b, UU80, UU83, Uni24a, War82, Win74b, Wol43a, Wol43b, Wol43c, Wol83, de 53, vTB86, SE86]. **Cryptanalyst** [Uni40, Fri39a, GPW85, Gle86]. **Cryptanalysts** [MB86]. **Cryptanalytic** [Dea87, Odl84, GC80, Hel81]. **Cryptanalytical** [Cha86b]. **cryptananysis** [CR88a]. **cryptic** [SD86, WW79]. **CRYPTO** [BC85, Bra90, Wil86b, CF88, Fåk87, O'C81, Wil85, CRS83, CRY81, Ger82, Odl87b, Pom88]. **Crypto-ease** [O'C81]. **Crypto-Functions** [Wil85]. **Cryptogram** [Ano60]. **Cryptograms** [MM83, Nan36, Nan74]. **cryptograph** [Bar77, Gyl36, Gyl38]. **Cryptographer** [Sca86, Wol70]. **Cryptographia** [Con39, Put27, Col64]. **Cryptographic** [ARS83, Agn87, Agn88, AT83, BIB89, BCI85, Bry67, CP87, CP88, DLM82, DHM80, Dif82b, EMMT78, Fei70, Gif81, GJ82, GGM85, Gun88b, Gyl34, Ham71, Hen81, KV89, KMM$^+$80, Lea87, LT85, MTMA85, MM78, QV89, Ritxx, San88, Ser85, Sha83a, Sie84, Smi83, Uni88a, Van69, VA88, Ano86b, BOCS83, Bla79, Bur88, Com76, CF88, Coh87a, D$^+$83, Erd86, Fei74, FNS75, FF57, FM76, GY58, Gro74, HS85, HFL$^+$85, Her81, HC88, IN89, Lau81, Lev83, LR86, Mas83, NY89b, NY89a, Odl85, Par85, Pic86, PH78, Sed88, Smi71a, Smi74, SB84, Uni82a, Uni82b, Wei83]. **Cryptographically** [BM82, BM84a, KM88, Sha83b, Ayo83, Ste87]. **Cryptographie** [vN83, S.73, Val92, Bau39, Bau46, Giv25, Giv32, Jos85, LS25, Sac51, dlS02, du 44]. **Cryptography** [Ame81, Ano76, Ano88c, Ano88b, BBB$^+$81, BP89, BB85, Bet83, BGK77, BE76, BE79, Bur84a, Bur84b, CG75, Cop87, CM79, Dav81, DB81, Den82, DH76b, Dif88, ECW75, Fei73, Fis84, Fri76c, Gro82, Gud80, GL82, Hel79b, Hil29, Hil31, Hul98, Kon81, LM22, Lan81, Len78, Lev58, Lev61a, Lev61b, Mau14, MM82, Mil86, Mor66, SP89, Sha87, Sha45, SE86, Smi43, Smi44, Smi55, Smi71b, Smi83, Tur41a, Wil82a, dRHG$^+$99, AS83, Are21, Are22, BCB88, Bau39, Bau46, BB89, BS82, Bra81, Buc82, Cho86, DK85, Des88, DH76c, Fri76a, Fri76e, Gag88b, Gal88, Ger82, Giv78, Gui76, HHL89, Hel76, Hit43, IL89, vN83, Kil88, Kob87a, Kra86, LS25, LS81, Lec89, Lev61c, MS76, Men39, Mey73, Mic88, Mil43a, Mil43b, Mil43c, ML67, NBS76, Nea75]. **cryptography** [Per85, Pie77, Pri83, Sac36, Sac47, Sac51, Sac77, Sch84, Sch86, SW61, Shu76, Shu82, SNO72, TP63, Uni42, VS41, Vol41, Wal00, Wel88b, Wel89, Wie87, Wil82b, Woo82, dlS02, BCKS$^+$83, Col64, du 44, Kon89, Lei79a, Lei79b, Ano82a, ST89]. **Cryptologia** [Hig88b]. **Cryptologic** [Ale45, Jou88, Sny79, Sny80]. **cryptologist** [Cla77b, FFW55]. **Cryptology** [AM85, BC85, Boy86, Bra89b, Bra89a, Cal92, CRS83, CP87, Com87, DKKM87, DK$^+$89, Fer87, Gir72, Kah66, Kah79, Kah84, Kon89, Las85, Lem79, LP87, Mar70a, Mar70b, Mei83, Nai89, Por84, QV89, Rug85, She86, She87,

[Fis84]. **deck** [Her89]. **decoder** [Boy88]. **decoders** [MP86]. **decree** [Bud29, Bud76]. **d'écrire** [S.73]. **Decrypting** [Rub79, Sie85]. **Decryption** [Hen81, Beh54, Hen82, Per90, Sau89, Uni79b, Wil86c]. **Dee** [Shu82]. **defeat** [Lew82]. **defies** [SS86]. **Defined** [BS86]. **definitions** [Kah63]. **Degenerate** [Ber09]. **degree** [Hås88]. **Degrees** [WTE+85]. **deinde** [Hei76]. **Demands** [Fåk87]. **Demonstrating** [CEvdGP87]. **demotic** [Bud76, Bud29]. **d'encres** [S.73]. **denies** [Ano79]. **Denmark** [Bro86, Wor87]. **Denning** [Bv82]. **Density** [LO85]. **denudata** [Con39]. **DEP** [FMP85]. **Dependence** [DQD85]. **dependency** [O'S88]. **depositions** [GB82]. **depth** [Dat85]. **description** [Riv80]. **d'escrire** [du 44]. **desiderata** [Hei76]. **Design** [Cha86a, Flo83, Gud80, Mey73, PW86a, PR85a, SRC84, Sha88, Ayo83, Fåk87, FLR77, HL88, KD78, KD79, MM82, MPS02, MT86, 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** [AWL+88, NS89, Ano78c, Bro81, Kah82, Uni78b]. **Developments** [Ano88h, AWL+88, WTE+85, Jur86]. **Deviates** [Ran55, Ran01]. **device** [Sha88, Smi71a, Tex84]. **devices** [Ano87d, Dat85, Spe87]. **diagnostic** [Sau89]. **Dickson** [MN86, Nöb88]. **Dickson-polynomials** [Nöb88]. **Dickson-scheme** [MN86]. **dictionary** [O'C81, Kah63]. **diem** [Hei76]. **Dierstein** [Ano88a]. **Difference** [BCKS+83, Fåk86]. **difficult** [Jur86]. **difficulty** [TIF+88]. **Diffusion** [AWL+88]. **digest** [Rud82]. **Digital** [AWL+88, Den84a, FMP85, GMR88, Her89, Mat79, MA81, Mer88, Mer89, Oka88, Par85, Ran82b, RSA78, RSA83, Sim85b, Zei79, Ano80, Bar87, Cha79, Cha81, CC81, Dem88, Fun78, Lie81, RSA82, Sal78, Sch84, Sch86, Sny79, TC85, TC86, Bur81]. **Digitalized** [Rab77]. **Digits** [Ran55, Ran01]. **Digraphic** [Bow59]. **dimension** [MM82]. **Diophantine** [Lag84a]. **diplomacy** [TP63]. **Diplomatic** [Web79, Shu80a, Shu80b]. **Direct** [Bou85]. **Directions** [DH76b]. **Directly** [MOI82]. **Dirichlet** [BD74]. **disaster** [Far67, Far69]. **Discrete** [COS86, ElG85b, Odl85, Adl79, CEvdGP87, DO86, EG85a, ElG85a, ElG85c, 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, Eck85, Kak84, LLH89]. **Dits** [BCKS+83]. **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** [Hit43]. **Door** [IW81, MH78]. **Doorbell** [Sto65]. **Doran** [AWL+88]. **double** [Cou86]. **Dr.** [Ano60]. **Draft** [Bra75a, CR85]. **Dual** [NM88]. **Duke** [Wal00]. **Dupont** [BBB+81]. **durch** [Sch20]. **during** [Bar79c, Bar79b, Men89]. **Dutch** [BWV+88]. **Dvorak** [WTE+85]. **Dynamic** [Pro85, Tsu89, WCWG86]. **dzialan** [Kos83].

E. [WTE+85]. **Early** [BWV+88, Goo79, Zor87, BWV+88]. **Eary** [Riv87]. **ease** [O'C81]. **East** [Str89]. **Easy** [Gai78, Gor85, VV86]. **Eavesdropper** [RS84]. **ECL** [HR82]. **écriture** [S.73, Zaf63]. **écritures** [Per90]. **ECS** [Nea75]. **ed** [AWL+88]. **Edgar** [Sau89]. **Edited** [CM82].

[Hei76]. **Hackers** [WTE+85]. **Hagelin** [Bar77, RRM78]. **Hall** [ST89]. **handbook** [CF88]. **Happenings** [ML87]. **Harbor** [Far67, Far69]. **Hard** [ACGS88, Gef73, GL89, Wil82c]. **hard-core** [GL89]. **harder** [AB81]. **Hardware** [Cia86, DDG+85, Fåk86, Gai77, Gai80c, Gru84, Hig87e, HGD85]. **Hariot** [Sea56]. **Harmonia** [Mer44]. **Harold** [Hig88a]. **Hartree** [Ano88h, WTE+85, AWL+88]. **Harvard** [AWL+88]. **Hash** [MRW89, QG89, WC81, Win83, Win84, NY89b, NY89a, Riv74a]. **hash-coding** [Riv74a]. **Hash-Functions** [QG89]. **hashfunctions** [PBGV89]. **Having** [MS87, Gyl38]. **Hayden** [Hig83]. **heat** [BR88]. **Hebraicis** [Hei76]. **held** [Ano78a, BGK77, EKMN84, RR86, Uni78a]. **Hellman** [Bra79, Dav79, Lag84b, Sha82, Sha84, Tuc79a, Tuc79b]. **Hemel** [ST89]. **Hempstead** [ST89]. **Henry** [Ric74]. **Herlestam** [Riv79]. **heterogeneous** [PW86b, PW87b]. **heuristic** [Gul83]. **Hides** [BG85, LW88]. **Hiding** [MH78]. **Hierarchical** [LS89]. **Hierarchy** [AT83, MTMA85, San88]. **hieroglyphic** [Bud76, Bud29]. **Hieroglyphs** [Cas76, Bud76]. **High** [Ano87b, Lev61a, Pur74, Sed88, VK83, Lom83, Rud82]. **High-Level** [VK83]. **High-Speed** [Lev61a, Ano87b]. **Hilton** [IEE81, IEE82b]. **him** [FF57]. **Hinsley** [SBET85]. **Hisperic** [MS76]. **Historical** [Lan46, Gal45a, Gal45b, Gal45c, Gal70]. **History** [Adl87, Ale45, Ano81a, AWL+88, Bur81, Cal92, LM85, Riv87, SWT+81, Bar79c, Bar79b, Bud76, Cam87, DK+89, Hul98, Rejxx]. **Hitler** [Win74b]. **hobby** [Fra86]. **hoc** [Tri06c, Tri21c]. **Höhepunkt** [Roh75]. **Holland** [Had84]. **homomorphic** [Chu89]. **Honest** [GMW87, RBO89]. **honours** [Bud29, Bud76]. **Hord** [BCKS+83]. **horizon** [Ano60]. **horoscope** [Shu82]. **horses** [Kar87]. **Host** [Erd86]. **Hotel** [IEE82b, Rud82]. **Houghton** [Ano84a]. **Houthalen** [QV89]. **hucusq** [Hei76]. **Hughes** [Ano88d]. **Humanities** [Lei79a, Lei79b]. **hunc** [Hei76]. **Hungarian** [HS87]. **Hut** [BCKS+83, Wel82a]. **HX.229** [Roh77]. **HX.229/SC122** [Roh77]. **Hydraulica** [Mer44]. **Hypergrowth** [WTE+85]. **hypothesis** [Mil76].

I. [BCKS+83]. **i.e** [Sch33]. **IBM** [Ber80, Dea87, Gir71, WCWG86]. **IC** [CSB89]. **idempotent** [PR85a]. **Identification** [St.93, Ano88j, Cha85c, FS87, O'S88, Sha86]. **identify** [Jur86]. **Identifying** [Spe87]. **Identity** [PT89, Sha85]. **Identity-Based** [Sha85]. **IEEE** [Lu80, Rud82, IEE87b, IEE87c]. **IEEE/IEICE** [IEE87b]. **IEICE** [IEE87b]. **IFIP** [Fêa83, Had84, San86, CSB89]. **IFIP/Sec'83** [Fêa83, Had84]. **IFIP/Sec'84** [San86]. **II** [Elv87, Bur84b, Cla77a, Hig87b, Hig88f, Hig89, Lew78, Men89, OW84, Pli98, Ric74, She86, She87, She88, Win74b]. **III** [Dav79]. **illegal** [Hor85]. **Illiac** [BCKS+83]. **Illinois** [ACM88, IEE82a]. **Illus** [Shu80a, Shu80b, Lei79a, Lei79b]. **illustrata** [Hei76]. **'Ilm** [MTA87]. **im** [Roh75]. **Images** [Sch69]. **imaging** [Fun78]. **Imai** [DDOP85]. **Immanuel** [Vam85]. **Immunity** [Sie84]. **Impact** [Ano88h, AWL+88, WTE+85]. **Imperfect** [Wel88a, Hog88]. **Implementation** [Bis88b, Bis88c, Bis88d, Mor88, Van86, AG84, APW85, Bis88a, Erd86, Hig88c, HGD85, MM82, ORS+87, Riv80, Roh75, Roy86, San88]. **implementations** [DDG+85, Gai77, Gai80c]. **Implementing** [Bar87, CF78, EMMT78, Jun87, Jun88, Ano81b, Bra75a, CL88, Uni81]. **implementors** [CF88]. **Implications** [Tsu89]. **impossibilibus** [Hei76]. **Impossible** [Blu82, Blu83a]. **improved** [PH78]. **improvement** [HC88].

prepared [BBB+81]. **Presence** [CGMA85]. **present** [Riv85]. **presents** [Tuc79a, Tuc79b]. **Press** [Man60]. **Prevent** [Cha85b]. **Price** [ST89]. **Primality** [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, Dre79, 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** [McC75, KP89]. **Probable-Word-Proof** [McC75]. **Problem** [AT83, BCKS+83, Cal89, CN87, GMR85, LSP82, Lam73, Mau14, Ryt86, Sim83, WM85, Bar79a, Com87, Gai78, GY58, Jon86, Rei85, Tho74, Vou80b, Wil83b]. **Problems** [BS86, Blu82, Blu83a, BO85d, CG87, LO85, Eve85, FS87, Fri76b, Jur86, MP86, Roh75, Rou84, Ses81, Wil82c]. **procédés** [S.73]. **Procedure** [Bir85, Pur74, Wil80]. **Procedures** [Lin93, Bau82, Lin87, Lin88, Lin89, Uni88a]. **Proceedings** [ACM82, ACM83, ACM85, ACM87, ACM89a, ACM89b, ACM89c, BC85, CP87, EKMN84, Gle87, HW76, IEE80, IEE82b, IEE83, IEE87c, Ker75, QV89, RR86, San86, USE88b, USE88c, USE88a, USE89b, USE89a, Ano78a, Ano87a, Ano88g, Bet83, BCI85, CRS83, CP88, CSB89, CRY81, Fêa83, Gun88b, Had84, Mor89, Odl87b, Pic86, Pom88, Uni78a, Wil86b, ACM86, ACM88, AWL+88, Bra90]. **Process** [Bv82, Hel81, 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, BCKS+83]. **Programowa** [Kos83]. **Programs** [FH74, KMM+80, Dea87]. **Progressions** [BD74]. **Project** [Muf88, Bla75]. **projections** [Gyl38]. **promissa** [Hei76]. **Proof** [BM84b, GMR89, McC75, Fit89]. **Proofs** [BOGKW88]. **Propagation** [Pro85]. **properties** [Chu89]. **property** [Ale98]. **proposal** [Rou84]. **Proposed** [NBS75b, Dif75, DH76a, McC75]. **propositional** [Kar89a]. **Prospective** [Ano88h, AWL+88, WTE+85]. **protect** [Gef73]. **Protecting** [EHMS00]. **Protection** [Cha86a, Coh87b, HRU76, HP87, Hog88, Sal73, Wel88a, Ale98, Ano86b, BP82, Ber80, Bra75b, CF78, CF88, Coh87a, Dif75, NBS75a, SB84, Uni87, Wel80, vdAvE86]. **protein** [GY58]. **Protocol** [BBF83, Blu82, Blu83a, Bra87a, St.93, VK84, EGL85, Mil87b, Sak89]. **Protocols** [CCD88, CMS89, DM83, FM85, GMW87, Mer80, Mer82a, Sid81, VK83, Yao82a, BO85a, BO85b, BO85c, Cam87, DLM82, D+83, Eve85, Kem89, RBO89]. **Prototype** [SBC85, BB89]. **Provable** [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, Gab82, LR86, Plu83, VV85, Mit76]. **Pseudo-Inversen** [Gab82]. **Pseudo-Random** [BM82, BM84a, Boy89b, Plu83, VV85, FHJ+84, LR86, Mit76]. **pseudoinverses** [Gab82]. **pseudonym** [Ano60]. **pseudonyms** [Cha79, Cha81]. **Pseudoprimes** [PSW80]. **Pseudorandom** [MT72, Por84, Sha83b, KM88, Lev85, LR88b, RT88]. **Ptolemy** [Bud29, Bud76].

[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** [Fêa83]. **Stokes** [BCKS$^+$83]. **Stone** [Bud22, Bud29, Bud76]. **Stones** [Hau74]. **Storage** [CM79, Ano87b]. **storage/backup** [Ano87b]. **Stored** [TS88]. **stories** [Bon47, Fut73]. **Storing** [KBD89]. **Story** [Cas76, Gin70, Ritxx, Far67, Far69, Kah67a, Kah67b, Kah96, Pra39, Wel82a, BCKS$^+$83]. **Strandberg** [Wor87]. **Strandbergs** [Bro86]. **strategy** [Ben89, HT79, HH79]. **Stream** [Rub79, Sie85, Bar84]. **Strong** [BM82, BM84a, Gor85, Sha83b]. **Structure** [MS87, Wil83a]. **Structured** [KD79, KD78, War82]. **structures** [ISN87]. **studies** [Uni79a]. **Study** [Ame81, BBB$^+$81, DB81, Buc82, Cou86, Gai39, Gai40, Gai43, Gai44, Gai56, Lan81, Per85, Sie83, Tuc70]. **subcategory** [Uni81]. **subexponential** [Adl79, ElG85c]. **subexponential-time** [ElG85c]. **subkey** [Wel80, Wel82b]. **Subkeys** [DWK81]. **Subliminal** [Sim83, Sim85b, Hol87]. **subroutine** [Com76]. **Subscription** [Yun85a]. **subsequences** [Koo86]. **Subset** [LO85, IN89]. **Substitution** [HM83, Lev58, PR79, Bar75, Bow59, Fri35b, Fri35c, KD78, KD79, Lau81, Mit76]. **substitution-permutation** [KD78, KD79]. **substitutions** [SY86a, SY86b]. **subtile** [du 44]. **subtle** [du 44]. **Subtractive** [Mor83]. **sui** [Tri06c, Tri21c]. **Suitable** [Dav85]. **Sum** [LO85, IN89]. **summary** [Uni78b]. **summe** [Hei76]. **Summer** [Bur81, Ass88, USE89b, USE89a]. **sunt** [Con39]. **Supercomputing** [ACM89b, Bis89a]. **Superincreasing** [Wil83a]. **Support** [BGK77, Bra79, Hel76, MPS02, NBS76, Van86]. **supposititia** [Hei76]. **surveillance** [Uni88a]. **Survey** [BO88, Cha86b, Tho86, PvL86, Pop89]. **Sweden** [Fêa83]. **Swedish** [Gyl31]. **Swift** [Wil41]. **Switching** [IEE74]. **Switzerland** [Gun88b]. **SX** [LtW88a, LtW88b]. **SX-2** [LtW88a, LtW88b]. **Symmetric** [QG89, Sim79c, Sim82b]. **symmetry** [Fri35c, RF35]. **sympathiques** [S.73]. **Symposium** [ACM82, ACM83, ACM85, ACM86, ACM87, ACM88, ACM89a, ACM89c, AWL$^+$88, IEE74, IEE79, IEE80, IEE82a, IEE83, IEE84, IEE85, IEE86b, IEE87a, IEE87c, IEE89]. **Synchronizing** [Pro85]. **Synthese** [SB82]. **synthesis** [GY58]. **System** [AT&T86, **?**, ARS83, Bur84a, Bur84b, Bur85, DWK81, GW76, Gud80, Hen81, HR82, IL83, LHM84, LB89a, LB89b, Pro85, QSA88, RW84, SRC84, Sat89, SBC85, Smi83, TS88, TT84a, TT84b, ALN87b, BCB88, BCW86, Cho86, Dro89, FLR77, Fei74, Fra89, Fun78, Her81, Lan89, Lei80, Mil85, MPS02, Mul81, MT86, Sil83, SNO72, Smi74, Sor80, TIF$^+$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, Fit89, Fri35b, Fri41, FF57, Gon89, Gro74, Hoo80, HW88, Lau81, Mer82b, MM82, NBWH78, Pea80, PR85b, Ses81, Tuc70, Wil68a, Wil68b, Wil72, Wil75, CA83b, CA83a].

T [Mul89b, WG82]. **T.** [BCKS$^+$83, SBET85]. **T0L** [SSA87]. **Täfelungen** [Gab82]. **take** [Gar77]. **tale** [Bro86, Fra84, Fra85b, Vam85, 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, Kul35, RF35]. **technice** [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, Dif82b, Gai80a, Rud82, BCKS+83]. **Telecommunications** [IEE87b, Uni82c]. **Telecryptograph** [Gua04]. **telegram** [FM76, Tuc66]. **Telegraph** [Ver26]. **Telegraphic** [Ver26]. **Telegraphing** [Gua04]. **teleinformatics** [GL82]. **Telephone** [Blu82, Blu83a, Gua04, Hon19, NBWH78]. **telephones** [Wab87]. **Telephoning** [Mea20]. **Teletrust** [Rih87]. **television** [Eck85]. **telex** [FVTS87]. **Templars** [GB82]. **Ten** [Dif88, Hel79a]. **ter** [Muf88]. **Term** [SE86]. **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]. **TH1/TH4** [Uni88a]. **TH4** [Uni88a]. **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]. **theorica** [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** [Fåk86]. **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** [Gyl31]. **Time** [CMS89, FH74, QSA88, Wil68a, Wil68b, Wil72, Wil75, AIR83, Bra81, ElG85c, 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** [BE79]. **TMS7500** [Tex84]. **TMS75C00** [Tex84]. **today** [DKKM87, Fåk86]. **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, Wel82b]. **trails** [Cam87]. **Trainer** [Uni82b]. **Traité** [LS25, dlS02]. **Trans** [Lu80]. **transaction** [Cha85c, ADDS91]. **Transactional** [O'N86]. **transcendental** [KLL88]. **Transfer** [BW85, Ano85b, Gra82, Kem88, Kil88, Rab81]. **Transformation** [Hil31, Com76, NM88]. **transformations** [YY89]. **transformed** [MOI82]. **Transition** [Lem79]. **translating** [Col64]. **translations** [Bud76]. **transmission** [Ano88d]. **transparent** [Hig88f]. **Transport** [VK84]. **Transposition** [Fri41, Bar61, Cou86]. **Trap** [IW81, MH78]. **Trap-Door** [IW81]. **Trapdoor** [Wil83a, Yao82b, GM85, SM83].

[BCKS+83, Dif88, Ash87, Gar77]. **Yeheskel** [Ano88i]. **yesterday** [DKKM87]. **York** [ACM87, Ano82a, HJH85, Hig88d, Lei79a, Lei79b, MZS79, Sin77]. **York/London** [Lei79a, Lei79b]. **yourself** [FS87].

Z [Kno79]. **zastosowan** [Kos83]. **Zeit** [Sch20]. **Zendian** [Cal89]. **Zero** [WTE+85, BFM88]. **zero-knowledge** [BFM88]. **Zimmermann** [FM76, Tuc66]. **zone** [Ano89]. **Zufallsgeneratoren** [Gab82]. **Zur** [SB82].

References

ANSI:1988:FIE

[AA88] American National Standards Institute and American Bankers Association.Secretariat. *Financial institution encryption of wholesale financial messages: X9.23*. American Bankers Association, Washington, DC, USA, 1988. vii + 28 pp.

Asmuth:1981:EAC

[AB81] C. A. Asmuth and G. R. Blakley. An efficient algorithm for constructing a cryptosystem which is harder to break than two other cryptosystems. *Computers and Mathematics with Applications*, 7 (6):447–450, 1981. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic).

Alexi:1984:RRB

[ACGS84] W. Alexi, B. Chor, O. Goldreich, and C. P. Schnorr. RSA/Rabin bits are $1/2 + 1\text{Poly}(\log N)$ secure. In IEEE [IEE84], pages 449–457. CODEN ASFPDV. ISBN 0-8186-8591-3, 0-8186-0591-X (paperback), 0-8186-4591-1 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1984. IEEE catalog no. 84CH2085-9.

Alexi:1988:RRF

[ACGS88] Werner Alexi, Benny Z. Chor, Oded Goldreich, and Claus-P. Schnorr. RSA and Rabin functions: Certain parts are as hard as the whole. *SIAM Journal on Computing*, 17(2):194–209, April 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

ACM:1982:PFA

[ACM82] ACM, editor. *Proceedings of the fourteenth annual ACM Symposium on Theory of Computing, San Francisco, California, May 5–7, 1982*. ACM Press, New York, NY 10036, USA, 1982. ISBN 0-89791-070-2. LCCN QA75.5 .A14 1982. ACM order no. 508820.

ACM:1983:PFA

[ACM83] ACM, editor. *Proceedings of the fifteenth annual ACM Symposium on Theory of Computing, Boston, Massachusetts, April 25–27, 1983*. ACM Press, New York, NY 10036, USA, 1983. ISBN 0-89791-099-0. LCCN QA75.5.A14 1983. ACM order no. 508830.

ACM:1985:PSA

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

posium on Theory of Computing, Providence, Rhode Island, May 6–8, 1985. ACM Press, New York, NY 10036, USA, 1985. ISBN 0-89791-151-2 (paperback). LCCN QA 76.6 A13 1985. ACM order no. 508850.

ACM:1986:PEA

[ACM86] ACM, editor. *Proceedings of the Eighteenth annual ACM Symposium on Theory of Computing, Berkeley, California, May 28–30, 1986*. ACM Press, New York, NY 10036, USA, 1986. ISBN 0-89791-193-8. LCCN QA 76.6 A13 1986. ACM order number 508860.

ACM:1987:PNA

[ACM87] ACM, editor. *Proceedings of the nineteenth annual ACM Symposium on Theory of Computing, New York City, May 25–27, 1987*. ACM Press, New York, NY 10036, USA, 1987. ISBN 0-89791-221-7. LCCN QA 76.6 A13 1987.

ACM:1988:PTA

[ACM88] ACM, editor. *Proceedings of the twentieth annual ACM Symposium on Theory of Computing, Chicago, Illinois, May 2–4, 1988*. ACM Press, New York, NY 10036, USA, 1988. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988. ACM order no. 508880.

ACM:1989:PEA

[ACM89a] ACM, editor. *Proceedings of the Eighth Annual ACM Symposium on Principles of Distributed Computing: Edmonton, Alberta, Canada, August 14–16, 1989*. ACM Press, New York, NY 10036, USA, 1989. ISBN 0-89791-326-4. LCCN QA 76.9 D5 A26 1989.

ACM:1989:PSN

[ACM89b] ACM, editor. *Proceedings, Supercomputing '89: November 13–17, 1989, Reno, Nevada*. ACM Press, New York, NY 10036, USA, 1989. ISBN 0-89791-341-8. LCCN QA 76.5 S87 1989. IEEE 89CH2802-7.

ACM:1989:PTF

[ACM89c] *Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing: Seattle, Washington, May 15–17, 1989*. ACM Press, New York, NY 10036, USA, 1989. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989.

Ahlswede:1981:BCG

[AD81] R. Ahlswede and G. Dueck. Bad codes are good ciphers. Report, Universität Bielefeld, Bielefeld, Germany, 1981. Submitted in Nov. 1980 to the proceedings of the International Colloquium on Information Theory, to be held at Budapest in August 1981.

Abraham:1991:TSS

[ADDS91] D. G. Abraham, G. M. Dolan, G. P. Double, and J. V. Stevens. Transaction Security System. *IBM Systems Journal*, 30(2):206–229, 1991. CODEN IBMSA7. ISSN 0018-8670. See erratum [**?**].

Adleman:1979:SAD

[Adl79] L. M. Adleman. A subexponential algorithm for the discrete logarithm. In IEEE [IEE79], pages 55–60. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA267 .S95 1979; TK7885.A1 S92 1979.

Adleman:1983:BGK

[Adl83] Leonard M. Adleman. On breaking generalized knapsack public key cryptosystems. In ACM [ACM83], pages 402–412. ISBN 0-89791-099-0. LCCN QA75.5.A14 1983. ACM order no. 508830.

Adleman:1987:PRD

[Adl87] Leonard Adleman. Pre-RSA days: History and lessons. In Ashenhurst [Ash87], page ?? ISBN 0-201-07794-9. LCCN QA76.24 .A33 1987. ACM Turing Award lecture.

Apostolico:1984:PMM

[AG84] A. Apostolico and R. Giancarlo. Pattern matching machine implementation of a fast test for unique decipherability. *Information Processing Letters*, 18 (3):155–158, March 30, 1984. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Apostolico:1985:CAW

[AG85] Alberto Apostolico and Zvi Galil, editors. *Combinatorial algorithms on words (Maratea, Italy, June 18–22, 1984)*, volume 12 of *NATO Adv. Sci. Inst. Ser. F: Comput. Systems Sci.* Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1985. ISBN 0-387-15227-X. LCCN QA164 .N35 1984.

Agnew:1987:RSC

[Agn87] G. B. Agnew. Random sources for cryptographic systems. In Chaum and Price [CP87], pages 77–81. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). LCCN QA76.9.A25 E963 1987.

Agnew:1988:RSC

[Agn88] G. B. Agnew. Random sources for cryptographic systems. In Chaum and Price [CP87], pages 77–81. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). LCCN QA76.9.A25 E963 1987.

Akritas:1983:CEA

[AIR83] A. G. Akritas, S. S. Iyengar, and A. A. Rampuria. Computationally efficient algorithms for a one-time pad scheme. *International Journal of Computer and Information Sciences*, 12 (4):285–316, August 1983. CODEN IJCIAH. ISSN 0091-7036.

Alberti:1470:TC

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

Alexander:1945:CHG

[Ale45] C. H. O'D. Alexander. Cryptologic history of the German

Naval Enigma. GC&CS Report HW 25/7, British National Archives, ????, 1945.

Alexandre:1998:JBP

[Ale98] Thomas J. Alexandre. A Java-based platform for intellectual property protection on the World Wide Web. *Computer Networks and ISDN Systems*, 30(1–7):591–593, April 1, 1998. CODEN CNISE9. ISSN 0169-7552 (print), 1879-2324 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072101.html; http://www.elsevier.com/cas/tree/store/comnet/sub/1998/30/1-7/1863.pdf`.

Ahituv:1987:PED

[ALN87a] Niv Ahituv, Yeheskel Lapid, and Seev Neumann. Processing encrypted data. *Communications of the Association for Computing Machinery*, 30(9): 777–780, September 1987. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/30404.html`.

Ahituv:1987:VAI

[ALN87b] Niv Ahituv, Yeheskel Lapid, and Seev Neumann. Verifying the authentication of an information system user. *Computers and Security*, 6(2): 152–157, April 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404887900861`.

Akl:1985:FPR

[AM85] Selim G. Akl and Henk Meijer. A fast pseudo random permutation generator with applications to cryptology. In Blakley and Chaum [BC85], pages 269–275. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=269`. 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.

Adams:1988:SRC

[AM88] Carlisle M. Adams and Henk Meijer. Security-related comments regarding McEliece's public-key cryptosystem. *Lecture Notes in Computer Science*, 293:224–228, 1988. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Adams:1989:SRC

[AM89] Carlisle M. Adams and Henk Meijer. Security-related comments regarding McEliece's public-key cryptosystem. *IEEE*

Transactions on Information Theory, IT-35(2):454–455, 1989. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

ACE:1981:RPC

[Ame81] American Council on Education. Report of the Public Cryptography Study Group. *Communications of the Association for Computing Machinery*, 24 (7):435–450, July 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See the opposing view in [Dav81].

ANSI:1983:ANS

[Ame83] American National Standards Institute. *American National Standard for information systems: data encryption algorithm: modes of operation*. American National Standards Institute, 1430 Broadway, New York, NY 10018, USA, 1983. ?? pp.

Andrew:1986:TCB

[AN86] Christopher Andrew and Keith Neilson. Tsarist codebreakers and British codes. *Intelligence and National Security*, 1 (1):6–??, 1986. ISSN 0268-4527 (print), 1743-9019 (electronic).

Andree:1952:C

[And52] Richard Vernon Andree. *Cryptanalysis*. Yeshiva College, New York, NY, USA, 1952. 5–16 pp. Reprinted from Scripta mathematica, Vol. 28, No. 1. March, 1952.

Andelman:1979:MLE

[And79] Dov Andelman. *Maximum likelihood estimation applied to cryptanalysis*. Thesis (Ph.D.), Stanford University, Stanford, CA, USA, 1979. viii + 167 pp.

Andelman:1980:MLE

[And80] Dov Andelman. *Maximum likelihood estimation applied to cryptanalysis*. Thesis (Ph.D.), Department of Electrical Engineering, Stanford University, Stanford, CA, USA, 1980. viii + 167 pp.

Andrew:1986:CSI

[And86] Christopher Andrew. Codebreaking and signals intelligence. *Intelligence and National Security*, 1(1):1–??, 1986. ISSN 0268-4527 (print), 1743-9019 (electronic).

Anonymous:1922:PUS

[Ano22] Anonymous. Practical uses for the spectroscope, secret radio communication. *Scientific American*, 127(4):259, October 1922. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL `http://www.nature.com/scientificamerican/journal/v127/n4/pdf/scientificamerican1022-259.pdf`.

Anonymous:1939:ITM

[Ano39] Anonymous. Introductory talk to members of the William and Mary College cryptanalysis

class. Technical report, William and Mary College, Williamsburg, VA, USA, 1939. 7 pp.

Anonymous:1960:CNH

[Ano60] Anonymous. *Cryptanalysis, a new horizon, by Dr. Cryptogram [pseudonym]*. American Cryptogram Association, New York, NY, USA (??), 1960. 10 + 1 + 27 pp.

Anonymous:1976:CCA

[Ano76] Anonymous. *Cryptography and cryptanalysis articles*, volume 5 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1976. ISBN 0-89412-003-4. v + 144 pp. LCCN ????

Anonymous:1978:CSD

[Ano78a] Anonymous, editor. *Computer security and the Data Encryption Standard: proceedings of the Conference on Computer Security and the Data Encryption Standard held at the National Bureau of Standards in Gaithersburg, Maryland, on February 15, 1977*, volume 500-27 of *NBS special publication, computer science and technology*. United States Government Printing Office, Washington, DC, USA, 1978.

Anonymous:1978:NPAd

[Ano78b] Anonymous. New product applications: Single-board bipolar microcomputer emulates any mini- or microcomputer. *IEEE Spectrum*, 15(4):68–73, April 1978. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Anonymous:1978:ODA

[Ano78c] Anonymous. *The origin and development of the Army Security Agency, 1917–1947*, volume 16 of *A cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1978. ISBN 0-89412-025-5. 51 pp. LCCN UB290 .O75 1978.

Anonymous:1979:SSA

[Ano79] Anonymous. SB. Security Agency denies tampering with DES. *IEEE Spectrum*, 16(7):39, July 1979. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Anonymous:1980:ACS

[Ano80] Anonymous. An assessment of civil sector uses of digital data encryption. Technical report, Department of Engineering and Public Policy, Department of Social Sciences and School of Urban and Public Affairs, Carnegie-Mellon University, Pittsburgh, PA, USA, November 1980. 128 pp.

Anonymous:1981:CHP

[Ano81a] Anonymous. Corrections: How Polish Mathematicians Deciphered the Enigma, 3(3) 232, Reviews: H. H. Goldstine: A History of Numerical Analysis, 3(3) 293. *Annals of the History of Computing*, 3(4):407, October/

December 1981. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1981/pdf/a4400.pdf. See [Rej81, SWT+81].

Anonymous:1981:GIU

[Ano81b] Anonymous. *Guidelines for implementing and using the NBS Data Encryption Standard*, volume 74 of *United States. National Bureau of Standards. Federal information processing standards publication, FIPS PUB*. U.S. National Bureau of Standards, Gaithersburg, MD, USA, 1981. ISSN 0083-1816. 39 pp.

Anonymous:1982:BRCa

[Ano82a] Anonymous. Book review: *Cryptography: a primer*: Alan G. Konheim: New York: John Wiley and Sons, 1981. xiv + 432 pp. $34.95. *Computers and Security*, 1(1):84, January 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/016740488290030X.

Anonymous:1982:CC

[Ano82b] Anonymous. *A course in cryptanalysis*, volume 33, 34 of *Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1982. ISBN 0-89412-052-2 (vol. 1), 0-89412-053-0 (vol. 2). LCCN ????

Anonymous:1982:ESS

[Ano82c] Anonymous. Encryption scrambling the satellite signal for security, 1982. 1 sound cassette (75 min.).

Anonymous:1982:NNPa

[Ano82d] Anonymous. News and notices: Pioneer Award Established by Computer Society; Undergraduate Paper Competition in Cryptology. *Annals of the History of Computing*, 4(2):184, April/June 1982. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1982/pdf/a2184.pdf; http://www.computer.org/annals/an1982/a2184abs.htm.

Anonymous:1984:BRP

[Ano84a] Anonymous. Book review: *The puzzle palace: a report on NSA, America's most secret agency*: James Bamford: Boston: Houghton Mifflin Company, 1982, 465 pages. $16.95. *Computers and Security*, 3 (1):57, February 1984. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404884900300.

Anonymous:1984:ESC

[Ano84b] Anonymous. *EDP security: communications, database, end user, encryption: advanced security concepts*. Number 3 in FTP technical library EDP security. FTP, Port Jefferson Station, NY, USA, 1984. various pp.

Anonymous:1985:BM

[Ano85a] Anonymous. Back matter. In Blakley and Chaum [BC85], page ?? CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=??`. 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.

Anonymous:1985:DEA

[Ano85b] Anonymous. Data encryption algorithm: Electronic funds transfer: requirements for interfaces. Technical report, ????, ????, 1985. ISBN 0-7262-3764-7. 16 pp.

Anonymous:1986:MTT

[Ano86a] Anonymous. Modern technology tools for user authentication. *Computers and Security*, 5(3):184–185, September 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404886900039`.

Anonymous:1986:CPC

[Ano86b] Anonymous. On cryptographic protection of capabilities. *Computers and Security*, 5(2):98–99, June 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404886901306`.

Anonymous:1986:RE

[Ano86c] Anonymous. Remember the Enigma! *Computers and Security*, 5(4):288–289, December 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404886900489`.

Anonymous:1987:EVE

[Ano87a] Anonymous. *Enigma variations: encryption, emc/rfi, emp: 1987 conference proceedings*. Osprey Exhibitions, Watford, England, 1987. v + 243 pp.

Anonymous:1987:HSE

[Ano87b] Anonymous. High-speed encrypted storage/backup. *Computers and Security*, 6(5):370–373, October 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404887900034`.

Anonymous:1987:MAU

[Ano87c] Anonymous. Message authentication using the RSA. *Com-*

puters and Security, 6(5):373–376, October 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404887900046`.

Anonymous:1987:TWP

[Ano87d] Anonymous. Technology watch — personal authentication devices. *Computers and Security*, 6(1):10–11, February 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404887901143`.

Anonymous:1988:BRCb

[Ano88a] Anonymous. Book review: *Computer viruses — a secret threat*: Rudiger Dierstein. *Computers and Security*, 7(2):215, April 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888903537`.

Anonymous:1988:CCJc

[Ano88b] Anonymous. Cryptography and cryptosystems. January 1970–October 1987. *Computers and Security*, 7(5):519, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888902738`.

Anonymous:1988:CCJb

[Ano88c] Anonymous. Cryptography and cryptosystems. January 1987–December 1987 (citations from the INSPEC: Information Services for the Physics and Engineering Communities database). *Computers and Security*, 7(5):518, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888902593`.

Anonymous:1988:DEK

[Ano88d] Anonymous. Data encryption is key to safe file transmission: *Lawrence E. Hughes*. *Computers and Security*, 7(2):221, April 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888903926`.

Anonymous:1988:DESb

[Ano88e] Anonymous. Data encryption standard. 1975–January 1987 (citations from the INSPEC: Information Services for the Physics and Engineering Communities database). *Computers and Security*, 7(5):511, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888902155`.

Anonymous:1988:DESa

[Ano88f] Anonymous. Data Encryption Standard. January 1975–January 1988 (citations from the INSPEC: Information Services for the Physics and Engineering Communications Database). *Computers and Security*, 7(5):511, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888902143`.

Anonymous:1988:EVE

[Ano88g] Anonymous, editor. *Enigma variations: encryption, EMC/RFI, EMP: 1988 conference proceedings*. Osprey Exhibitions, Watford, England, 1988.

Anonymous:1988:ERH

[Ano88h] Anonymous. Errata: Reviews: Hartree: Calculating Machines: Recent and Prospective Developments and Their Impact on Mathematical Physics and Calculating Instruments and Machines, 10(1) 93. *Annals of the History of Computing*, 10(3):234, July/September 1988. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1988/pdf/a3234.pdf; http://www.computer.org/annals/an1988/a3234abs.htm`. See [AWL+88].

Anonymous:1988:PED

[Ano88i] Anonymous. Processing encrypted data: Niv Ahituv, Yeheskel Lapid, and Seev Neumann. *Computers and Security*, 7(1):103, February 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/016740488890524X`.

Anonymous:1988:RIA

[Ano88j] Anonymous. Remote identification and authentication of computer resource users: *Ken Weiss*. *Computers and Security*, 7(2):214, April 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888903495`.

Anonymous:1989:SZS

[Ano89] Anonymous. The safety zone (security products for microcomputers). *BYTE Magazine*, 14(6):290–291, June 1989. CODEN BYTEDJ. ISSN 0360-5280.

Aruliah:1985:PIE

[APW85] A. A. Aruliah, G. I. Parkin, and Brian A. Wichmann. A Pascal implementation of the DES encryption algorithm including cipher block chaining. NPL report DITC 61/85, National Physical Laboratory, Division of Information Technology and Computing, Teddington, Middlesex, UK, 1985. 37 pp.

Arensberg:1921:CD

[Are21] Walter Arensberg. *The cryptography of Dante*. Alfred A.

Knopf, New York, NY, USA, 1921. x + 494 pp. LCCN PQ4406.A7.

Arensberg:1922:CSP

[Are22] Walter Arensberg. *The cryptography of Shakespeare. Part one*. Howard Bowen, Los Angeles, CA, USA, 1922. ix + 280 pp. LCCN PR2944.A6. No more published. Source: Bequest of George Fabyan, 1940. DLC.

Adleman:1983:CCS

[ARS83] L. M. Adleman, R. L. Rivest, and A. Shamir. Cryptographic communications system and method. US Patent No. 4,405,829., September 20, 1983. URL `https://www.google.com/patents/US4405829`. Patent filed 14 September 1977.

Alpern:1983:KEU

[AS83] B. Alpern and F. B. Schneider. Key exchange using keyless cryptography. *Information Processing Letters*, 16(2):79–81, February 26, 1983. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Ashenhurst:1987:ATA

[Ash87] Robert L. Ashenhurst, editor. *ACM Turing Award Lectures: the first twenty years, 1966–1985*. ACM Press anthology series. ACM Press and Addison-Wesley, New York, NY 10036, USA and Reading, MA, USA, 1987. ISBN 0-201-07794-9. xviii + 483 pp. LCCN QA76.24 .A33 1987.

USENIX:1988:CSSb

[Ass88] USENIX Association, editor. *Computing Systems, Summer, 1988*. USENIX Association, Berkeley, CA, USA, Summer 1988.

Akl:1983:CSP

[AT83] Selim G. Akl and Peter D. Taylor. Cryptographic solution to a problem of access control in a hierarchy. *ACM Transactions on Computer Systems*, 1 (3):239–248, August 1983. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

ATT:1986:AUS

[AT&T86] AT&T. *AT&T UNIX System Readings and Applications*, volume II. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 1986. ISBN 0-13-939845-7. xii + 324 pp. LCCN QA76.76.O63 U553 1986.

Aspray:1988:RCD

[AWL+88] William Aspray, Maurice V. Wilkes, Albert C. Lewis, Greg Mellen, Harold Chucker, Robert V. D. Campbell, Wendy Wilkins, G. J. Tee, Ernest Braun, and Arthur L. Norberg. Reviews: Carpenter and Doran (eds.): A. M. Turing's ACE Report of 1946 and Other Papers; Masani (ed.): Norbert Wiener: Collected Works with Commentaries; Kozaczuk: Enigma: How

the German Machine Cipher Was Broken and How It Was Read by the Allies in World War Two; Worthy: William C. Norris: Portrait of a Maverick; Harvard Computation Laboratory: A Manual of Operation for the Automatic Sequence Controlled Calculator; Proceedings of a Symposium on Large-Scale Digital Calculating Machinery; Gardner: The Mind's New Science: A History of the Cognitive Revolution; Hartree: Calculating Machines: Recent and Prospective Developments and Their Impact on Mathematical Physics and Calculating Instruments and Machines; McLean and Rowland: The Inmos Saga; Pennings and Buifendam (eds.): New Technology as Organizational Innovation: The Development and Diffusion of Microelectronics; other literature. *Annals of the History of Computing*, 10(1):80–97, January/March 1988. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1988/pdf/a1080.pdf; http://www.computer.org/annals/an1988/a1080abs.htm. See minor erratum [Ano88h]: Hartree as a mathematical physicist, not a physical chemist.

Ayoub:1968:EKR

[Ayo68a] F. Ayoub. Encryption with keyed random permutations. *Electronics Letters*, 17(??):583–585, February 1968. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4245887.

Ayoub:1968:EEK

[Ayo68b] F. Ayoub. Erratum: Encryption with keyed random permutations. *Electronics Letters*, 17(??):??, February 1968. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4246020.

Ayoub:1981:EKR

[Ayo81] F. Ayoub. Encryption with keyed random permutations. *Electronics Letters*, 17(17):583–585, 1981. CODEN ELLEAK. ISSN 0013-5194.

Ayoub:1983:DCE

[Ayo83] F. Ayoub. The design of complete encryption networks using cryptographically equivalent permutations. *Computers and Security*, 2(3):261–267, November 1983. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/016740488390010X.

Bach:1988:HGF

[Bac88] Eric Bach. How to generate factored random numbers. *SIAM Journal on Computing*, 17(2):179–193, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Bamford:1982:PPR

[Bam82] James Bamford. *The puzzle palace: a report on America's most secret agency*. Houghton-Mifflin, Boston, MA, USA, 1982. ISBN 0-395-31286-8. 465 pp. LCCN KF7683.N32 B3.

Burrows:1989:LAb

[BAN89a] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *Operating Systems Review*, 23(5):1–13, December 1989. CODEN OSRED8. ISSN 0163-5980.

Burrows:1989:LAa

[BAN89b] Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. Technical Report 39, Digital Equipment Corporation, Systems Research Centre, February 28, 1989. 48 pp.

Barker:1961:CSC

[Bar61] Wayne G. Barker. *Cryptanalysis of the single columnar transposition cipher*. C. E. Tuttle Co., Rutland, VT, USA, 1961. x + 1 + 140 pp. LCCN Z103 Z32.

Bartek:1974:EDS

[Bar74] Douglas J. Bartek. Encryption for data security. *Honeywell Computer Journal*, 8(2):86–89, ???? 1974. CODEN HNCJA3. ISSN 0046-7847.

Barker:1975:CSS

[Bar75] Wayne G. Barker. *Cryptanalysis of the simple substitution cipher with word divisions using non-pattern word lists*. A Cryptographic series. Aegean Park Press, Laguna Hills, CA, USA, 1975. ISBN ???? 20 + 108 pp. LCCN Z103 .B3.

Barker:1977:CHC

[Bar77] Wayne G. Barker. *Cryptanalysis of the Hagelin cryptograph*, volume 17 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1977. ISBN 0-89412-022-0. xi + 223 pp. LCCN ????

Barker:1979:CEC

[Bar79a] Wayne G. Barker. *Cryptanalysis of an enciphered code problem: where an "additive" method of encipherment has been used*. A Cryptographic series. Aegean Park Press, Laguna Hills, CA, USA, 1979. ISBN 0-89412-037-9. vii + 174 pp. LCCN Z103 .B333.

Barker:1979:HCCb

[Bar79b] Wayne G. Barker, editor. *The history of codes and ciphers in the United States during the period between the World Wars*, volume 22, 54 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1979. ISBN 0-89412-039-5 (part 1), 0-89412-165-0 (part 2). various pp. LCCN UB290 .H47 1979. Two volumes. This book was written about 1946 by the Historical Section of the Army Security Agency.

Barker:1979:HCCa

[Bar79c] Wayne G. Barker, editor. *The history of codes and ciphers in the United States during World War I*, volume 20 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1979. ISBN 0-89412-031-X. 263 pp. LCCN D639.C75 H57 1979.

Barker:1984:CSG

[Bar84] Wayne G. Barker. *Cryptanalysis of shift-register generated stream cipher systems*, volume 39 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1984. ISBN 0-89412-062-X. ix + 247 pp. LCCN Z 104 B37 1984.

Barrett:1987:IRS

[Bar87] Paul Barrett. Implementing the Rivest, Shamir and Adleman public-key encryption algorithm on a standard digital signal processor. In Odlyzko [Odl87b], pages 311–323. CODEN LNCSD9. ISBN 3-540-18047-8, 0-387-18047-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1986. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0263.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=263`. Conference held at the University of California, Santa Barbara, Aug. 11–15, 1986.

Baudouin:1939:ECF

[Bau39] Roger Baudouin. *Éléments de cryptographie. (French) [Elements of cryptography]*. A. Pedone, Paris, France, 1939. 336 pp.

Baudouin:1946:ECF

[Bau46] Roger Baudouin. *Éléments de cryptographie. (French) [Elements of cryptography]*. A. Pedone, Paris, France, 1946. 336 pp.

Bauer:1982:KVM

[Bau82] Friedrich L. Bauer. Kryptologie — Verfahren und Maximen. (German) [Cryptology — procedures and maxims]. *Informatik Spektrum*, 5(??):74–81, ???? 1982. CODEN INSKDW. ISSN 0170-6012 (print), 1432-122X (electronic).

Bowers:1960:PC

[BB60] William Maxwell Bowers and William G. Bryan. *Practical cryptanalysis*. American Cryptogram Association, Greenfield, MA, USA, 1960. ?? pp. LCCN Z103 .B6. Bound in printed paper wrappers. Contents: v. 1. Digraphic substitution; the playfair cypher, the four square cypher.– v. 2. The Bifid cipher. — v. 3. The Trifid cipher.– v. 4. Cryptographic ABC'S; Substitution and transposition ciphers, by William G. Bryan. — v. 5. Cryptographic ABC's; periodic ciphers, miscellaneous, by William G. Bryan.

Bowers:1967:PC

[BB67] William Maxwell Bowers and William G. Bryan. *Practical cryptanalysis*. American Cryptogrm Association, Greenfield, MA, USA, 1967. various pp.

Blakley:1979:RSA

[BB79] G. R. Blakley and I. Borosh. Rivest–Shamir–Adleman public key cryptosystems do not always conceal messages. *Computers and Mathematics with Applications*, 5(3):169–178, 1979. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic).

Bennett:1985:UQC

[BB85] Charles H. Bennett and Gilles Brassard. An update on quantum cryptography. In Blakley and Chaum [BC85], pages 475–480. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=475`. 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.

Bennett:1989:EQC

[BB89] C. H. Bennett and G. Brassard. Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working. *ACM SIGACT News*, 20 (4):78–80, November 1989. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Baum:1981:RPC

[BBB+81] Werner A. Baum, David H. Brandin, R. Creighton Buck, George I. Davida, George Handelman, Martin E. Hellman, Ira Michael Heyman, Wilfred Kaplan, and Daniel C. Schwartz. Report of the Public Cryptography Study Group, prepared for American Council on Education, One Dupont Circle, Washington, DC 20036, February 7, 1981. *Communications of the Association for Computing Machinery*, 24 (7):435–445, July 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See the opposing view in [Dav81].

Bauer:1983:KDP

[BBF83] R. K. Bauer, T. A. Berson, and R. J. Feiertag. A key distribution protocol using event markers. *ACM Transactions on Computer Systems*, 1(3):249–255, August 1983. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

Bennett:1988:PAP

[BBR88] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Blakley:1985:ACP

[BC85] George Robert Blakley and David Chaum, editors. *Advances in Cryptology: Proceedings of CRYPTO 84*, volume 196 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1985. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0196.htm`; `http://www.springerlink.com/content/cemajg0qmeev/`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=196`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Barker:1988:ECT

[BCB88] W. C. Barker, P. Cochrane, and M. Branstad. Embedding cryptography into a Trusted Mach system. In IEEE [IEE88], pages 379–383. ISBN 0-8186-0895-1. LCCN TL787 .A471 1988; QA76.9.A25 A39 1988. IEEE catalog number 88CH2629-5. IEEE Computer Society order number 895.

Beth:1985:ACP

[BCI85] Thomas Beth, N. Cot, and I. Ingemarsson, editors. *Advances in cryptology: proceedings of EUROCRYPT 84, a Workshop on the Theory and Application of Cryptographic Techniques, Paris, France, April 9–11, 1984*, volume 209 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1985. CODEN LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). 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.

Bromley:1983:RFM

[BCKS+83] Allan G. Bromley, Martin Campbell-Kelly, K. W. Smillie, Eric A. Weiss, Saul Rosen, and Cipher A. Deavours. Reviews:

O. I. Franksen: Mr. Babbage, the Difference Engine, and the Problem of Notation: An Account of the Origin of Recursiveness and Conditionals in Computer Programming; H. Lukoff: from Dits to Bits; I. Asimov: Asimov's Biographical Encyclopedia of Science and Technology; J. Futrelle: Thinking Machine; R. M. Hord: The Illiac IV; C. H. Meyer and S. M. Matyas: Cryptography; T. J. Peters and R. H. Waterman: In Search of Excellence; J. W. Stokes: 70 Years of Radio Tubes and Valves; G. Welchman: The Hut Six Story; capsule reviews. *Annals of the History of Computing*, 5(4):411–427, October/December 1983. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1983/pdf/a4411.pdf`; `http://www.computer.org/annals/an1983/a4411abs.htm`.

Birnbaum:1986:VPS

[BCW86] Martha Birnbaum, Larry A. Cohen, and Frank X. Welsh. Voice password system for access security. *AT&T Technical Journal*, 65(5):68–74, September 1986. CODEN ATJOEM. ISSN 2376-676X (print), 8756-2324 (electronic).

Borucki:1974:MNN

[BD74] L. J. Borucki and J. B. Diaz. Mathematical notes: a note on primes, with arbitrary initial or terminal decimal ciphers, in Dirichlet arithmetic progressions. *American Mathematical Monthly*, 81(9):1001–1002, November 1974. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Bright:1976:CUM

[BE76] H. S. Bright and R. L. Enison. Cryptography using modular software elements. *AFIPS Conference Proceedings*, 45(??): 113–123, ???? 1976.

Bright:1979:QRN

[BE79] Herbert S. Bright and Richard L. Enison. Quasi-random number sequences from a long-period TLP generator with remarks on application to cryptography. *ACM Computing Surveys*, 11(4):357–370, December 1979. CODEN CMSVAN. ISSN 0010-4892.

Beardsley:1972:YCI

[Bea72] C. W. Beardsley. Is your computer insecure? *IEEE Spectrum*, 9(1):67–78, January 1972. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Becker:1982:EDE

[Bec82] Michael S. Becker. An exercise with the Data Encryption Standard. Master of science, plan ii, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, Berkeley, CA, USA, 1982. 56 pp.

Beckett:1988:IC

[Bec88] Brian Beckett. *Introduction to cryptology*. Professional and industrial computing series. Blackwell Scientific Publications, Oxford, UK, 1988. ISBN 0-632-01836-4 (paperback), 0-632-02243-4 (hardcover). xiv + 344 pp. LCCN QA76.9.A25 B431 1988. UK£14.95 (paperback), UK£35.00 (hardcover). See [Bec97].

Beckett:1997:ICP

[Bec97] Brian Beckett. *Introduction to cryptolology and PC security*. McGraw-Hill, New York, NY, USA, 1997. ISBN 0-07-709235-X (hardback). viii + 356 pp. LCCN QA76.9.A25 B43 1997. Updated edition of *Introduction to cryptology* [Bec88].

Beesly:1981:CIW

[Bee81] Patrick Beesly. *Cryptanalysis and its influence on the war at sea 1914–1918*. U.S. Naval Academy, Annapolis, MD, USA, 1981. 13 pp.

Behrens:1954:EUP

[Beh54] Carl E. Behrens. Effects on U-boat performance of intelligence from decryption of Allied communication. Technical report OEG study 553, Distributed by NTIS, Springfield, VA, USA, 1954. various pp.

Bell:1977:IVU

[Bel77] Ernest L. Bell. *An initial view of Ultra as an American weapon*. T S U Press, Keene, NH, USA, 1977. iii + 110 pp. LCCN D810.C88 B45.

Bennett:1980:UWN

[Ben80] Ralph Francis Bennett. *Ultra in the West: the Normandy campaign, 1944–45*. Scribner, New York, NY, USA, 1980. ISBN 0-684-16704-2. xvi + 336 pp. LCCN D756.5.N6 B44 1980. US$17.50.

Bennett:1988:AEA

[Ben88] John Bennett. Analysis of the encryption algorithm used in the WordPerfect word processing program. *Computers and Security*, 7(1): 105, February 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888905366`.

Bennett:1989:UMS

[Ben89] Ralph Francis Bennett. *Ultra and Mediterranean strategy 1941–1945*. H. Hamilton, London, UK, 1989. ISBN 0-241-12687-8. 496 pp. LCCN D766 .B46x 1989b.

Bertrand:1973:EOP

[Ber73] Gustave Bertrand. *Enigma; ou, La plus grande énigme de la guerre 1939–1945*. Plon, Paris, France, 1973. 295 + 2 + 16 pp. LCCN ????

Berstis:1980:SPD

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

System/38. *ACM SIGARCH Computer Architecture News*, 8 (3):245–252, 1980. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Bertrand:1983:EGE

[Ber83] Gustave Bertrand. *Enigma, or, The greatest enigma of the 1939–1945 war*. ????, ????, 1983. vi + 415 pp. LCCN ???? English translation by Russell Babcock Holmes of [Ber73].

Bergmann:2009:DKR

[Ber09] Seth D. Bergmann. Degenerate keys for RSA encryption. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 41 (2):95–98, June 2009. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Beth:1983:CPW

[Bet83] Thomas Beth, editor. *Cryptography: proceedings of the Workshop on Cryptography, Burg Feuerstein, Germany, March 29–April 2, 1982*, volume 149 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1983. CODEN LNCSD9. ISBN 0-387-11993-0 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN Z102.5 .C78 1983. DM43.00.

Betts:1988:ESG

[Bet88] Mitch Betts. Encryption standard to get reprieve. *Computers and Security*, 7(1): 106, February 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888905470`.

Blum:1988:NIZ

[BFM88] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In ACM [ACM88], pages 103–112. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988. URL `http://www.acm.org/pubs/articles/proceedings/stoc/62212/p103-blum/p103-blum.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/62212/p103-blum/`. ACM order no. 508880.

Blum:1985:EPP

[BG85] Manuel Blum and Shafi Goldwasser. An efficient probabilistic public-key encryption scheme which hides all partial information. In Blakley and Chaum [BC85], pages 289–302. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=289`. 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.

Branstad:1977:RWC

[BGK77] Dennis K. Branstad, Jason Gait, and Stuart Katzke, editors. *Report of the Workshop on Cryptography in Support of Computer Security, held at the National Bureau of Standards, September 21–22, 1976*. U.S. National Bureau of Standards, Gaithersburg, MD, USA, 1977.

Bar-Ilan:1989:NFC

[BIB89] J. Bar-Ilan and D. Beaver. Non-cryptographic fault-tolerant computing in a constant number of rounds. In ACM [ACM89a], pages 201–209. ISBN 0-89791-326-4. LCCN QA 76.9 D5 A26 1989.

Birrell:1985:SCU

[Bir85] Andrew D. Birrell. Secure communication using remote procedure calls. *ACM Transactions on Computer Systems*, 3 (1):1–14, February 1985. CODEN ACSYEC. ISSN 0734-2071. URL `http://www.acm.org:80/pubs/citations/journals/tocs/1985-3-1/p1-birrell/`.

Bishop:1988:AFDa

[Bis88a] Matt Bishop. An application of a fast Data Encryption Standard implementation. Technical report PCS-TR 88-138, Department of Mathematics and Computer Science, Dartmouth College, Hanover, NH, USA, 1988. 25 pp.

Bishop:1988:AFDb

[Bis88b] Matt Bishop. An application of a fast data encryption standard implementation. In Association [Ass88], pages 221–254.

Bishop:1988:AFDc

[Bis88c] Matt Bishop. An application of a fast Data Encryption Standard implementation. *Computing Systems*, 1(3):221–254, Summer 1988. CODEN CMSYE2. ISSN 0895-6340.

Bishop:COMPSYS-1-3-221

[Bis88d] Matt Bishop. An application of a fast data encryption standard implementation. *Computing Systems*, 1(3):221–254, Summer 1988. CODEN CMSYE2. ISSN 0895-6340.

Bishop:1988:FEP

[Bis88e] Matt Bishop. The fast encryption package. Technical report, Research Institute for Advanced Computer Science, Moffett Field, CA, USA, 1988. various pp. RIACS memorandum 88.3, NASA contractor report NASA CR-185397.

Bishop:1989:USS

[Bis89a] M. Bishop. UNIX security in a supercomputing environment. In ACM [ACM89b], pages 693–698. ISBN 0-89791-341-8. LCCN QA 76.5 S87 1989. IEEE 89CH2802-7.

Bishop:1989:FEP

[Bis89b] Matt Bishop. *The fast encryption package*. Moffett Field, CA, USA, 1989. ?? pp. Microfiche.

Book:1980:UDC

[BK80] R. V. Book and Sai Choi Kwan. On uniquely decipherable codes with two codewords. *IEEE Transactions on Computers*, C-29(4):324–325, April 1980. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1675571`.

Blatman:1975:MMC

[Bla75] Peter Blatman. Method of modern cryptanalysis: research project. Thesis (M.S. in Electrical Engineering), Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, Berkeley, CA, USA, June 1975. various pp.

Blakley:1979:SCK

[Bla79] G. R. Blakley. Safeguarding cryptographic keys. In Merwin et al. [MZS79], pages 313–317.

Blahut:1983:TPE

[Bla83] Richard E. Blahut. *Theory and Practice of Error Control Coding*. Addison-Wesley, Reading, MA, USA, 1983. ISBN 0-201-10102-5. xi + 500 pp. LCCN QA268 .B54 1983.

Blakley:1985:ITF

[Bla85] G. R. Blakley. Information theory without the finiteness assumption, I: Cryptosystems as group-theoretic objects. In Blakley and Chaum [BC85], pages 314–338. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=314`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Blanchard:1989:CSS

[Bla89] F. Blanchard. Certain sofic systems engendered codes. *Theoretical Computer Science*, 68(3): 253–265, November 12, 1989. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Brickell:1983:EAA

[BLO83] E. F. Brickell, J. C. Lagarias, and A. M. Odlyzko. Evaluation of the Adleman attack on multiply iterated knapsack cryptosystems. In Chaum et al. [CRS83], pages 39–42. ISBN 1-4757-0604-9 (print), 1-4757-0602-2. LCCN QA76.9.A25 C79 1982.

Brickell:1984:EAA

[BLO84] E. F. Brickell, J. C. Lagarias, and A. M. Odlyzko. Evaluation of the Adleman attack on multiply iterated knapsack cryptosystems (abstract). In *Advances in cryptology (Santa Barbara, Calif., 1983)*, pages 39–42. Plenum, New York, 1984.

Brillhart:1975:NPC

[BLS75] John Brillhart, D. H. Lehmer, and J. L. Selfridge. New primality criteria and factorizations of $2^m \pm 1$. *Mathematics of Computation*, 29(130):620–647, April 1975. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Blum:1982:CFT

[Blu82] Manuel Blum. Coin flipping by telephone — a protocol for solving impossible problems. In Rudolph [Rud82], pages 133–137. ISBN ???? LCCN TK7885.A1 C53 1982. IEEE catalog number 82CH1739-2.

Blum:1983:CFT

[Blu83a] Manuel Blum. Coin flipping by telephone — a protocol for solving impossible problems. *ACM SIGACT News*, 15(1): 23–27, January 1983. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Blum:1983:HES

[Blu83b] Manuel Blum. How to exchange (secret) keys. *ACM Transactions on Computer Systems*, 1 (2):175–193, May 1983. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic). Previously published in ACM STOC '83 proceedings, pages 440–447.

Blum:1984:IUC

[Blu84] Manuel Blum. Independent unbiased coin flips from a correlated biased source: a finite state Markov chain. In IEEE [IEE84], pages 425–433. CODEN ASFPDV. ISBN 0-8186-8591-3, 0-8186-0591-X (paperback), 0-8186-4591-1 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1984. IEEE catalog no. 84CH2085-9.

Bayer:1975:EST

[BM75] Rudolf Bayer and J. K. Metzger. On the encipherment of search trees and random access files. In Kerr [Ker75], page 452. ISBN ???? ISSN 0278-2596. LCCN QA76.9.D3 I55 1975. US$15.00. URL `http://www.vldb.org/dblp/db/conf/vldb/BayerM75.html`.

Bayer:1976:EST

[BM76] R. Bayer and J. K. Metzger. On the encipherment of search trees and random access files. *ACM Transactions on Database Systems*, 1(1):37–52, March 1976. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1976-1-1/p37-bayer/p37-bayer.pdf`; `http:`

//www.acm.org/pubs/citations/journals/tods/1976-1-1/p37-bayer/. Also published in [Ker75, p. 508–510].

Blum:1982:HGC

[BM82] Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudo-random bits. In IEEE [IEE82a], pages 112–117. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA76.6 .S95 1982. IEEE catalog no. 82CH1806-9. IEEE Computer Society order no. 440.

Blum:1984:HGC

[BM84a] Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM Journal on Computing*, 13(4): 850–864, ???? 1984. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Boyer:1984:PCR

[BM84b] Robert S. Boyer and J. Strother Moore. Proof checking the RSA public key encryption algorithm. *American Mathematical Monthly*, 91(3):181–189, 1984. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Blakley:1985:SRS

[BM85] G. R. Blakley and Catherine Meadows. Security of ramp schemes. In Blakley and Chaum [BC85], pages 242–268. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=242. 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.

Beale:1989:EUR

[BM89] M. Beale and M. F. Monaghan. Encryption using random Boolean functions. In *Cryptography and coding (Cirencester, 1986)*, volume 20 of *Inst. Math. Appl. Conf. Ser. New Ser.*, pages 219–230. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1989.

Blake:1985:CLG

[BMV85] I. F. Blake, R. C. Mullin, and S. A. Vanstone. Computing logarithms in GF(2^n). In Blakley and Chaum [BC85], pages 73–82. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=

0&spage=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.

Book:1985:SNP

[BO85a] R. V. Book and F. Otto. On the security of name-stamp protocols. *Theoretical Computer Science*, 39(2-3):319–325, August 1985. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Book:1985:SNS

[BO85b] R. V. Book and F. Otto. On the security of name-stamp protocols. *Theoretical Computer Science*, 39(2-3):319–325, August 1985. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Book:1985:VTA

[BO85c] R. V. Book and F. Otto. On the verifiability of two-party algebraic protocols. *Theoretical Computer Science*, 40(2-3):101–130, ???? 1985. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Book:1985:CRE

[BO85d] Ronald V. Book and Friedrich Otto. Cancellation rules and extended word problems. *Information Processing Letters*, 20 (1):5–11, January 2, 1985. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Brickell:1988:CSR

[BO88] Ernest F. Brickell and Andrew M. Odlyzko. Cryptanalysis: a survey of recent results. *Proceedings of the IEEE*, 76(5):578–593, May 1988. CODEN IEEPAD. ISSN 0018-9219 (print), 1558-2256 (electronic).

Ben-Or:1983:CSS

[BOCS83] Michael Ben-Or, Benny Chor, and Adi Shamir. On the cryptographic security of single RSA bits. In ACM [ACM83], pages 421–430. ISBN 0-89791-099-0. LCCN QA75.5.A14 1983. ACM order no. 508830.

Ben-Or:1988:MIP

[BOGKW88] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi-prover interactive proofs: How to remove intractability. In ACM [ACM88], pages 113–131. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988. ACM order no. 508880.

Ben-Or:1988:CTN

[BOGW88] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for noncryptographic fault-tolerant distributed computations. In ACM [ACM88], pages 1–10. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988. ACM order no. 508880.

Bond:1947:FSC

[Bon47] Raymond T. (Raymond Tostevin) Bond. *Famous stories of code and cipher*. Rinehart and Company, New York; Toronto, 1947. xxvi + 342 pp. LCCN PS648.C6 B65. Reprinted in 1965 by Collier Books.

Booth:1981:ASU

[Boo81] K. S. Booth. Authentication of signatures using public key encryption. *Communications of the Association for Computing Machinery*, 24(11):772–774, November 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Bosworth:1982:CCC

[Bos82] Bruce Bosworth. *Codes, ciphers, and computers: an introduction to information security*. Hayden Book Co., Rochelle Park, NJ, USA, 1982. ISBN 0-8104-5149-2. 259 pp. LCCN Z103.B58 1982.

Bounas:1985:DDS

[Bou85] Adam C. Bounas. Direct determination of a "seed" binary matrix. *Information Processing Letters*, 20(1):47–50, January 2, 1985. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Bowers:1959:DSP

[Bow59] William Maxwell Bowers. *Digraphic substitution: the Playfair cipher, the four square cipher*. Practical cryptanalysis; v. 1. American Cryptogram Association, Greenfield, MA, USA, 1959. 46 pp.

Bowers:1960:BC

[Bow60a] William Maxwell Bowers. *The bifid cipher*. Practical cryptanalysis; v. 2. American Cryptogram Association, Greenfield, MA, USA, 1960. 48 pp.

Bowers:1960:TC

[Bow60b] William Maxwell Bowers. *The trifid cipher*. Practical cryptanalysis; v. 3. American Cryptogram Association, Greenfield, MA, USA, 1960. ix + 55 pp.

Boyd:1986:CPC

[Boy86] Waldo T. Boyd. *Cryptology and the personal computer: with programming in Basic*, volume 47 of *A Cryptographic Series*. Aegean Park Press, Laguna Hills, CA, USA, 1986. ISBN 0-89412-145-6 (hardcover), 0-89412-144-8 (paperback). 157 pp. LCCN ????

Boyd:1988:CCB

[Boy88] Waldo T. Boyd. *Computer cryptology: beyond decoder rings*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 1988. ISBN 0-13-166133-7 (paperback). xv + 268 pp. LCCN Z103 .B65 1988. US$21.95.

Boyar:1989:ISPb

[Boy89a] Joan Boyar. Inferring sequences produced by a linear congruential generator missing low-order bits. *Journal of Cryptology*, 1

(3):177–184, ???? 1989. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Boyar:1989:ISPa

[Boy89b] Joan Boyar. Inferring sequences produced by pseudo-random number generators. *Journal of the Association for Computing Machinery*, 36(1):129–141, January 1989. CODEN JACOAH. ISSN 0004-5411. URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/59305.html`; `http://www.imada.sdu.dk/~joan/`.

Beker:1982:CSP

[BP82] Henry Beker and F. C. (Frederick Charles) Piper. *Cipher systems: the protection of communications*. John Wiley and Sons, Inc., New York, NY, USA, 1982. ISBN 0-471-89192-4. 427 pp. LCCN Z104 .B39 1982.

Beker:1985:SSC

[BP85] Henry Beker and F. C. (Frederick Charles) Piper. *Secure speech communications*, volume 3 of *Microelectronics and signal processing*. Academic Press, New York, NY, USA, 1985. ISBN 0-12-084780-9. xi + 267 pp. LCCN TK5102.5 .B354 1985.

Beker:1989:CC

[BP89] Henry Beker and F. C. Piper, editors. *Cryptography and coding*, The Institute of Mathematics and Its Applications conference series; new ser., 20. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1989. ISBN 0-19-853623-2. LCCN QA268.C74 1989. UK£35.00, US$52.00. Held in December 1986. "Based on the proceedings of a conference organized by the Institute of Mathematics and its Applications on cryptography and coding, held at the Royal Agricultural College, Cirencester on 15th-17th December 1986.".

Blakley:1988:CBA

[BR88] G. R. Blakley and William Rundell. Cryptosystems based on an analog of heat flow. *Lecture Notes in Computer Science*, 293:306–329, 1988. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Branstad:1975:DGI

[Bra75a] D. K. Branstad. Draft guidelines for implementing and using the NBS Data Encryption Standard. Report ??, U.S. National Bureau of Standards, Gaithersburg, MD, USA, November 10, 1975.

Branstad:1975:EPC

[Bra75b] D. K. Branstad. Encryption protection in computer data communications,. In ????, editor, *Fourth Data Communications Symposium, 7–9 October 1975, Quebec City, Canada*, page ?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1975.

Branstad:1979:VHD

[Bra79] D. Branstad. V. 'Hellman's data does not support his conclusion'. *IEEE Spectrum*, 16(7):41, July 1979. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Brassard:1981:TLT

[Bra81] Gilles Brassard. A time-luck tradeoff in relativized cryptography. *Journal of Computer and System Sciences*, 22 (3):280–311, June 1981. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0022000081900349`.

Bracha:1987:ERR

[Bra87a] Gabriel Bracha. An $O(\log n)$ expected rounds randomized Byzantine generals protocol. *Journal of the Association for Computing Machinery*, 34(4): 910–920, October 1987. CODEN JACOAH. ISSN 0004-5411. URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/42229.html`.

Brassard:1987:IMC

[Bra87b] Gilles Brassard. Introduction to modern cryptology. Publication 606, Université de Montreal, Dèpartement d'Informatique et de Recherche Opèrationnelle, Montréal, Québec, Canada, 1987. 56 pp.

Brassard:1988:MCT

[Bra88] Gilles Brassard. *Modern cryptology: a tutorial*, volume 325 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988. CODEN LNCSD9. ISBN 0-387-96842-3. ISSN 0302-9743 (print), 1611-3349 (electronic). vi + 107 pp. LCCN Z103 .B721 1988. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0325.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=325`.

Brassard:1989:CCb

[Bra89a] G. Brassard. Cryptology — column 2. *ACM SIGACT News*, 20(4):13, November 1989. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Brassard:1989:CCa

[Bra89b] Gilles Brassard. Cryptology column. *ACM SIGACT News*, 20(3):15–19, July 1989. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Brassard:1990:ACC

[Bra90] Gilles Brassard, editor. *Advances in cryptology: CRYPTO '89: proceedings*, volume 435 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. CODEN LNCSD9. ISBN 0-387-97317-6, 3-540-97317-6. ISSN 0302-

9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1989. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0435.htm; http://www.springerlink.com/content/978-0-387-97317-3; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=435. Conference held Aug. 20–24, 1989 at the University of California, Santa Barbara.

Brickell:1985:BIK

[Bri85] Ernest F. Brickell. Breaking iterated knapsacks. In Blakley and Chaum [BC85], pages 342–358. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=342. 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:1986:CKC

[Bri86] Ernest F. Brickell. The cryptanalysis of knapsack cryptosystems. In Ringeisen and Roberts [RR86], pages 3–23. ISBN 0-89871-219-X. LCCN QA76.9.M35C65 1986.

Brickell:1988:CKC

[Bri88] Ernest F. Brickell. The cryptanalysis of knapsack cryptosystems. In *Applications of discrete mathematics (Clemson, SC, 1986)*, pages 3–23. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1988.

Brown:1975:BL

[Bro75] Anthony Cave Brown. *Bodyguard of lies*. Harper & Row, New York, NY, USA, 1975. ISBN 0-06-010551-8. x + 947 + 8 pp. LCCN D810.S7 C36 1975.

Brownell:1981:ODN

[Bro81] George A. Brownell. *The origin and development of the National Security Agency*, volume 35 of *A cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1981. ISBN 0-89412-054-9. x + 98 pp. LCCN UB290 .B76 1981. Edited by Wayne G. Barker. Originally published as report of the Ad hoc Committee to Study the Communications Intelligence Activities of the United States, George A. Brownell, chairman.

Brooke:1986:BRB

[Bro86] N. Michael Brooke. Book review: *Mr. Babbage's secret: the tale of a Cypher — and APL*: O. I. Franksen. Strandbergs Forlag, Denmark (1984). 320 pp.

Dkr. 320.00. ISBN: 87-872-0086-4. *Information Processing and Management*, 22(1):67–68, ???? 1986. CODEN IPMADK. ISSN 0306-4573 (print), 1873-5371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/030645738690018X`.

Bryan:1967:CA

[Bry67] William G. Bryan. *Cryptographic ABC's*. Practical cryptanalysis; v. 4, 5. American Cryptogram Association, Greenfield, MA, USA, 1967.

Brillhart:1967:SFR

[BS67] John Brillhart and J. L. Selfridge. Some factorizations of $2^n \pm 1$ and related results. *Mathematics of Computation*, 21(97): 87–96, January 1967. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Branstad:1982:ISS

[BS82] Dennis K. Branstad and Miles E. Smid. Integrity and security standards based on cryptography. *Computers and Security*, 1(3):255–260, November 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/016740488290044X`.

Brickell:1983:SRK

[BS83] Ernest F. Brickell and Gustavus J. Simmons. A status report on knapsack based public key cryptosystems. *Congressus Numerantium*, 37:3–72, 1983. ISSN 0384-9864.

Benois:1986:CSE

[BS86] Michèle Benois and Jacques Sakarovitch. On the complexity of some extended word problems defined by cancellation rules. *Information Processing Letters*, 23(6):281–287, December 3, 1986. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Bateman:1989:NMC

[BSW89] 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

[Buc82] R. Creighton Buck. The public cryptography study group. *Computers and Security*, 1(3): 249–254, November 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404882900438`.

Budge:1922:RS

[Bud22] Sir E. A. Wallis (Ernest Alfred Wallis) Budge. *The Rosetta Stone*. British Museum Press, London, UK, 1922. 8 + 1 pp. LCCN PJ1531.R3 1913. Reprinted with revisions in 1935, 1950, and 1968.

Budge:1929:RSB

[Bud29] Sir E. A. Wallis(Ernest Alfred Wallis) Budge. *The Rosetta Stone in the British Museum: the Greek, Demotic and Hieroglyphic texts of the decree inscribed on the Rosetta Stone conferring additional honours on Ptolemy V. Epiphanes (203-181 B.C.) ...*. British Museum Press, London, UK, 1929. viii + 323 pp. LCCN PJ1531 .R3 1929. Reprinted with revisions in 1929, 1935, 1950, and 1968.

Budge:1976:RSB

[Bud76] Sir E. A. Wallis (Ernest Alfred Wallis) Budge. *The Rosetta stone in the British Museum: the Greek, demotic, and hieroglyphic texts of the decree inscribed on the Rosetta stone conferring additional honours on Ptolemy V Epiphanes (203-181 B.C.) with English translations and a short history of the decipherment of the Egyptian hieroglyphs, and an appendix containing translations of the stelae of San (Tanis) and Tall al-Maskhutah*. AMS Press, New York, NY, USA, 1976. ISBN 0-404-11362-1. 325 + 22 pp. LCCN PJ1531.R5 B8 1976.

Burchard:1981:NNF

[Bur81] Hank Burchard. News and notices: Finerman and Lee Receive ACM Awards; summer positions at Digital Computer Museum; CBI Fellowship 1982–1983; GMD activities in the history of computing; request for articles; Edwards speaks at Digital Computer Museum; exhibit of cipher machines. *Annals of the History of Computing*, 3(4):410–413, October/December 1981. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1981/pdf/a4410.pdf`.

Burton:1984:RPKa

[Bur84a] Charles E. Burton. RSA: a public key cryptography system part I. *Dr. Dobb's Journal of Software Tools*, 9(3): 16–??, March 1984. CODEN DDJOEB. ISSN 1044-789X.

Burton:1984:RPKb

[Bur84b] Charles E. Burton. RSA: a public key cryptography system part II. *Dr. Dobb's Journal of Software Tools*, 9(4):32–??, April 1984. CODEN DDJOEB. ISSN 1044-789X.

Burton:1985:EAC

[Bur85] Charles E. Burton. An enhanced ADFGVX cipher system. *Dr. Dobb's Journal of Software Tools*, 10(2):48–??, February 1985. CODEN DDJOEB. ISSN 1044-789X.

Burnham:1988:DES

[Bur88] B. Burnham. DES (data encryption standard) cryptographic services designed for the DOE wide band communications network. *Computers and Security*, 7(5): 510, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/016740488890212X`.

Brouwer:1982:NMK

[Bv82] Andries E. Brouwer and Peter van Emde Boas. A note on: "Master keys for group sharing" [Inform. Process. Lett. **12** (1981), no. 1, 23–25; MR 82d:94046] by D. E. Denning and F. B. Schneider. *Information Processing Letters*, 14(1): 12–14, March 27, 1982. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [DS81].

Beker:1985:KMS

[BW85] Henry Beker and Michael Walker. Key management for secure electronic funds transfer in a retail environment. In Blakley and Chaum [BC85], pages 401–410. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=??&volume=0&issue=0&spage=401`. 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.

Buchholz:1988:CQDc

[BWV+88] Werner Buchholz, Maurice V. Wilkes, Alfred W. Van Sinderen, C. J. Fern, Jr., and W. L. van der Poel. Comments, queries, and debate: Babbage and the Colossus; Babbage and Bowditch; Two Early European Computers; Early Dutch Computer. *Annals of the History of Computing*, 10(3):218–221, July/September 1988. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1988/pdf/a3218.pdf`; `http://www.computer.org/annals/an1988/a3218abs.htm`.

CBEMA:1981:ANS

[CA81] Computer and Business Equipment Manufacturers Association and American National Standards Institute. *American National Standard Data Encryption Algorithm*. American National Standards Institute, 1430 Broadway, New York, NY 10018, USA, December 30, 1981. 16 pp. LCCN ???? ANSI X3.92-1981.

CBEMA:1983:ANSb

[CA83a] Computer and Business Equipment Manufacturers Association and American National Standards Institute. American National Standard for Information Systems: Data Encryption Algorithm — modes of operation. ???? ANSI X3.106-1983, American National Standards Institute, 1430 Broadway, New York, NY 10018, USA, May 16, 1983. 16 pp.

CBEMA:1983:ANSa

[CA83b] Computer and Business Equipment Manufacturers Association and American National Standards Institute. American National Standard for Information Systems: Data link encryption. ???? ANSI X3.105-1983, American National Standards Institute, 1430 Broadway, New York, NY 10018, USA, May 16, 1983. 20 pp.

Calvocoressi:1980:TSU

[Cal80] Peter Calvocoressi. *Top secret ultra*. Pantheon Books, New York, NY, USA, 1980. ISBN 0-394-51154-9. 132 pp. LCCN D810.C88C34 1980.

Callimahos:1989:TAZ

[Cal89] Lambros D. Callimahos. *Traffic Analysis and the Zendian Problem: an exercise in communications intelligence operations*. Aegean Park Press, Laguna Hills, CA, USA, 1989. ISBN 0-89412-162-6, 0-89412-161-8 (paperback). 256 pp. LCCN ????

Callimahos:1992:HC

[Cal92] Lambros D. Callimahos. A history of cryptology. *Cryptolog*, 19(3):23–35, June 1992. ISSN 0740-7602. URL `https://archive.org/download/cryptolog_125/cryptolog_125.pdf`.

Campaigne:1971:REC

[Cam71] H. H. Campaigne. Reviews: *Elementary Cryptanalysis — A Mathematical Approach*, by Abraham Sinkov. *American Mathematical Monthly*, 78(4): 423, April 1971. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Campbell:1987:MBC

[Cam87] Q. G. Campbell. Meteor burst communications protocols — the history and role of computing technology in radio communication via meteor trails. Technical Report 246, University of Newcastle upon Tyne, Newcastle upon Tyne, UK, November 1987. ??–?? pp. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1007.html`.

Cammack:1988:MDE

[Cam88] William Ervin Cammack. Methods of data encryption and a random polygraphic cipher algorithm for ASCII files. Thesis, University of Southern Mississippi, Hattiesburg, MS, USA, 1988. vi + 108 pp.

Casson:1976:SAD

[Cas76] Lionel Casson. *The Story of Archaeological Decipherment, from Egyptian Hieroglyphs to Linear B* by Maurice Pope (review). *Technology and Culture*, 17(3):530–531, July 1976. CODEN TECUA3. ISSN 0040-165X (print), 1097-3729 (electronic). URL `https://muse.jhu.edu/pub/1/article/891767/pdf`.

Clark:1981:ECC

[CC81] George C. Clark, Jr. and J. Bibb Cain. *Error-correction coding for digital communications*. Plenum Press, New York, NY, USA; London, UK, 1981. ISBN 0-306-40615-2. xii + 422 pp. LCCN TK5102.5 .C52.

Chaum:1988:MUS

[CCD88] D. Chaum, C. Crepeau, and I. Damgård. Multiparty unconditionally secure protocols. In ACM [ACM88], pages 11–19. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988. ACM order no. 508880.

Coppersmith:1985:AF

[CD85] D. Coppersmith and J. H. Davenport. An application of factoring. *Journal of Symbolic Computation*, 1(2):241–243, June 1985. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic).

Chaum:1986:CRN

[CE86] David Chaum and Jan-Hendrik Evertse. Cryptanalysis of DES with a reduced number of rounds: sequences of linear factors in block ciphers. *Lecture Notes in Computer Science*, 218:192–211, 1986. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chaum:1987:DPD

[CEvdGP87] David Chaum, Jan-Hendrik Everse, Jeroem van de Graaf, and René Peralta. Demonstrating possession of a discrete logarithm without revealing it. In Odlyzko [Odl87b], pages 200–212. CODEN LNCSD9. ISBN 3-540-18047-8, 0-387-18047-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1986. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0263.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=263`. Conference held at the University of California, Santa Barbara, Aug. 11–15, 1986.

Chaum:1978:ICP

[CF78] D. L. Chaum and R. S. Fabry. Implementing capability-based protection using encryption. Technical Report UCB/ERL M78/46, University of California, Berkeley, Berkeley, CA, USA, 1978. i + 9 pp.

Christoffersson:1988:CUH

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

tographic protection in computer systems. Elsevier, Amsterdam, The Netherlands, 1988. ISBN 0-444-70484-1. vii + 93 pp. LCCN QA76.9.A25 C821 1988.

Coppersmith:1975:GCA

[CG75] Don Coppersmith and Edna Grossman. Generators for certain alternating groups with applications to cryptography. *SIAM Journal on Applied Mathematics*, 29(4):624–627, December 1975. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Chor:1985:RRL

[CG85] Benny Chor and Oded Goldreich. RSA/Rabin least significant bits are $\frac{1}{2} + \frac{1}{\mathrm{poly}(\log N)}$ secure (extended abstract). In Blakley and Chaum [BC85], pages 303–313. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=303`. 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.

Cover:1987:OPC

[CG87] Thomas M. Cover and B. Gopinath, editors. *Open Problems in Communication and Computation*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1987. ISBN 0-387-96621-8. LCCN TK5102.5 .O243 1987. US$25.00.

Chor:1988:UBS

[CG88] Benny Chor and Oded Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM Journal on Computing*, 17(2):230–261, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Chor:1985:VSS

[CGMA85] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In IEEE [IEE85], pages 383–395 (or 335–344??). ISBN 0-8186-0644-4 (paperback), 0-8186-4644-6 (microfiche), 0-8186-8644-8 (hardcover). LCCN QA 76 S979 1985.

Chaum:1979:UEM

[Cha79] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Thesis (M.S. in Computer Science), University of California, Berkeley, Berkeley, CA, USA, June 1979.

Chaum:1981:UEM

[Cha81] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the Association for Computing Machinery*, 24(2):84–88, February 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1019.html`.

Chandler:1983:IMC

[Cha83a] W. W. Chandler. The installation and maintenance of Colossus. *Annals of the History of Computing*, 5(3):260–262, July/September 1983. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1983/pdf/a3260.pdf; http://www.computer.org/annals/an1983/a3260abs.htm`.

Chaum:1983:BSU

[Cha83b] D. Chaum. Blind signatures for untraceable payments. In ????, editor, *Advances in Cryptology, Proceedings of CRYPTO 82*, pages 199–203. Plenum Press, New York, NY, USA; London, UK, 1983.

Chaum:1985:HKS

[Cha85a] David Chaum. How to keep a secret alive extensible partial key, key safeguarding, and threshold systems. In Blakley and Chaum [BC85], pages 481–485. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=481`. 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.

Chaum:1985:NSC

[Cha85b] David Chaum. New secret codes can prevent a computerized big brother. In Blakley and Chaum [BC85], pages 432–433. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=432`. 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.

Chaum:1985:SIT

[Cha85c] David Chaum. Security with-

out identification: transaction systems to make big brother obsolete. *Communications of the Association for Computing Machinery*, 28(10):1030–1044, October 1985. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/4373.html`; `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1022.html`.

Chang:1986:DKL

[Cha86a] C. C. Chang. On the design of a key-lock-pair mechanism in information protection systems. *BIT*, 26(4):410–417, 1986. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic).

Chapman:1986:NFS

[Cha86b] J. W. M. Chapman. No final solution: a survey of the cryptanalytical capabilities of German military agencies, 1926–35. *Intelligence and National Security*, 1(1):13–??, 1986. ISSN 0268-4527 (print), 1743-9019 (electronic).

Chesson:1973:CC

[Che73] F. W. (Frederick William) Chesson. Computers and cryptology. *Datamation*, ??(??):62–77, January 1973. CODEN DTMNAT. ISSN 0011-6963.

Chor:1986:TIP

[Cho86] Ben-Zion Chor. *Two issues in public key cryptography: RSA bit security and a new knapsack type system*. ACM distinguished dissertations. MIT Press, Cambridge, MA, USA, 1986. ISBN 0-262-03121-3. 78 pp. LCCN TK5102.5 .C4781 1986. Originally presented as the author's thesis (doctoral — MIT, 1985).

Christiansen:1978:SL

[Chr78] D. Christiansen. Spectral lines. *IEEE Spectrum*, 15(1):23, January 1978. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Christoffersson:1988:MAE

[Chr88] Per Christoffersson. Message authentication and encryption combined. *Computers and Security*, 7(1):65–71, February 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888905056`.

Chuang:1989:NES

[Chu89] Ta-Fu Chuang. *Non-homomorphic encryption schemes and properties of Chinese remainder theorem*. Thesis (Ph.D. in engineering), University of Wisconsin-Milwaukee, Milwaukee, WI, USA, 1989. vi + 58 pp.

Ciarcia:1986:BHD

[Cia86] Steve Ciarcia. Build a hardware data encryptor. *BYTE Magazine*, 11(??):??, ?? 1986. CODEN BYTEDJ. ISSN 0360-5280.

Chan:1988:IEC

[CL88] Yeng Kit Chan and Rudolf Lidl. On implementing elliptic curve cryptosystems. In *Contributions to general algebra, 6*, pages 155–166. Hölder-Pichler-Tempsky, Vienna, 1988.

Claudy:1912:TMS

[Cla12] C. H. Claudy. A triple mirror for secret signaling. *Scientific American*, 107(17):346, October 26, 1912. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL `http://www.nature.com/scientificamerican/journal/v107/n17/pdf/scientificamerican10261912-346.pdf`.

Clark:1977:MWBa

[Cla77a] Ronald William Clark. *The man who broke Purple: the life of Colonel William F. Friedman, who deciphered the Japanese code in World War II.* Little, Brown, Boston, MA, USA, 1977. ISBN 0-316-14595-5. ix + 271 pp. LCCN UB290 .C58 1977.

Clark:1977:MWBb

[Cla77b] Ronald William Clark. *The man who broke Purple: the life of the world's greatest cryptologist, Colonel William F. Friedman.* Weidenfeld and Nicolson, London, UK, 1977. ISBN 0-297-77279-1. xi + 212 + 4 pp. LCCN UB290 .C58 1977b.

Culik:1979:SIS

[CM79] K. Culik, II and H. A. Maurer. Secure information storage and retrieval using new results in cryptography. *Information Processing Letters*, 8(4): 181–186, April 30, 1979. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Ciampi:1982:EVS

[CM82] Constantino Ciampi and A. A. Martino, editors. *Edited versions of selected papers from the International Conference on "Logic, Informatics, Law," Florence, Italy, April 6–10, 1981.* Elsevier Science Publishers, Amsterdam, The Netherlands, 1982. ISBN 0-444-86413-X (set), 0-444-86414-8 (vol. 1), 0-444-86415-6 (vol. 2). LCCN K662.I4 I58. Two volumes. Vol. 1: Artificial intelligence and legal information systems. Vol. 2: Deontic logic, computational linguistics, and legal information systems.

Chan:1985:NMP

[CM85] B. Chan and H. Meijer. A note on the method of puzzles for key distribution. *International Journal of Computer and Information Sciences*, 14(4):221–223, August 1985. CODEN IJCIAH. ISSN 0091-7036.

Chor:1989:SCT

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

Journal of the Association for Computing Machinery, 36(3): 591–614, July 1989. CODEN JACOAH. ISSN 0004-5411. URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/65956.html`. **Review: Computing Reviews**, June 1990.

Crilly:1987:BPB

[CN87] Tony Crilly and Shekhar Nandy. The birthday problem for boys and girls. *The Mathematical Gazette*, 71(455): 19–22, March 1987. CODEN MAGAAS. ISSN 0025-5572. URL `http://links.jstor.org/sici?sici=0025-5572%28198703%292%3A71%3A455%3C19%3ATBPFBA%3E2.0.CO%3B2-7`.

Cohen:1987:CCI

[Coh87a] Fred Cohen. A cryptographic checksum for integrity protection. *Computers and Security*, 6(6):505–510, December 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404887900319`.

Cohen:1987:IIP

[Coh87b] Fred Cohen. *Introductory Information Protection*. ????, ????, 1987. ISBN ???? ???? pp. LCCN ???? URL `http://all.net/books/ip/`.

Colaco:1864:CRO

[Col64] F. N. Colaço. *A cryptographia revelada, ou, Arte de traduzir e decifrar as escrituras obscuras, quaesquer que sejao os caracteres empregados. (Portuguese) [Cryptography revealed, or, the art of translating and deciphering obscure writings, whatever the characters employed]*. De Santos e Cia, Pernambuco, Brazil, 1864. 93 pp. LCCN Z104 .C68 1846.

CPI:1976:CMS

[Com76] Computation Planning Incorporated. Cryptopak: modular subroutine library for cryptographic transformation. Report, Computation Planning Incorporated, Bethesda, MD, USA, 1976.

Cominsky:1987:CAP

[Com87] Isabeth Cominsky. Cryptology: ancient problem modern solutions. Thesis (M.S.), State University of New York, College of Technology at Utica/Rome, Utica/Rome, NY, USA, 1987. iv + 91 pp.

Conradi:1739:CDS

[Con39] David Arnold Conradi. *Cryptographia denudata; sive, Ars deciferandi, quae occulte scripta sunt in quocunque linguarum genere, praecipue in Germanica, Batava, Latina, Anglica, Gallica, Italica, Graeca*. Apud P. Bonk, Lugduni Batavorum, 1739. 73 pp. LCCN Z103 .C66.

Coombs:1983:MC

[Coo83] Allen W. M. Coombs. The making of Colossus. *Annals of the History of Com-*

puting, 5(3):253–259, July/ September 1983. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1983/pdf/a3253.pdf; http://www.computer.org/annals/an1983/a3253abs.htm`.

Coppersmith:1984:FEL

[Cop84] D. Coppersmith. Fast evaluations of logarithms in fields of characteristic two. *IEEE Transactions on Information Theory*, IT-30(4):587–594, ???? 1984. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Coppersmith:1987:C

[Cop87] D. Coppersmith. Cryptography. *IBM Journal of Research and Development*, 31(2): 244–248, March 1987. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Coppersmith:1989:AID

[Cop89] D. Coppersmith. Analysis of ISO/CCITT document X.509 annex D. Internal memo., IBM T. J. Watson Center, Yorktown Heights, NY, USA, June 11, 1989. ?? pp.

Coppersmith:1986:DL

[COS86] Don Coppersmith, Andrew M. Odlyzko, and Richard Schroeppel. Discrete logarithms in GF(p). *Algorithmica*, 1(1):1–15, 1986. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Courville:1986:MCC

[Cou86] Joseph B. Courville. *Manual for cryptanalysis of the columnar double transposition cipher: a study of cryptanalysis*. J. B. Courville, 10240 Virginia Ave, South Gate, CA, 90280, USA, 1986. iv + 91 pp.

Chaum:1987:ACE

[CP87] David Chaum and Wyn L. Price, editors. *Advances in Cryptology–EUROCRYPT '87: Workshop on the Theory and Application of Cryptographic Techniques, Amsterdam, The Netherlands, April 13–15, 1987: Proceedings*, volume 304 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1987. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). LCCN QA76.9.A25 E963 1987.

Chaum:1988:ACE

[CP88] David Chaum and Wyn L. Price, editors. *Advances in cryptology — EUROCRYPT '87: Workshop on the Theory and Application of Cryptographic Techniques, Amsterdam, The Netherlands, April 13–15, 1987: proceedings*, volume 304 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988. CODEN LNCSD9. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). ISSN 0302-9743

(print), 1611-3349 (electronic). LCCN QA76.9.A25 E9631 1987; QA267.A1 L43 no.304. Sponsored by the International Association for Crytologic Research.

Chor:1985:KTP

[CR85] 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. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=54`. See also revised version in [CR88c].

Carroll:1988:ACP

[CR88a] John M. Carroll and Lynda Robbins. The automated cryptananysis of polyalphabetic ciphers. *Computers and Security*, 7(1):104, February 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888905354`.

Carroll:1988:CC

[CR88b] John M. Carroll and Lynda E. Robbins. Computer cryptanalysis. Report 223, Department of Computer Science, University of Western Ontario, London, UK, 1988. ISBN 0-7714-1070-0. 55 pp.

Chor:1988:KTP

[CR88c] Benny Chor and Ronald L. Rivest. A knapsack-type public key cryptosystem based on arithmetic in finite fields. *IEEE Transactions on Information Theory*, IT-34(5, part 1):901–909, 1988. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Chaum:1983:ACP

[CRS83] David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors. *Advances in Cryptology: proceedings of CRYPTO 82*. Plenum Press, New York, NY, USA; London, UK, 1983. ISBN 1-4757-0604-9 (print), 1-4757-0602-2. LCCN QA76.9.A25 C79 1982.

Crypto:1981:ACP

[CRY81] *Advances in cryptology: proceedings of CRYPTO*, page various, 1981. Plenum Press, New York, NY, USA; London, UK. Volumes for 1984 to 1989 were published in the Springer-Verlag Lecture Notes in Computer Science series.

Cesarini:1983:ACC

[CS83] F. Cesarini and G. Soda. An algorithm to construct a compact B-tree in case of ordered keys. *Information Processing Letters*, 17(1):13–16, July 19, 1983. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Chaum:1989:SCF

[CSB89] David Chaum and Ingrid Schaumuller-Bichl, editors. *Smart card 2000: the future of IC cards: proceedings of the IFIP WG 11.6 International Conference on Smart Card 2000–the Future of IC Cards, Laxenburg, Austria, 19–20 October 1987*. North-Holland, Amsterdam, The Netherlands, 1989. ISBN 0-444-70545-7. LCCN TK7895.S62 I35 1987.

Ciminiera:1989:AMM

[CV89] L. Ciminiera and A. Valenzano. Authentication mechanisms in microprocessor-based local area networks. *IEEE Transactions on Software Engineering*, 15(5):654–658, May 1989. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=24716`.

DeMillo:1983:ACC

[D+83] Richard A. DeMillo et al. *Applied cryptology, cryptographic protocols, and computer security models*, volume 29 of *Proceedings of symposia in applied mathematics. AMS short course lecture notes*. American Mathematical Society, Providence, RI, USA, 1983. ISBN 0-8218-0041-8. ISSN 0160-7634. xi + 192 pp. LCCN QA1 .A56 v.29 1981. Expanded version of notes prepared for the AMS short course entitled Cryptology in revolution, mathematics and models, held in San Francisco, CA, Jan. 5–6, 1981, by Richard A. DeMillo and others.

DAgapeyeff:1939:CC

[D'A39] Alexander D'Agapeyeff. *Codes and ciphers*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1939. 160 pp. LCCN Z104 .D3 1939.

DAgapeyeff:1971:CC

[D'A71] Alexander D'Agapeyeff. *Codes and ciphers*. Gryphon Books, Ann Arbor, MI, USA, 1971. ISBN ???? 160 pp. LCCN Z103 .D35 1971. Reprint of [D'A39].

DRC:1985:AAN

[Dat85] Datapro Research Corporation. *All about network access control and data encryption devices: with in-depth analyses of leading devices*. Datapro Research Corporation, Delran, NJ, USA, June 1985. 65 pp.

Davida:1979:IHS

[Dav79] G. I. Davida. III. 'Hellman's scheme breaks DES in its basic form'. *IEEE Spectrum*, 16 (7):39, July 1979. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Davida:1981:CAR

[Dav81] 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

[Dav85] Donald Watts Davies. A message authenticator algorithm suitable for a mainframe computer. In Blakley and Chaum [BC85], pages 393–400. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=393`. 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.

Dawson:1985:COL

[Daw85] M. J. Dawson. *Cryptanalysis of ornithological literature*, volume 4 of *Caliologists' series*. Oriel Stringer, Brighton, 1985. ISBN 0-948122-04-8 (paperback). 40 pp. LCCN ????

Denning:1981:SRR

[DB81] Peter J. Denning and David H. Brandin. Special report: Report of the Public Cryptography Study Group. *Communications of the Association for Computing Machinery*, 24 (7):434, July 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

denBoer:1988:CF

[dB88] Bert den Boer. Cryptanalysis of F.E.A.L. *Lecture Notes in Computer Science*, 330:293–299, 1988. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Denning:1989:EET

[DB89] Dorothy Elizabeth Robling Denning and William E. Baugh, Jr. *Encryption and evolving technologies: tools of organized crime and terrorism*. US Working Group on Organized Crime monograph series. National Strategy Information Center, Washington, DC, USA, 1989. ISSN 1093-7269. ii + 52 pp.

deJonge:1986:ASR

[dC86] W. de Jonge and D. Chaum. Attacks on some RSA signatures. In Williams [Wil86b], pages 18–27. CODEN LNCSD9. ISBN 0-387-16463-4 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1985; QA267.A1 L43 no.218. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0218.htm`; `http://www.springerlink.com/content/978-0-387-16463-2`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=218`.

deJonge:1987:SVR

[dC87] Wiebren de Jonge and David Chaum. Some variations on RSA signatures & their security. In Odlyzko [Odl87b], pages 49–59. CODEN LNCSD9. ISBN 3-540-18047-8, 0-387-18047-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1986. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0263.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=263`. Conference held at the University of California, Santa Barbara, Aug. 11–15, 1986.

Davio:1985:EHS

[DDG+85] Marc Davio, Yvo Desmedt, Jo Goubert, Frank Hoornaert, and Jean-Jacques Quisquater. Efficient hardware and software implementations for the DES. In Blakley and Chaum [BC85], pages 144–146. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=144`. 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.

Delsarte:1985:FCM

[DDOP85] P. Delsarte, Y. Desmedt, A. Odlyzko, and P. Piret. Fast cryptanalysis of the Matsumoto–Imai public key scheme. In Beth et al. [BCI85], pages 142–149. CODEN LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E951 1984. URL `http://www.research.att.com/~amo/doc/arch/break.mi.scheme.pdf; http://www.research.att.com/~amo/doc/arch/break.mi.scheme.ps; http://www.research.att.com/~amo/doc/arch/break.mi.scheme.troff`. Held at the University of Paris, Sorbonne.

deVries:1953:SMC

[de 53] M. de Vries. *Statistical methods in cryptanalysis*. Rapport ZW 1953-014. Math. Centrum Amsterdam, Amsterdam, The Netherlands, 1953. 15 pp.

Deavours:1987:CPI

[Dea87] Cipher A. Deavours. *Cryptanalytic programs for the IBM PC*. A Cryptographic series. Aegean Park Press, Laguna Hills, CA, USA, 1987. 44 pp.

Deavours:1988:BPS

[Dea88] Cipher A. Deavours. *Breakthrough '32: the Polish solution of the Enigma*, volume 51 of *A Cryptographic series*. Aegean

Park Press, Laguna Hills, CA, USA, 1988. ISBN 0-89412-152-9 (paperback). v + 85 pp. LCCN ????

Demirdogen:1988:FDM

[Dem88] A. Caner Demirdogen. Flaw detection methods based on digital signature analysis for rotating machinery quality control. Thesis (M.S.), Tennessee Technological University, Cookeville, TN, USA, 1988. xii + 189 pp.

Denning:1979:SPC

[Den79a] Dorothy E. Denning. Secure personal computing in an insecure network. *Communications of the Association for Computing Machinery*, 22(8): 476–482, August 1979. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Denning:1979:EOS

[Den79b] Peter J. Denning. Editor's overview — special section on data encryption. *ACM Computing Surveys*, 11(4):283, December 1979. CODEN CMSVAN. ISSN 0010-4892.

Denning:1982:CDS

[Den82] Dorothy Elizabeth Robling Denning. *Cryptography and data security*. Addison-Wesley, Reading, MA, USA, 1982. ISBN 0-201-10150-5. xiii + 400 pp. LCCN QA76.9.A25 .D46 1982. US$22.95.

Denning:1984:DSR

[Den84a] Dorothy E. Denning. Digital signatures with RSA and other public-key cryptosystems. *Communications of the Association for Computing Machinery*, 27 (4):388–392, April 1984. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Denning:1984:FEA

[Den84b] Dorothy E. Denning. Field encryption and authentication. In *Advances in cryptology (Santa Barbara, Calif., 1983)*, pages 231–247. Plenum Press, New York, NY, USA; London, UK, 1984.

Denniston:1986:GCC

[Den86] A. G. Denniston. The Government Code and Cypher School between the Wars. *Intelligence and National Security*, 1 (1):48–??, 1986. ISSN 0268-4527 (print), 1743-9019 (electronic).

Desmedt:1988:SGC

[Des88] Y. Desmedt. Society and group-oriented cryptography: a new concept. In Pomerance [Pom88], pages 120–127. CODEN LNCSD9. ISBN 0-387-18796-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1987; QA267.A1 L43 no.293. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0293.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&`

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.

Davison:1957:SCG

[DG57] W. H. T. Davison and M. Gordon. Sorting for chemical groups using Gordon–Kendall–Davison ciphers. *American Documentation*, 8(3):202–210, July 1957. CODEN AMDOA7. ISSN 0096-946X.

Diffie:1976:CPD

[DH76a] Whitfield Diffie and Martin E. Hellman. A critique of the proposed Data Encryption Standard. *Communications of the Association for Computing Machinery*, 19(3):164–165, March 1976. URL https://dl.acm.org/doi/pdf/10.1145/360018.360031.

Diffie:1976:NDC

[DH76b] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, November 1976. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic). URL https://ee.stanford.edu/~hellman/publications/24.pdf.

Diffie:1976:PKC

[DH76c] Whitfield Diffie and Martin E. Hellman. Public key cryptography. In IEEE, editor, *IEEE International Symposium on Information Theory, June 21–24, 1976, Ronneby, Sweden*, page ?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1976.

Diffie:1977:ECN

[DH77] Whitfield Diffie and Martin E. Hellman. Exhaustive cryptanalysis of the NBS Data Encryption Standard. *Computer*, 10 (6):74–84, June 1977. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Davis:1985:NRI

[DH85a] J. A. Davis and D. B. Holdridge. New results on integer factorizations. *Congressus Numerantium*, 46:65–78, 1985. ISSN 0384-9864. Proceedings of the fourteenth Manitoba conference on numerical mathematics and computing (Winnipeg, Man., 1984).

Davis:1985:UFS

[DH85b] J. A. Davis and D. B. Holdridge. An update on factorization at Sandia National Laboratories. In Blakley and Chaum [BC85], page 114. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=

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.

Diffie:1980:CAM

[DHM80] B. W. Diffie, M. E. Hellman, and R. C. Merkle. Cryptographic apparatus and method. US Patent No. 4,200,770A., April 29, 1980. URL `https://www.google.com/patents/US4200770`. Patent filed 6 September 1977.

Dieringer:1988:TAE

[Die88] Jeffrey A. Dieringer. Tools for analog encryption. Thesis (M.S. in Computer Science), University of Wisconsin-Milwaukee, Milwaukee, WI, USA, 1988. vi + 93 pp.

Diffie:1975:PRN

[Dif75] Whitfield Diffie. Preliminary remarks on the National Bureau of Standards proposed standard encryption algorithm for computer data protection. Unpublished report, Stanford University, Stanford, CA, USA, May 1975.

Diffie:1982:CVP

[Dif82a] Whitfield Diffie. Conventional versus public key cryptosystems. In *Secure communications and asymmetric cryptosystems*, volume 69 of *AAAS Sel. Symp. Ser.*, pages 41–72. Westview, Boulder, CO, 1982.

Diffie:1982:CTF

[Dif82b] Whitfield Diffie. Cryptographic technology: fifteen year forecast. *ACM SIGACT News*, 14(4):38–57, Fall–Winter 1982. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Diffie:1988:FTY

[Dif88] Whitfield Diffie. The first ten years of public-key cryptography. *Proceedings of the IEEE*, 76:560–576, 1988. CODEN IEEPAD. ISSN 0018-9219.

Deavours:1985:MCM

[DK85] Cipher A. Deavours and Louis Kruh. *Machine cryptography and modern cryptanalysis*. The Artech House telecom library. Artech House Inc., Norwood, MA, USA, 1985. ISBN 0-89006-161-0. xiv + 258 pp. LCCN Z103 .D431 1985.

Deavours:1989:CMH

[DK+89] Cipher A. Deavours, David Kahn, et al., editors. *Cryptology: machines, history, & methods*. Artech House Inc., Norwood, MA, USA, 1989. ISBN 0-89006-399-0. x + 508 pp. LCCN Z103 .C75 1989. Second volume of selected papers from issues of Cryptologia.

Deavours:1987:CYT

[DKKM87] Cipher A. Deavours, David Kahn, Louis Kruh, and Greg

Mellen, editors. *Cryptology yesterday, today, and tomorrow*. The Artech House communication and electronic defense library. Artech House Inc., Norwood, MA, USA, 1987. ISBN 0-89006-253-6. xi + 519 pp. LCCN Z103.C76 1987. US$60.00. First volume of selected papers from issues of Cryptologia.

DeMillo:1982:CP

[DLM82] Richard A. DeMillo, Nancy A. Lynch, and Michael J. Merritt. Cryptographic protocols. In ACM [ACM82], pages 383–400. ISBN 0-89791-070-2. LCCN QA75.5 .A14 1982. ACM order no. 508820.

delaStelle:1902:TCF

[dlS02] Félix-Marie de la Stelle. *Traité de cryptographie. (French) [Treatise on cryptography]*. Gauthier-Villars, Paris, France, 1902. ???? pp.

DeMillo:1983:PDS

[DM83] R. DeMillo and M. Merritt. Protocols for data security. *Computer*, 16(2):39–50, February 1983. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1004.html`.

Denning:1981:MMK

[DMS81] D. E. Denning, H. Meijer, and F. B. Schneider. More on master keys for group sharing. *Information Processing Letters*, 13(3): 125–126, December 13, 1981. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Desmedt:1986:CTA

[DO86] Y. G. Desmedt and A. M. Odlyzko. A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes. In Williams [Wil86b], pages 516–522. CODEN LNCSD9. ISBN 0-387-16463-4 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1985; QA267.A1 L43 no.218. URL `http://www.research.att.com/~amo/doc/arch/rsa.attack.pdf`; `http://www.research.att.com/~amo/doc/arch/rsa.attack.ps`; `http://www.research.att.com/~amo/doc/arch/rsa.attack.troff`.

Desmedt:1985:DOI

[DQD85] Yvo Desmedt, Jean-Jacques Quisquater, and Marc Davio. Dependence of output on input in DES: Small avalanche characteristics. In Blakley and Chaum [BC85], pages 359–376. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=359`. CRYPTO 84: a Workshop on the Theory and Appli-

cation of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Dreher:1979:PSC

[Dre79] Felix F. Dreher. Privacy and security in computer based systems using encryption. Pittsburg State University. School of Business monograph series 7, Pittsburg State University. Gladys A. Kelce School of Business and Economics., Pittsburg, KS, USA, 1979. 8 pp.

deRaadt:1999:COO

[dRHG+99] Theo de Raadt, Niklas Hallqvist, Artur Grabowski, Angelos D. Keromytis, and Niels Provos. Cryptography in OpenBSD: An overview. In USENIX [USE99], pages 93–101. ISBN 1-880446-33-2. LCCN A76.8.U65 U843 1999. URL `http://www.openbsd.org/papers/crypt-paper.ps`.

Dror:1989:SCG

[Dro89] Asael Dror. Secret codes (any good data security system must rely on encryption). *BYTE Magazine*, 14(6):267–270, June 1989. CODEN BYTEDJ. ISSN 0360-5280.

Denning:1981:MKG

[DS81] Dorothy E. Denning and Fred B. Schneider. Master keys for group sharing. *Information Processing Letters*, 12(1):23–25, February 13, 1981. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See also note [Bv82].

Dolev:1983:AAB

[DS83] D. Dolev and H. R. Strong. Authenticated algorithms for Byzantine agreement. *SIAM Journal on Computing*, 12(4): 656–666, ???? 1983. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

duCarlet:1644:CCV

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

Davida:1981:DES

[DWK81] George I. Davida, David L. Wells, and John B. Kam. A database encryption system with subkeys. *ACM Transactions on Database Systems*, 6(2):312–328, June 1981. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1981-6-2/p312-davida/p312-davida.pdf`; `http://www.acm.org/pubs/citations/journals/tods/1981-6-2/p312-davida/`.

Ecker:1982:MGE

[Eck82] A. Ecker. Über die mathematischen Grundlagen einiger Chiffrierverfahren. (German) [On the mathematical foundations of some cryptosystems]. *Computing*, 29(4):277–287, 1982. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Ecker:1983:FSR

[Eck83] A. Ecker. Finite semigroups and the RSA-cryptosystem. *Lecture Notes in Computer Science*, 149:353–369, 1983. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ecker:1985:STS

[Eck85] Allen Ecker. Satellite television, signal encryption and the future of broadband distribution. Seminar notes, Communications Forum, Massachusetts Institute of Technology, Cambridge, MA, USA, September 19, 1985. 13 pp.

Ellis:1975:PKC

[ECW75] James Ellis, Clifford Cocks, and Malcolm Williamson. Public-key cryptography. Classified reports (titles uncertain) at Government Communications Headquarters (GCHQ), Cheltenham, UK., 1975. URL `http://www.gchq.gov.uk/Press/Pages/100th-IEEE-milestone-award.aspx`. Work declassified in 1997. Awarded the 100th IEEE Milestone Award for the first discovery (albeit long secret) of public-key cryptography.

Edwards:1915:CCT

[Edw15] E. C. Edwards. Cipher codes and their uses. *Scientific American*, 113(1):9, July 3, 1915. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL `http://www.nature.com/scientificamerican/journal/v113/n1/pdf/scientificamerican07031915-9.pdf`.

Epstein:1956:FBC

[EE56] Sam Epstein and Beryl Epstein. *The first book of codes and ciphers*. Franklin Watts, New York, NY, USA, 1956. LCCN Z104 .E68. Pictures by Laszlo Roth.

El-Gamal:1985:PCS

[EG85a] T. El-Gamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, IT-31(4): 469–472, 1985. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Even:1985:PCC

[EG85b] S. Even and O. Goldreich. On the power of cascade ciphers. *ACM Transactions on Computer Systems*, 3(2): 108–116, May 1985. CODEN ACSYEC. ISSN 0734-2071. URL `http://www.acm.org:80/pubs/citations/journals/tocs/1985-3-2/p108-even/`.

Even:1985:RPS

[EGL85] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Communications of the Association for Computing Machinery*, 28(6): 637–647, June 1985. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/3818.html`.

Ellison:2000:PSK

[EHMS00] Carl Ellison, Chris Hall, Randy Milbert, and Bruce Schneier. Protecting secret keys with personal entropy. *Future Generation Computer Systems*, 16(4): 311–318, February 2000. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.counterpane.com/personal-entropy.pdf; http://www.elsevier.com/gej-ng/10/19/19/41/27/26/abstract.html`.

Eigenthaler:1984:CGA

[EKMN84] G. Eigenthaler, H. K. Kaiser, W. B. Müller, and W. Nöbauer., editors. *Contributions to general algebra, 3. Proceedings of the Vienna conference held in Vienna, June 21–24, 1984.* Hölder-Pichler-Tempsky, Vienna, Austria, 1984. ISBN 3-209-00591-5, 3-519-02762-3. LCCN ????

Evans:1974:UAS

[EKW74] Arthur Evans, Jr., William Kantrowitz, and Edwin Weiss. A user authentication scheme not requiring secrecy in the computer. *Communications of the Association for Computing Machinery*, 17(8):437–442, August 1974. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

ElGamal:1985:PKCa

[ElG85a] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, IT-31(4): 469–472, 1985. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

ElGamal:1985:PKCb

[ElG85b] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In Blakley and Chaum [BC85], pages 10–18. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=10`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

ElGamal:1985:STA

[ElG85c] Taher ElGamal. A subexponential-time algorithm for computing discrete logarithms over GF(p^2). *IEEE Transactions on Information Theory*, IT-31(4): 473–481, 1985. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Elvin:1987:CWW

[Elv87] Robert Scott Elvin. A cryptanalysis 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.).

Ehrsam:1978:CKM

[EMMT78] William F. Ehrsam, Stephen M. Matyas, Carl H. Meyer, and Walter L. Tuchman. A cryptographic key management scheme for implementing the Data Encryption Standard. *IBM Systems Journal*, 17(2):106–125, 1978. CODEN IBMSA7. ISSN 0018-8670.

Er:1989:NAG

[Er89] M. C. Er. A new algorithm for generating binary trees using rotations. *The Computer Journal*, 32(5):470–473, October 1989. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_32/Issue_05/tiff/470.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_32/Issue_05/tiff/471.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_32/Issue_05/tiff/472.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_32/Issue_05/tiff/473.tif`.

Erdem:1986:HCO

[Erd86] Hilmi Erdem. Host cryptographic operations: a software implementation. *Computers and Security*, 5(4):344–346, December 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/016740488690057X`.

Estell:1980:BW

[Est80] Robert G. Estell. Benchmarks and watermarks. *ACM SIGMETRICS Performance Evaluation Review*, 9(3):39–44, Fall 1980. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Even:1985:CSW

[Eve85] Shimon Even. On the complexity of some word problems that arise in testing the security of protocols. In Apostolico and Galil [AG85], pages 299–314. ISBN 0-387-15227-X. LCCN QA164 .N35 1984.

Even:1998:FVA

[Eve98] S. Even. Four value-adding algorithms. *IEEE Spectrum*, 35(5):33–38, May 1998. CO-

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

Faak:1986:SVH

[Fåk86] Viiveke Fåk. Software versus hardware encryption — is there any difference today? *Computers and Security*, 5(2):167, June 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404886901434`.

Faak:1987:CMM

[Fåk87] Viiveke Fåk. Crypto management made manageable — demands on crypto equipment design. *Computers and Security*, 6 (1):36–40, February 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404887901234`.

Falk:1988:DST

[Fal88] Adam Falk. DBMS security through encryption. Thesis (M.S.), San Francisco State University, San Francisco, CA, USA, 1988. xii + 295 pp.

Farago:1967:BSS

[Far67] Ladislas Farago. *The broken seal: the story of Operation Magic and the Pearl Harbor disaster*. Random House, New York, NY, USA, 1967. 439 pp. LCCN D742.U5 F3. See also reprint [Far69].

Farago:1969:BSS

[Far69] Ladislas Farago. *The broken seal: the story of Operation Magic and the Pearl Harbor disaster*. Mayflower, London, UK, 1969. 415 pp. LCCN D742.U5 F3. Reprint of [Far67].

Feak:1983:SIS

[Fêa83] Viiveke Fêak, editor. *Security, IFIP/Sec'83: proceedings of the First Security Conference, Stockholm, Sweden, 16–19 May 1983*. North-Holland, Amsterdam, The Netherlands, 1983. ISBN 0-444-86669-8 (Elsevier). LCCN QA76.9.A25 S4 1983.

Feistel:1970:CCD

[Fei70] Horst Feistel. Cryptographic coding for data-bank privacy. Research Report RC-2827, IBM T. J. Watson Research Center, Yorktown Heights, NY, USA, March 18, 1970.

Feistel:1973:CCP

[Fei73] Horst Feistel. Cryptography and computer privacy. *Scientific American*, 228(5):15–23, May 1973. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Feistel:1974:BCC

[Fei74] Horst Feistel. Block cipher cryptographic system. U.S. Patent No. 3,798,359., March 19, 1974.

Feldman:1987:PSN

[Fel87] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In IEEE [IEE87a],

pages 427–437. ISBN 0-8186-0807-2, 0-8186-4807-4 (fiche), 0-8186-8807-6 (case). LCCN QA 76 S979 1987.

Ferris:1987:WBC

[Fer87] John Ferris. Whitehall's Black Chamber: British cryptology and the Government Code and Cypher School, 1919–29. *Intelligence and National Security*, 2 (1):54–??, 1987. ISSN 0268-4527 (print), 1743-9019 (electronic).

Feynman:1982:SPC

[Fey82] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6–7):467–488, 1982. CODEN IJTPBM. ISSN 0020-7748. Physics of computation, Part II (Dedham, Mass., 1981).

Friedman:1957:SCE

[FF57] William F. (William Frederick) Friedman and Elizebeth S. (Elizebeth Smith) Friedman. *The Shakespearean Ciphers Examined: an analysis of cryptographic systems used as evidence that some author other than William Shakespeare wrote the plays commonly attributed to him*. Cambridge University Press, New York, NY, USA, 1957. 4 + vii–xvi + 1 + 302 + 1 pp. LCCN PR2937 .F7.

Friedman:1955:CLS

[FFW55] William F. (William Frederick) Friedman, Elizebeth Friedman, and Louis B. (Louis Booker) Wright. *The cryptologist looks at Shakespeare*. ????, ????, 1955. ???? pp. LCCN ???? Original typescript, awarded Folger literary prize, 1955.

Friedman:1974:ETR

[FH74] Theodore D. Friedman and Lance J. Hoffman. Execution time requirements for encipherment programs. *Communications of the Association for Computing Machinery*, 17 (8):445–449, August 1974. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See letter [McC75].

Frederickson:1984:PRT

[FHJ+84] P. Frederickson, R. Hiromoto, T. L. Jordan, B. Smith, and T. Warnock. Pseudo-random trees in Monte Carlo. *Parallel Computing*, 1(2):175–180, December 1984. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

Frieze:1988:RTI

[FHK+88] Alan M. Frieze, Johan Håstad, Ravi Kannan, Jeffrey C. Lagarias, and Adi Shamir. Reconstructing truncated integer variables satisfying linear congruences. *SIAM Journal on Computing*, 17(2):262–280, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Filby:1977:TPT

[Fil77] P. William Filby. Teaching Purple to talk saved thousands. *Baltimore Sun*, ??(??):??, October 16, 1977. Review of *The Man Who Broke Purple*, by Ronald Clark.

Filby:1978:BRM

[Fil78] P. William Filby. Book review: *The Man Who Broke Purple*, by Ronald Clark, 271 pages, Little, Brown. *Cryptolog*, 5(1):13–14, January 1978. ISSN 0740-7602. URL `https://archive.org/download/cryptolog_38/cryptolog_38.pdf`. Reprint of [Fil77].

Fisher:1984:CCS

[Fis84] Warren W. Fisher. Cryptography for computer security: Making the decision. *Computers and Security*, 3(3):229–233, August 1984. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404884900440`.

Fitzgerald:1989:QIP

[Fit89] K. Fitzgerald. The quest for intruder-proof computer systems. *IEEE Spectrum*, 26(8):22–26, August 1989. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Flowers:1983:DC

[Flo83] Thomas H. Flowers. The design of Colossus. *Annals of the History of Computing*, 5(3):239–253, July/September 1983. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1983/pdf/a3239.pdf`; `http://www.computer.org/annals/an1983/a3239abs.htm`. Foreword by Howard Campaigne.

Feiertag:1977:PMS

[FLR77] R. J. Feiertag, K. N. Levitt, and L. Robinson. Proving multilevel security of a system design. *Operating Systems Review*, 11(5):57–65, November 1977. CODEN OSRED8. ISSN 0163-5980.

Friedman:1976:ZTJ

[FM76] William F. (William Frederick) Friedman and Charles Jastrow Mendelsohn. *The Zimmermann telegram of January 16, 1917, and its cryptographic background*. A Cryptographic series. Aegean Park Press, Laguna Hills, CA, USA, 1976. ISBN 0-89412-009-3. 33 pp. LCCN D511 .F683 1976.

Fortune:1985:PP

[FM85] Steven Fortune and Michael Merritt. Poker protocols. In Blakley and Chaum [BC85], pages 454–464. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.`

asp?genre=article&issn=??
??&volume=0&issue=0&spage=
454. 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

[FMC85] R. C. Fairfield, R. L. Mortenson, and K. B. Coulthart. An LSI random number generator (RNG). In Blakley and Chaum [BC85], pages 203–230. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=203. 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:LDE

[FMP85] R. C. Fairfield, A. Matusevich, and J. Plany. An LSI Digital Encryption Processor (DEP). In Blakley and Chaum [BC85], pages 115–143. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=115. 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.

Feistel:1975:SCT

[FNS75] H. Feistel, W. A. Notz, and J. L. Smith. Some cryptographic techniques for machine-to-machine data communications. *Proceedings of the IEEE*, 63(??):1545–1534, 1975. CODEN IEEPAD. ISSN 0018-9219 (print), 1558-2256 (electronic). URL https://ieeexplore.ieee.org/document/1451934.

Flajolet:1989:RMS

[FO89] Philippe Flajolet and Andrew M. Odlyzko. Random mapping statistics. In Jean-Jacques Quisquater and Joos Vandewalle, editors, *EUROCRYPT 1989: Advances in Cryptology — EUROCRYPT '89: Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*, volume 434 of *Lecture Notes in Computer Science*, pages 329–354. Springer-Verlag, Berlin, Germany / Heidelberg,

Germany / London, UK / etc., 1989.

Foster:1982:CM

[Fos82] Caxton C. Foster. *Cryptanalysis for microcomputers*. Hayden Book Co., Rochelle Park, NJ, USA, 1982. ISBN 0-8104-5174-3 (paperback). 333 pp. LCCN Z103.F67 1982. US$14.95.

Franksen:1984:MBS

[Fra84] Ole Immanuel Franksen. *Mr. Babbage's secret: the tale of a cypher and APL*. Strandberg, Birkerod, Denmark, 1984. ISBN 87-87200-86-4. 319 pp. LCCN Z103.B2 F72 1984.

Franklin:1985:MID

[Fra85a] Matthew Keith Franklin. Mathematical investigations of the Data Encryption Standard. Thesis (M.A. in Mathematics), Department of Mathematics, University of California, Berkeley, Berkeley, CA, USA, May 1985. 36 pp.

Franksen:1985:MBS

[Fra85b] Ole Immanuel Franksen. *Mr. Babbage's secret: the tale of a cypher and APL*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 1985. ISBN 0-13-604729-7. 319 pp. LCCN Z103.B2 F721 1985.

Franksen:1986:SHM

[Fra86] O. I. Franksen. The secret hobby of Mr. Babbage. *Systems Anal. Modelling Simulation*, 3 (2):183–194, 1986. ISSN 0232-9298.

Frankel:1989:TIC

[Fra89] Yair Frankel. Two issues in cryptology: algebraic analysis of DES and a shared public key system. Thesis (M.S. in Computer Science), University of Wisconsin-Milwaukee, Milwaukee, WI, USA, 1989. ix + 32 pp.

Friedman:1935:ICA

[Fri35a] William F. (William Frederick) Friedman. *The index of coincidence and its applications in cryptanalysis: technical paper*. United States Government Printing Office, Washington, DC, USA, 1935. 87 + 3 pp.

Friedman:1935:MCP

[Fri35b] William F. (William Frederick) Friedman. *Military cryptanalysis. Part 1, monoalphabetic substitution systems*. Number 30 in Cryptographic series. Aegean Park Press, Laguna Hills, CA, USA, 1935. ISBN 0-89412-044-1. 149 pp. LCCN Z103.5.F77 1992. Four volumes.

Friedman:1935:PIS

[Fri35c] William F. (William Frederick) Friedman. *The principles of indirect symmetry of position in secondary alphabets and their application in the solution of polyalphabetic substitution ciphers: technical paper*. United States Government Printing Office, Washington, DC, USA, 1935. ???? pp.

Friedman:1939:CAC

[Fri39a] 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

[Fri39b] William F. (William Frederick) Friedman. *Military cryptanalysis*. New York Public Library, New York, NY, USA, 1939. 1 microfilm reel.

Friedman:1941:MCP

[Fri41] William F. (William Frederick) Friedman. *Military cryptanalysis. Part IV, Transposition and fractionating systems*. Cryptographic series; 61. Aegean Park Press, Laguna Hills, CA, USA, 1941. ISBN 0-89412-198-7 (paperback), 0-89412-199-5 (library bound). 189 pp. LCCN Z103.5.F77 1992.

Friedman:1942:MC

[Fri42] William F. (William Frederick) Friedman. *Military cryptanalysis*. United States Government Printing Office, Washington, DC, USA, third edition, 1942. various pp.

Friedman:1956:CCC

[Fri56] William F. (William Frederick) Friedman. *Codes and ciphers (cryptology)*. Encyclopaedia Britannica, Chicago, IL, USA, 1956. 8 pp.

Friedman:1963:SLC

[Fri63] William F. (William Frederick) Friedman. *Six lectures on cryptology*. ????, ????, 1963. iii + 182 pp.

Friedman:1976:AMC

[Fri76a] William F. (William Frederick) Friedman. *Advanced military cryptography*. A Cryptographic series. Aegean Park Press, Laguna Hills, CA, USA, 1976. ISBN 0-89412-011-5. 113 pp. LCCN ???? Continuation of Elementary military cryptography, Aegean Park Press, 1976.

Friedman:1976:CEC

[Fri76b] William F. (William Frederick) Friedman. *The classic elements of cryptanalysis: with new added problems for the solver*, volume 3. Aegean Park Press, Laguna Hills, CA, USA, 1976. ISBN 0-89412-002-6. ???? pp.

Friedman:1976:CCA

[Fri76c] William F. (William Frederick) Friedman. *Cryptography and cryptanalysis articles*, volume 5–6 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1976. ?? pp. LCCN Z103 .C79 1976.

Friedman:1976:EC

[Fri76d] William F. (William Frederick) Friedman. *Elements of cryptanalysis*, volume 3 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1976. 172 pp. LCCN ????

Friedman:1976:EMC

[Fri76e] William Frederick Friedman. *Elementary military cryptography*. A Cryptographic series. Aegean Park Press, Laguna Hills, CA, USA, 1976. ISBN 0-89412-010-7. 86 pp. LCCN Z104 .F8740 1976. On cover: Formerly Special text no. 165 (1935).

Friedman:1987:ICA

[Fri87] William F. (William Frederick) Friedman. *The index of coincidence and its applications in cryptanalysis*, volume 49 of *A cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1987. ISBN 0-89412-137-5 (soft cover), 0-89412-138-3 (library bound). 95 pp. LCCN ????

Fiat:1987:HPY

[FS87] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Odlyzko [Odl87b], pages 181–187. CODEN LNCSD9. ISBN 3-540-18047-8, 0-387-18047-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1986. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0263.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=263`. Conference held at the University of California, Santa Barbara, Aug. 11–15, 1986.

Funk:1978:DUS

[Fun78] Mark Robert Funk. A digital ultrasound system for data collection, imaging, and tissue signature analysis. Thesis (M.S.), Department of Electrical Engineering, Michigan State University, East Lansing, MI 48824, USA, 1978. vii + 141 pp.

Futrelle:1973:BTM

[Fut73] Jacques Futrelle. *Best "Thinking Machine" detective stories*. Dover Publications, Inc., New York, NY, USA, 1973. ISBN 0-486-20537-1. ix + 241 pp. LCCN PS3511.U98 B4.

Fernandez:1987:ACA

[FVTS87] C. Fernández, A. Vaquero, J. M. Troya, and J. M. Sánchez. Automating the computation of authenticators for interbank telex messages. *Computers and Security*, 6(5):396–402, October 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404887900125`.

Gabriel:1982:VPI

[Gab82] Richard Gabriel. Verschlüsselungsabbildungen mit Pseudo-Inversen, Zufallsgeneratoren und Täfelungen. (German) [Encryption mapping with pseudoinverses, random generators and tilings]. *Kybernetika (Prague)*, 18(6):485–504, 1982. CODEN KYBNAI. ISSN 0023-5954.

Gaglione:1988:ITP

[Gag88a] A. M. Gaglione. Information theory and public key cryptosystems. *Computers and Security*, 7(5):511, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888902167`.

Gaglione:1988:SCT

[Gag88b] A. M. Gaglione. Some complexity theory for cryptography. *Computers and Security*, 7(5):519, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888902714`.

Gaines:1939:ECS

[Gai39] Helen Fouche Gaines. *Elementary cryptanalysis: a study of ciphers and their solution*. American Photographic Publishing Co., Boston, MA, USA, 1939. vi + 230 + 1 pp. LCCN Z104 .G3. First edition. Galland, p. 72. Inscribed by Gelett Burgess. Bound in gray cloth; stamped in red; top edges stained red. Library of the American Cryptogram Association (George C. Lamb Collection).

Gaines:1940:ECS

[Gai40] Helen Fouche Gaines. *Elementary cryptanalysis; a study of ciphers and their solution*. Chapman and Hall, Ltd., London, UK, 1940. vi + 230 + 23 pp.

Gaines:1943:ECS

[Gai43] Helen Fouche Gaines. *Elementary cryptanalysis: a study of ciphers and their solution*. American Photographic Publishing Co., Boston, MA, USA, 1943. vi + 230 + 1 pp.

Gaines:1944:CSC

[Gai44] Helen Fouche Gaines. *Cryptanalysis: a study of ciphers and their solution*. Dover Publications, Inc., New York, NY, USA, 1944.

Gaines:1956:CSC

[Gai56] Helen Fouché Gaines. *Cryptanalysis: a study of ciphers and their solution*. Dover Publications, Inc., New York, NY, USA, 1956. ISBN 0-486-20097-3. 237 pp. LCCN Z104 .G3 1956. Formerly published under the title: Elementary cryptanalysis.

Gait:1977:VCH

[Gai77] Jason Gait. *Validating the correctness of hardware implementations of the NBS Data Encryption Standard*. U.S. National Bureau of Standards, Gaithersburg, MD, USA, November 1977. iv + 40 pp.

Gait:1978:EEP

[Gai78] Jason Gait. Easy entry: the password encryption problem. *Operating Systems Review*, 12

(3):54–60, July 1978. CODEN OSRED8. ISSN 0163-5980.

Gait:1980:CST

[Gai80a] Jason Gait. Computer science and technology: maintenance testing for the Data Encryption Standard. United States. National Bureau of Standards Special publication 500-61, U.S. National Bureau of Standards, Gaithersburg, MD, USA, 1980. 25 pp.

Gait:1980:MTD

[Gai80b] Jason Gait. *Maintenance testing for the Data Encryption Standard*. U.S. National Bureau of Standards, Gaithersburg, MD, USA, August 1980. iii + 25 pp.

Gait:1980:VCH

[Gai80c] Jason Gait. *Validating the correctness of hardware implementations of the NBS Data Encryption Standard*. United States Government Printing Office, Washington, DC, USA, 1980. iv + 40 pp. US$2.25 (paperback).

Gaj:1989:GCM

[Gaj89] Kris Gaj. *German Cipher Machine Enigma — Methods of Breaking*. Wydawnictwa Komunikacji i Lacznosci, Warszawa, Poland, 1989. ISBN ???? ???? pp. LCCN ????

Galland:1945:HABa

[Gal45a] Joseph Stanislaus Galland. *An historical and analytical bibliography of the literature of cryptology*. Northwestern University studies in the humanities no. 10. Northwestern University, Evanston, IL, USA, 1945. viii + 11 + 209 pp. LCCN Z103.A1 G3. "Works consulted and utilized" in preface.

Galland:1945:HABb

[Gal45b] Joseph Stanislaus Galland. *An historical and analytical bibliography of the literature of cryptology*. Number 10 in Northwestern University humanities series; v. 10. AMS Press, New York, NY, USA, 1945. ISBN 0-404-50710-7. viii + 209 pp. LCCN Z103.A1G3 1970.

Galland:1945:HABc

[Gal45c] Joseph Stanislaus Galland. *An historical and analytical bibliography of the literature of cryptology*, volume 71 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1945. ISBN 0-89412-252-5. 209 pp. LCCN ????

Galland:1970:HAB

[Gal70] Joseph Stanislaus Galland. *An historical and analytical bibliography of the literature of cryptology*. Number 10 in Northwestern University studies in the humanities. AMS Press, New York, NY, USA, 1970. ISBN 0-404-50710-7. viii + 209 pp. LCCN Z103.A1 G3 1970.

Galil:1988:SIC

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

of *SIAM Journal on Computing*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1988. i–viii, 179–426 pp.

Gamble:1988:IDL

[Gam88] Robert Oscar Gamble. Investigation of discrete logarithmic encryption algorithms. Thesis (M.S.), University of South Carolina, Columbia, SC, USA, 1988. ii + 50 pp.

Gardner:1977:MGN

[Gar77] Martin Gardner. Mathematical games: A new kind of cipher that would take millions of years to break. *Scientific American*, 237(2):120–124, August 1977. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL `http://www.nature.com/scientificamerican/journal/v237/n2/pdf/scientificamerican0877-120.pdf`.

Garlinski:1979:IEW

[Gar79] Józef Garliński. *Intercept: the Enigma war*. J. M. Dent, London, UK, 1979. ISBN 0-460-04337-4. xx + 219 + 8 pp. LCCN D810.C88 G37.

Garlinski:1980:EW

[Gar80] Józef Garliński. *The Enigma war*. Scribner, New York, NY, USA, 1980. ISBN 0-684-15866-3. xx + 219 + 8 pp. LCCN D810.S7 G32 1980. US$14.95.

Gilmour-Bryson:1982:CDT

[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.".

Goethals:1980:CAL

[GC80] J.-M. Goethals and C. Couvreur. A cryptanalytic attack on the Lu-Lee public-key cryptosystem. *Philips Journal of Research*, 35(4-5):301–306, 1980. CODEN PHJRD9. ISSN 0165-5817.

Girault:1988:GBA

[GCC88] Marc Girault, Robert Cohen, and Mireille Campana. A generalized birthday attack. In Gunther [Gun88b], pages 129–156. CODEN LNCSD9. ISBN 0-387-50251-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.330; QA76.9.A25 E9641 1988. Sponsored by the International Association for Cryptologic Research.

Geffe:1973:HPD

[Gef73] 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

[Gel74] I. J. Gelb. Records, writing, and decipherment. *Visible Language*, VIII(4):293–318, Autumn 1974. CODEN VSLGAO. ISSN 0022-2224 (print), 2691-5529 (electronic). URL `https://s3-us-west-2.amazonaws.com/visiblelanguage/pdf/V8N4_1974_E.pdf`.

Gersho:1982:ACR

[Ger82] Allen Gersho. *Advances in cryptography: a report on CRYPTO 81*. Santa Barbara, CA, USA, 1982. viii + 156 pp. "Sponsored by the Data and Computer Communications Committees of the IEEE Communications Society with the cooperation of the Dept. of Electrical and Computer Engineering, University of California, Santa Barbara." — Verso of t.p. "August 20, 1982." Includes bibliographies.

Goldreich:1985:CAR

[GGM85] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. On the cryptographic applications of random functions (extended abstract). In Blakley and Chaum [BC85], pages 276–288. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=276`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Goldreich:1986:HCR

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How

to construct random functions. *Journal of the Association for Computing Machinery*, 33(4):792–807, October 1986. CODEN JACOAH. ISSN 0004-5411. URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/6503.html`. A computational complexity measure of the randomness of functions is introduced, and, assuming the existence of one-way functions, a pseudo-random function generator is presented.

Gifford:1981:CSI

[Gif81] David K. Gifford. Cryptographic sealing for information secrecy and authentication. *Operating Systems Review*, 15(5): 123–124, December 1981. CODEN OSRED8. ISSN 0163-5980.

Gingerich:1970:BRB

[Gin70] Owen Gingerich. Book review: *The Codebreakers. The Story of Secret Writing* by David Kahn. *Isis*, 61(3):405–406, Autumn 1970. CODEN ISISA4. ISSN 0021-1753 (print), 1545-6994 (electronic). URL `http://www.jstor.org/stable/229701`.

Girdansky:1971:DPC

[Gir71] M. B. Girdansky. Data privacy — cryptology and the computer at IBM Research,. *IBM Research Reports*, 7(4):12, 1971.

Girdansky:1972:CCD

[Gir72] M. B. Girdansky. Cryptology, the computer and data privacy. *Computers and Automation*, 21 (??):12–19, April 1972.

Girling:1987:CCL

[Gir87] C. G. Girling. Covert channels in LAN's. *IEEE Transactions on Software Engineering*, SE-13(2):292–296, February 1987. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1702208`.

Givierge:1925:CC

[Giv25] Marcel Givierge. *Cours de cryptographie*. Berger-Levrault, Paris, France, 1925. ix + 304 pp. LCCN Z104 .G43.

Givierge:1932:CC

[Giv32] Marcel Givierge. *Cours de cryptographie*. Berger-Levrault, Paris, France, deuxième edition, 1932. ix + 304 pp.

Givierge:1978:CC

[Giv78] Marcel Givierge. *Course in cryptography*, volume 19 of *A cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1978. ISBN 0-89412-028-X. 164 pp. English translation of [Giv32].

Garey:1979:CIG

[GJ79] Michael R. Garey and David S. Johnson. *Computers and Intractability: a Guide to the Theory of NP-Completeness*. W.H. Freeman, San Francisco, CA, USA and New York, NY, USA,

1979. ISBN 0-7167-1045-5, 0-7167-1044-7. x + 338 pp.

Gifford:1982:CSI

[GJ82] D. K. Gifford and A. K. Jones. Cryptographic sealing for information security and authentication. *Communications of the Association for Computing Machinery*, 25(4):274–286, April 1982. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Gligor:1979:OMA

[GL79] V. D. Gligor and B. G. Lindsay. Object migration and authentication. *IEEE Transactions on Software Engineering*, SE-5(6): 607–611, November/December 1979. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1702677`.

Guillou:1982:CT

[GL82] L. C. Guillou and B. Lorig. Cryptography and teleinformatics. *Computers and Security*, 1 (1):27–33, January 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404882900220`.

Goldreich:1989:HCP

[GL89] O. Goldreich and L. A. Levin. A hard-core predicate for all one-way functions. In ACM-TOC'89 [ACM89c], pages 25–32. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989. URL `http://www.acm.org/pubs/articles/proceedings/stoc/73007/p25-goldreich/p25-goldreich.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/73007/p25-goldreich/`.

Gleason:1957:ECP

[Gle57] Andrew M. Gleason. *Elementary course in probability*. National Security Agency, Office of Research and Development, Mathematical Research Division, Washington, DC, USA, second edition, 1957. various pp. LCCN Z104 .G53 1957. Revised by Walter F. Penney and Ronald E. Wyllys.

Gleason:1986:ECP

[Gle86] Andrew M. Gleason. *Elementary course in probability for the cryptanalyst*. Aegean Park Press, Laguna Hills, CA, USA, 1986. ISBN 0-89412-098-0. ???? pp. LCCN ????

Gleason:1987:PIC

[Gle87] Andrew M. Gleason, editor. *Proceedings of the International Congress of Mathematicians, 1986: August 3–11, 1986, Berkeley*. American Mathematical Society, Providence, RI, USA, 1987. ISBN 0-8218-0110-4. LCCN QA1 .I8 1986 v. 1-2. Two volumes.

Goldwasser:1982:PEH

[GM82] Shafi Goldwasser and Silvio Micali. Probabilistic encryption &

how to play mental poker keeping secret all partial information. In ACM [ACM82], pages 365–377. ISBN 0-89791-070-2. LCCN QA75.5 .A14 1982. ACM order no. 508820.

Goldwasser:1984:PE

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984. CODEN JCSSBM. ISSN 0022-0000. See also preliminary version in 14th STOC, 1982.

Goodman:1985:NTK

[GM85] R. M. F. Goodman and A. J. McAuley. A new trapdoor knapsack public key cryptosystem. *Lecture Notes in Computer Science*, 209:150–158, 1985. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Goldwasser:1985:PSS

[GMR85] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A "Paradoxical" solution to the signature problem. In Blakley and Chaum [BC85], page 467. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=467`. 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.

Goldwasser:1988:DSS

[GMR88] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308, April 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Goldwasser:1989:KCI

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1): 186–208, February 1989. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Good:1945:GRT

[GMT45] I. Jack Good, Donald Michie, and Geoffrey Timms. General report on Tunny. GC&CS report HW 25/4, British National Archives, ????, 1945.

Goldreich:1987:HPM

[GMW87] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game — A completeness theorem for protocols with honest majority. In ACM [ACM87], pages 218–229. ISBN 0-89791-221-7. LCCN QA 76.6 A13 1987.

Golomb:1967:SRS

[Gol67] S. Golomb. *Shift Register Sequences*. Holden-Day, San Francisco, CA, USA, 1967. xiv + 224 pp. LCCN QA267.5.S4 G6. Portions co-authored with Lloyd R. Welch, Richard M. Goldstein, and Alfred W. Hales.

Golomb:1982:SRS

[Gol82] S. Golomb. *Shift Register Sequences*. Aegean Park Press, Laguna Hills, CA, USA, revised edition, 1982. ISBN 0-89412-048-4. xvi + 247 pp. LCCN QA267.5.S4 G6 1982. Portions co-authored with Lloyd R. Welch, Richard M. Goldstein, and Alfred W. Hales.

Goldwasser:1984:PET

[Gol84] Shafrira Goldwasser. *Probabilistic encryption: theory and applications*. Thesis (Ph. D. in Computer Science), Department of Computer Science, University of California, Berkeley, Berkeley, CA, USA, December 1984. iv + 63 pp.

Gong:1989:SCB

[Gon89] Li Gong. On security in capability-based systems. *Operating Systems Review*, 23(2): 56–60, April 1989. CODEN OSRED8. ISSN 0163-5980.

Good:1979:EWC

[Goo79] I. J. Good. Early work on computers at Bletchley. *Annals of the History of Computing*, 1(1):38–48, July/September 1979. CODEN AHCOE5. 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

[Gor85] John A. Gordon. Strong primes are easy to find. In Beth et al. [BCI85], pages 216–223. CODEN LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). 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

[GPW85] Andrew M. Gleason, Walter F. Penney, and Ronald E. Wyllys. *Elementary course in probability for the cryptanalyst*, volume 41 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, revised edition, 1985. ISBN 0-89412-072-7. ???? pp. LCCN Z104 .G53 1985.

Gray:1982:ICT

[Gra82] 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

weaken the U.S. lead in innovation. *IEEE Spectrum*, 19 (5):64–68, May 1982. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Grossman:1974:GTR

[Gro74] E. Grossman. Group theoretic remarks on cryptographic systems based on two types of addition. Research Report RC-4742, IBM T. J. Watson Research Center, Yorktown Heights, NY, USA, February 26, 1974.

Grover:1982:CP

[Gro82] Derrick Grover. Cryptography: a primer. *The Computer Journal*, 25(3):400c–400, August 1982. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/25/3/400-c.full.pdf+html`.

Grundler:1984:DEH

[Gru84] Edward James Grundler. A data encryption hardware software package. Project (M.S.), California State University, Sacramento, Sacramento, CA, USA, 1984. vii + 81 pp.

Gaines:1978:SSP

[GS78] R. Stockton Gaines and Norman Z. Shapiro. Some security principles and their application to computer security. *Operating Systems Review*, 12(3): 19–28, July 1978. CODEN OSRED8. ISSN 0163-5980.

Grollmann:1984:CMP

[GS84] J. Grollmann and A. L. Selman. Complexity measures for public-key cryptosystems. In IEEE [IEE84], pages 495–503. CODEN ASFPDV. ISBN 0-8186-8591-3, 0-8186-0591-X (paperback), 0-8186-4591-1 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1984. IEEE catalog no. 84CH2085-9.

Grollmann:1988:CMP

[GS88] Joachim Grollmann and Alan L. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17(2):309–335, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Guarini:1904:MTT

[Gua04] Emile Guarini. The Malcotti telecryptograph for telegraphing upon telephone lines. *Scientific American*, 91(12):193–194, September 17, 1904. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL `http://www.nature.com/scientificamerican/journal/v91/n12/pdf/scientificamerican09171904193a.pdf`.

Guan:1987:CAP

[Gua87] Puhua Guan. Cellular automaton public-key cryptosystem. *Complex Systems*, 1(1):51–56, 1987. ISSN 0891-2513.

Gudes:1980:DCB

[Gud80] E. Gudes. The design of a cryptography based secure file system. *IEEE Transactions on Software Engineering*, SE-6(5): 411–420, September/October 1980. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1702757`.

Guillen:1976:AC

[Gui76] M. Guillen. Automated cryptography. *Science News (Washington, DC)*, 110(12):188–190, September 18, 1976. CODEN SCNEBK. ISSN 0036-8423 (print), 1943-0930 (electronic).

Gullichsen:1983:BHS

[Gul83] Eric Alexander Gullichsen. Bidirectional heuristic search and spectral S-box simplification for the cryptanalysis of the NBS Data Encryption Standard. Thesis (M.Sc.), University of British Columbia, Ottawa, ON, Canada, 1983. 3 microfiches (265 fr.).

Gunther:1988:ASG

[Gun88a] C. Gunther. Alternating step generators controlled by de Bruijn sequences. In Chaum and Price [CP88], pages 5–14. CODEN LNCSD9. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E9631 1987; QA267.A1 L43 no.304. Sponsored by the International Association for Crytologic Research.

Gunther:1988:ACE

[Gun88b] Christoph G. Gunther, editor. *Advances in cryptology — EUROCRYPT '88: Workshop on the Theory and Application of Cryptographic Techniques, Davos, Switzerland, May 25–27, 1988: proceedings*, volume 330 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988. CODEN LNCSD9. ISBN 0-387-50251-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.330; QA76.9.A25 E9641 1988. Sponsored by the International Association for Cryptologic Research.

Guy:1976:HFN

[Guy76] R. K. Guy. How to factor a number. In Hartnell and Williams [HW76], pages 49–89.

Griffiths:1976:AMR

[GW76] Patricia P. Griffiths and Bradford W. Wade. An authorization mechanism for a relational database system. *ACM Transactions on Database Systems*, 1(3):242–255, September 1976. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1976-1-3/p242-griffiths/p242-griffiths`.

pdf; http://www.acm.org/pubs/citations/journals/tods/1976-1-3/p242-griffiths/.

Gamow:1958:CAP

[GY58] George Gamow and Martynas Yças. 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

[GY87] Zvi Galil and Moti Yung. Partitioned encryption and achieving simultaneity by partitioning. *Information Processing Letters*, 26(2):81–88, October 19, 1987. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Gylden:1931:CEI

[Gyl31] Yves Gyldén. Chifferbyråernas insatser i världskriget till lands. (Swedish) [Cipher bureaus' operations in the World War on land]. Stockholm, Sweden, 1931.

Gylden:1933:CCB

[Gyl34] Yves Gyldén. The contribution of the cryptographic bureaus in the World War. *The Signal Corps Bulletin*, (75–81): ??, November–December 1933–1934. URL https://archive.org/download/cryptolog_96/cryptolog_96.pdf.

Gylden:1936:AMC

[Gyl36] Yves Gylden. *Analysis of model C-36 cryptograph from the viewpoint of cryptanalysis*. A. B. Teknik co., Stockholm, Sweden, 1936. 22 pp.

Gylden:1938:APV

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

Haddon:1984:BRS

[Had84] Bruce K. Haddon. Book review of "Security, IFIP/Sec'83: proceedings of the first security conference" North-Holland Publishing Co. 1983. *Operating Systems Review*, 18(3):14, July 1984. CODEN OSRED8. ISSN 0163-5980. See [Fêa83].

Hammer:1971:SSC

[Ham71] Carl Hammer. Signature simulation and certain cryptographic codes. *Communications of the Association for Computing Machinery*, 14(1):3–14, January 1971. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Hamming:1980:CIT

[Ham80] R. W. (Richard Wesley) Hamming. *Coding and information theory*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458,

USA, 1980. ISBN 0-13-139139-9. xii + 239 pp. LCCN QA268 .H35 1980. US$19.95.

Hamming:1986:CIT

[Ham86] R. W. (Richard Wesley) Hamming. *Coding and information theory*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, second edition, 1986. ISBN 0-13-139072-4. xii + 259 pp. LCCN QA268 .H35 1986. US$36.95.

Haskett:1984:PAU

[Has84] James A. Haskett. Pass-algorithms: a user validation scheme based on knowledge of secret algorithms. *Communications of the Association for Computing Machinery*, 27 (8):777–781, 1984. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Haastad:1987:OWP

[Hås87] Johan Håstad. One-way permutations in NC^0. *Information Processing Letters*, 26(3): 153–155, November 23, 1987. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Haastad:1988:SSM

[Hås88] Johan Håstad. Solving simultaneous modular equations of low degree. *SIAM Journal on Computing*, 17(2):336–341, April 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Haugen:1974:RSS

[Hau74] Einar Haugen. The rune stones of Spirit Pond, Maine. *Visible Language*, VIII(1):33–64, Winter 1974. CODEN VSLGAO. ISSN 0022-2224 (print), 2691-5529 (electronic). URL `https://s3-us-west-2.amazonaws.com/visiblelanguage/pdf/V8N1_1974_E.pdf`.

Huang:1988:SWP

[HC88] Yue Jiang Huang and Fred Cohen. Some weak points of one fast cryptographic checksum algorithm and its improvement. *Computers and Security*, 7(5): 503–505, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888902040`.

Heidel:1676:JTP

[Hei76] Wolfgango Ernesto Heidel. *Johannis Trithemii primo Spanheimensis deinde Divi Jacobi Peapolitani abbatis Steganographia: quae hucusq[ue] 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 concin-*

natae: deinde solvuntur & exhibentur artificia nova steganographica a Trithemio in literis ad Arnoldum Bostium & Polygraphia promissa, in hunc diem a nemine capta, sed pro paradoxis & impossibilibus habita & summe desiderata. Wormatiense, Moguntiae. Sumptibus Joannis Petri Zubrodt, 1676. 8 + 394 (or 396) + 4 pp. LCCN Z103 .T84 1676. Includes Heidel's life of Trithemius and his vindication of the Steganographia.

Hellman:1976:SPN

[Hel76] M. E. Hellman. Statement to participants at NBS workshop on cryptography in support of computer security. Unpublished memorandum, ????, ????, September 21, 1976.

Hellman:1979:WTI

[Hel79a] M. E. Hellman. I. 'DES will be totally insecure within ten years'. *IEEE Spectrum*, 16 (7):32–40, July 1979. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Hellman:1979:MPK

[Hel79b] Martin E. Hellman. The mathematics of public-key cryptography. *Scientific American*, 241 (2):146–157 (Intl. ed. 130–139), August 1979. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Hellman:1981:ACA

[Hel81] M. E. Hellman. Another cryptanalytic attack on "A cryptosystem for multiple communication" [Inform. Process. Lett. **10**(4–5), 5 July 1980, pp. 180–183]. *Information Processing Letters*, 12(4):182–183, August 13, 1981. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [LM80, Mei81].

Henry:1981:BJB

[Hen81] P. S. Henry. B.S.T.J. briefs: Fast decryption algorithm for the knapsack cryptographic system. *The Bell System Technical Journal*, 60(5):767–773, May–June 1981. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol60/bstj60-5-767.pdf`.

Henry:1982:FDA

[Hen82] Paul S. Henry. Fast decryption algorithm for the knapsack cipher. *Computers and Security*, 1(1):80–83, January 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404882900293`.

Herlestam:1978:CRS

[Her78] Tore Herlestam. Critical remarks on some public-key cryptosystems. *BIT*, 18(4):493–496, December 1978. CODEN NBITAB. ISSN 0006-

3835 (print), 1572-9125 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=18&issue=4&spage=493`.

Hershey:1981:DLP

[Her81] J. E. (John E.) Hershey. The discrete logarithm public cryptographic system. NTIA report 81-81, PB82-130097, U.S. Dept. of Commerce, National Telecommunications and Information Administration, Washington, DC, USA (??), September 1981. iv + 40 pp.

Hersch:1989:DSA

[Her89] Jeffrey Stuart Hersch. Digital signature analysis of radar reflections for the assessment of concrete bridge deck deterioration. Thesis (M.S.), Massachusetts Institute of Technology, Department of Civil Engineering, Cambridge, MA, USA, 1989. 165 pp. Supervised by Kenneth R. Maser and Alexander Slocum.

Hardy:1985:ECC

[HFL+85] John M. Hardy, Dorothy W. Fuller, Douglas R. Long, Jane C. Hartin, and Faye Davis. *Electronic cryptographic communications equipment specialist (AFSC 30650)*. Extension Course Institute, Air University, ????, 1985. various pp.

Hoornaert:1985:EHI

[HGD85] Frank Hoornaert, Jo Goubert, and Yvo Desmedt. Efficient hardware implementation of the DES. In Blakley and Chaum [BC85], pages 147–173. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=147`. 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.

Hinsley:1979:BISb

[HH79] F. H. (Francis Harry) Hinsley and Michael Eliot Howard. *British intelligence in the Second World War: its influence on strategy and operations*. Cambridge University Press, New York, NY, USA, 1979. ISBN 0-521-22940-5 (vol. 1). various pp. LCCN D810.S7 H47 1979b. Vols. 3-4 in series: History of the Second World War. Vol. 4 has subtitle: Security and counter-intelligence; Vol. 5 has subtitle: Strategic deception.

Harn:1989:PAU

[HHL89] L. Harn, D. Huang, and C. S. Laih. Password authentication using public-key cryptography. *Computers and Math-*

ematics with Applications, 18 (12):1001–1017, ???? 1989. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/089812218990028X`.

Higenbottam:1973:CC

[Hig73] Frank Higenbottam. *Codes and ciphers*. English Universities Press, London, UK, 1973. ISBN 0-340-12493-8. 180 (est.) pp. LCCN ????

Highland:1983:BRCb

[Hig83] Harold Joseph Highland. Book review: *Codes, ciphers and computers: an introduction to information security*: Bruce Bosworth: Rochelle Park NJ: Hayden Book Company, Inc., 1982. viii + 259 pp., $13.95. *Computers and Security*, 2(1): 83–84, January 1983. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/016740488390041X`.

Highland:1987:CC

[Hig87a] Harold Joseph Highland. Cipher cracking. *Computers and Security*, 6(3):205, June 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404887901015`.

Highland:1987:DES

[Hig87b] Harold Joseph Highland. Data encryption standard II? *Computers and Security*, 6(3): 195–196, June 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404887900952`.

Highland:1987:EP

[Hig87c] Harold Joseph Highland. Encryption package. *Computers and Security*, 6(3): 199–202, June 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404887900988`.

Highland:1987:HSY

[Hig87d] Harold Joseph Highland. How secure are your encryption keys? *Computers and Security*, 6(2): 99–100, April 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404887900757`.

Highland:1987:HEM

[Hig87e] Harold Joseph Highland. How to evaluate microcomputer encryption software and hardware. *Computers and Security*, 6(3):229–244, June 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404887901040`.

Highland:1988:PEM

[Hig88a] Esther H. Highland. Picking encryption method is no time for secrets: Harold Joseph Highland, Government Computer News, April 29, 1988, p. 39. *Computers and Security*, 7(4):431, August 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888906360`.

Highland:1988:RRC

[Hig88b] Esther H. Highland. A redundancy reducing cipher: Peter Wayner, Cryptologia, April 1988, pp. 107–112. *Computers and Security*, 7(4):431–432, August 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888906414`.

Highland:1988:TSC

[Hig88c] Esther H. Highland. Top secret — concepts and implementation. *Computers and Security*, 7(3):329, June 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888901034`.

Highland:1988:TSV

[Hig88d] Esther H. Highland. Top secret, and vulnerable: John Markoff, The New York Times, April 25, 1988, pp. D1, D4. *Computers and Security*, 7 (4):430, August 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888906311`.

Highland:1988:EAE

[Hig88e] Harold Joseph Highland. Encryption, attacks and ethics. *Computers and Security*, 7(1): 5–6, February 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888904890`.

Highland:1988:SIT

[Hig88f] Harold Joseph Highland. Secretdisk II — transparent automatic encryption. *Computers and Security*, 7(1):27–34, February 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888904981`.

Highland:1989:SDI

[Hig89] Harold Joseph Highland. Secret disk II — administrator. *Computers and Security*, 8(7): 563–568, November 1989. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404889900485`.

Hill:1929:CAA

[Hil29] Lester S. Hill. Cryptography in an algebraic alphabet. *American Mathematical Monthly*, 36(6):306–312, June/July 1929. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Hill:1931:CCL

[Hil31] Lester S. Hill. Concerning certain linear transformation apparatus of cryptography. *American Mathematical Monthly*, 38 (3):135–154, March 1931. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Hitt:1943:MSM

[Hit43] Parker Hitt. *Manual for the solution of military ciphers ... For use in Donald D. Millikin's cryptography and cryptanalysis classes*. New York University Bookstore, New York, NY, USA, 1943. viii + 101 + 22 pp.

HJH:1985:BRK

[HJH85] HJH. Book review: *Kahn on codes: Secrets of the new cryptology*. David Kahn New York: Macmillan Publishing Company, 1984. 344 + viii pages, $19.95. *Computers and Security*, 4(3):247, September 1985. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404885900379`.

He:1988:SDK

[HL88] Jing Min He and Kai Cheng Lu. The security and design of knapsack public key cryptosystems. *J. Tsinghua Univ.*, 28(1):89–97, 1988. CODEN QDXKE8. ISSN 1000-0054.

Hunter:1983:ERA

[HM83] D. G. N. Hunter and A. R. McKenzie. Experiments with relaxation algorithms for breaking simple substitution ciphers. *The Computer Journal*, 26(1): 68–71, February 1983. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Hule:1988:RCW

[HM88] Harald Hule and Winfried B. Müller. On the RSA-cryptosystem with wrong keys. In *Contributions to general algebra, 6*, pages 103–109. Hölder-Pichler-Tempsky, Vienna, 1988.

Hodges:1983:ATE

[Hod83] Andrew Hodges. *Alan Turing: the enigma*. Simon and Schuster, 1230 Ave. of the Americas, New York, NY 10020, USA, 1983. ISBN 0-671-49207-1, 0-09-152130-0 (Burnett Books). 587 pp. LCCN QA29.T8 H63 1983.

Hoffer:1955:MAC

[Hof55] Carol M. Hoffer. On the mathematical approach to cryptanalysis. Thesis, University of South Dakota, Vermillion, SD, USA, 1955. 65 pp.

Hogan:1988:PIS

[Hog88] Carole B. Hogan. Protection imperfect: the security of some computing environments. *Operating Systems Review*, 22(3): 7–27, July 1988. CODEN OSRED8. ISSN 0163-5980. See note [Wel88a].

Hollis:1987:TCA

[Hol87] J. B. Hollis. A technique for communicating AVL traffic by subliminal data signalling over a speech radio channel. In Muraszko [Mur87], pages 13/1–13/5. LCCN TE228 .C66 1987. Digest no.: 1987/21.

Honore:1919:STS

[Hon19] F. Honore. The secret telephone, are sound waves ever visible? *Scientific American*, 121(23):555, December 6, 1919. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL `http://www.nature.com/scientificamerican/journal/v121/n23/pdf/scientificamerican12061919-555.pdf`.

Hood:1980:EFS

[Hoo80] William Chester Hood. Encryption as a file security measure in large operating systems. Thesis (M.S.), University of Tennessee, Knoxville, Knoxville, TN, USA, 1980. iv + 116 pp.

Hoogendoorn:1982:SPK

[Hoo82] P. J. Hoogendoorn. On a secure public-key cryptosystem. In *Computational methods in number theory, Part I*, volume 154 of *Math. Centre Tracts*, pages 159–168. Math. Centrum, Amsterdam, 1982.

Horgan:1985:TIT

[Hor85] J. Horgan. Thwarting the information thieves: Fear of spying through simple or sophisticated electronics has spawned an industry whose challenge is to block the illegal interception of intelligence. *IEEE Spectrum*, 22(7):30–41, July 1985. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Herzberg:1987:PPS

[HP87] Amir Herzberg and Shlomit S. Pinter. Public protection of software. *ACM Transactions on Computer Systems*, 5(4): 371–393, November 1987. CODEN ACSYEC. ISSN 0734-2071. URL `http://www.acm.org:80/pubs/citations/journals/tocs/1987-5-4/p371-herzberg/`.

Holland:1982:GSA

[HR82] Edward R. Holland and James L. Robertson. GUEST — a signature analysis based test system for ECL logic. *Hewlett-Packard Journal: technical information from the laboratories of Hewlett-Packard Company*, 33(3): 26–29, March 1982. CODEN HPJOAX. ISSN 0018-1153.

Harrison:1976:POS

[HRU76] Michael A. Harrison, Walter L. Ruzzo, and Jeffrey D. Ullman. Protection in operating

systems. *Communications of the Association for Computing Machinery*, 19(8):461–471, August 1976. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Haastad:1985:CST

[HS85] J. Håstad and A. Shamir. The cryptographic security of truncated linearly related variables. In ACM [ACM85], pages 356–362. ISBN 0-89791-151-2 (paperback). LCCN QA 76.6 A13 1985. URL `http://www.acm.org/pubs/articles/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:EUH

[HS87] Joseph Hammer and Dinesh G. Sarvate. Encryption using Hungarian rings. *Discrete Applied Mathematics*, 16(2):151–155, 1987. CODEN DAMADU. ISSN 0166-218X.

Hardjono:1989:TCB

[HS89] Thomas Hardjono and Jennifer Seberry. *Towards the cryptanalysis of Bahasa Indonesia and Malaysia*, volume 2 of *CCSR Tutorial Series in Computer Security*. Centre for Commuter Security Research, Canberra, Australia, 1989. ISBN 0-7317-0091-0. vi + 148 pp. LCCN ????

Hinsley:1979:BISa

[HT79] F. H. (Francis Harry) Hinsley and E. E. Thomas. *British intelligence in the Second World War: its influence on strategy and operations*. London, UK, 1979. various pp. UK£10.00 (vol. 1). Vol. 3, pt. 2 has additional author C. A. G. Simkins.

Huang:1988:APE

[Hua88] Min Qiang Huang. An attack to Pless' encryption scheme. *Kexue Tongbao (English Ed.)*, 33(11):885–889, 1988. ISSN 0250-7862.

Hulme:1898:CHP

[Hul98] F. Edward (Frederick Edward) Hulme. *Cryptography; or, The history, principles, and practice of cipher-writing*. Ward, Lock and Co., Limited, ????, 1898. 192 pp. LCCN Z 104 H91. First edition. Galland, p. 94. Bound in yellow cloth; stamped in black. Library of the American Cryptogram Association (George C. Lamb Collection).

Hunter:1985:ARK

[Hun85] D. G. N. Hunter. Algorithm 121: RSA key calculation in Ada. *The Computer Journal*, 28(3):343–348, July 1985. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/28/3/343.full.pdf+html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_`

28/Issue_03/tiff/343.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_28/Issue_03/tiff/344.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_28/Issue_03/tiff/345.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_28/Issue_03/tiff/346.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_28/Issue_03/tiff/347.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_28/Issue_03/tiff/348.tif. See note [Wic87].

Hardy:1975:ITN

[HW75] Godfrey H. Hardy and Edward M. Wright. *An Introduction to the Theory of Numbers*. Clarendon Press, Oxford, UK, fourth edition, 1975. ISBN 0-19-853310-7 (invalid checksum??). 421 pp. LCCN ????

Hartnell:1976:PFM

[HW76] B. L. Hartnell and H. C. Williams, editors. *Proceedings of the Fifth Manitoba Conference on Numerical Mathematics, October 1–4, 1975*, volume 16 of *Congressus Numerantium*. Utilitas Mathematica Publishers, Winnipeg, MN, Canada, 1976.

Hardy:1979:ITN

[HW79] G. H. (Godfrey Harold) Hardy and Edward Maitland Wright. *An introduction to the theory of numbers*. Clarendon Press, Oxford, UK, fifth edition, 1979. ISBN 0-19-853170-2, 0-19-853171-0 (paperback). xvi + 426 pp. LCCN QA241 .H28 1979.

Huthnance:1988:UPP

[HW88] E. Dennis Huthnance and Joe Warndof. On using primes for public key encryption systems. *Applied Mathematics Letters*, 1 (3):225–227, 1988. CODEN AMLEEL. ISSN 0893-9659.

IEEE:1974:ASS

[IEE74] 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

[IEE79] IEEE, editor. *20th Annual Symposium on Foundations of Computer Science: Oct. 29–31, 1979, San Juan, Puerto Rico*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1979. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA267 .S95 1979; TK7885.A1 S92 1979.

IEEE:1980:PSS

[IEE80] IEEE, editor. *Proceedings of the 1980 Symposium on Security and Privacy, April 14–16, 1980 Oakland, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver

Spring, MD 20910, USA, 1980. LCCN QA76.9.A25S95 1980.

IEEE:1981:CLC

[IEE81] IEEE, editor. *6th Conference on Local Computer Networks, Hilton Inn, Minneapolis, Minnesota, October 12–14, 1981*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1981. CODEN CLCPDN. LCCN TK 5105.5 C66 1981. IEEE catalog no. 81CH1690-7.

IEEE:1982:ASF

[IEE82a] IEEE, editor. *23rd annual Symposium on Foundations of Computer Science, November 3–5, 1982, Chicago, Illinois*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1982. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA76.6 .S95 1982. IEEE catalog no. 82CH1806-9. IEEE Computer Society order no. 440.

IEEE:1982:CFP

[IEE82b] IEEE, editor. *COMPCON Fall '82: Proceedings of the 25th International Conference of the Institute of Electrical and Electronics Engineers Computer Society, Capitol Hilton Hotel, Washington, DC, 1982*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1982. ISBN ???? LCCN QA76.5 I578 1982. IEEE catalog no. 82CH1796-2.

IEEE:1983:PSS

[IEE83] IEEE, editor. *Proceedings of the 1983 Symposium on Security and Privacy, April 25–27, 1983, Oakland, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1983. ISBN 0-8186-0467-0 (paperback), 0-8186-4467-2 (microfiche), 0-8186-8467-4 (hardcover). LCCN QA76.9.A25 S95 1983.

IEEE:1984:ASF

[IEE84] IEEE, editor. *25th annual Symposium on Foundations of Computer Science, October 24–26, 1984, Singer Island, Florida*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1984. CODEN ASFPDV. ISBN 0-8186-8591-3, 0-8186-0591-X (paperback), 0-8186-4591-1 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1984. IEEE catalog no. 84CH2085-9.

IEEE:1985:FOC

[IEE85] IEEE, editor. *26th annual Symposium on Foundations of Computer Science, October 21–23, 1985, Portland, OR*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1985. ISBN 0-8186-0644-4 (paperback), 0-8186-4644-6 (microfiche), 0-8186-8644-8 (hardcover). LCCN QA 76 S979 1985.

IEE:1986:CEC

[IEE86a] IEE. *Colloquium on "Encryption for Cable and DBS": Wednesday, 19 February 1986*, volume 1986/24. Institution of Electrical Engineers, London, UK, 1986. various pp.

IEEE:1986:ASF

[IEE86b] IEEE, editor. *27th annual Symposium on Foundations of Computer Science, October 27–29, 1986, Toronto, ON, Canada*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1986. ISBN 0-8186-0740-8 (paperback), 0-8186-4740-X (microfiche), 0-8186-8740-1 (casebound). LCCN QA 76 S979 1986; TK7885.A1 S92 1986.

IEEE:1987:ASF

[IEE87a] IEEE, editor. *28th annual Symposium on Foundations of Computer Science, October 12–14, 1987, Los Angeles, CA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1987. ISBN 0-8186-0807-2, 0-8186-4807-4 (fiche), 0-8186-8807-6 (case). LCCN QA 76 S979 1987.

IEEE:1987:IIG

[IEE87b] IEEE, editor. *IEEE/IEICE Global Telecommunications Conference: conference record, Nov. 15–18, 1987, Tokyo, Japan [GLOBECOM Tokyo '87]*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1987. Three volumes. IEEE catalog no. 87CH2520-5.

IEEE:1987:PIS

[IEE87c] IEEE, editor. *Proceedings / 1987 IEEE Symposium on Security and Privacy, April 27–29, 1987, Oakland, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1987. ISBN 0-8186-8771-1 (hardback), 0-8186-0771-8 (paperback), 0-8186-4771-X (microfiche). LCCN QA 76.9 A25 I43 1987. IEEE catalog number 87CH2416-6. Computer Society Order Number 771.

IEEE:1988:FAC

[IEE88] IEEE, editor. *Fourth Aerospace Computer Security Applications Conference, Orlando, FL, USA, December 12–16, 1988*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. ISBN 0-8186-0895-1. LCCN TL787 .A471 1988; QA76.9.A25 A39 1988. IEEE catalog number 88CH2629-5. IEEE Computer Society order number 895.

IEEE:1989:ASF

[IEE89] IEEE, editor. *30th annual Symposium on Foundations of Computer Science, October 30–November 1, 1989, Research Triangle Park, NC*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1989. CODEN

ASFPDV. ISBN 0-8186-1982-1 (casebound), 0-8186-5982-3 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1989. IEEE catalog number 89CH2808-4.

Israel:1983:AOS

[IL83] J. E. Israel and T. A. Linden. Authentication in office system internetworks. *ACM Transactions on Office Information Systems*, 1(3):193–210, July 1983. CODEN ATOSDO. ISSN 0734-2047. URL `http://www.acm.org:80`.

Impagliazzo:1989:OWF

[IL89] R. Impagliazzo and M. Luby. One-way functions are essential for complexity based cryptography. In IEEE [IEE89], pages 230–235. CODEN ASFPDV. ISBN 0-8186-1982-1 (casebound), 0-8186-5982-3 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1989. IEEE catalog number 89CH2808-4.

Imai:1986:AMC

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

Impagliazzo:1989:ECS

[IN89] Russell Impagliazzo and Moni Naor. Efficient cryptographic schemes provably as secure as subset sum. In IEEE [IEE89], pages 236–241. CODEN ASFPDV. ISBN 0-8186-1982-1. ISSN 0272-5428. LCCN QA 76 S979 1989. IEEE catalog number 89CH2808-4.

IRD:1979:DVE

[Int79] International Resource Development, Inc. *Data and voice encryption*. International Resource Development, New Canaan, CT, USA, 1979. iv + 124 pp.

IDC:1981:DE

[Int81a] International Data Corporation. Data encryption. Research memorandum IDC #ISPS-M81-10., International Data Corporation, Framingham, MA, USA, October 1981. 30 pp.

IRD:1981:DTV

[Int81b] International Resource Development, Inc. Data, text, and voice encryption equipment. Report 183, IRD, 30 High St., Norwalk, CT 06851, USA, 1981. vi + 154 pp.

IRD:1984:DTV

[Int84] International Resource Development, Inc. Data, text, and voice encryption equipment. Report 630, International Resource Development, 6 Prowitt St., Norwalk, CT 06855, USA, 1984. vi + 184 pp.

IRD:1987:DTV

[Int87] International Resource Development, Inc. Data, text and voice encryption worldwide markets.

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

IRD:1988:DTV

[Int88] International Resource Development, Inc. Data, text and voice encryption worldwide markets. Report 754, International Resource Development, New Canaan, Conn., U.S.A. (21 Locust Ave., New Canaan 06840), 1988. viii + 285 pp.

Impagliazzo:1989:LPC

[IR89] R. Impagliazzo and S. Rudich. Limits on the provable consequences of one-way permutations. In ACM-TOC'89 [ACM89c], pages 44–61. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989.

Ito:1987:SSS

[ISN87] 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.

Ingemarsson:1981:UAS

[IW81] Ingemar Ingemarsson and C. K. Wong. Use authentication scheme for shared data based on a trap-door one-way function. *Information Processing Letters*, 12(2):63–67, April 1981. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Jackson:1987:NTS

[Jac87] T. H. Jackson. *From number theory to secret codes*. Hilger, Bristol, UK, 1987. ISBN 0-85274-077-8 (paperback), 0-85274-078-6. vi + 86 pp. LCCN Z104 .J3 1987.

Jeffery:1986:GCC

[Jef86] Keith Jeffery. The Government Code and Cypher School; A memorandum by Lord Curzon. *Intelligence and National Security*, 1(3):454–??, 1986. ISSN 0268-4527 (print), 1743-9019 (electronic).

Jevons:1874:PS

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

Jones:1975:ESP

[JL75] Anita K. Jones and Richard J. Lipton. The enforcement of security policies for computation. *Operating Systems Review*, 9(5): 197–206, November 1975. CODEN OSRED8. ISSN 0163-5980.

Jurgensen:1984:SRI

[JM84] H. Jürgensen and D. E. Matthews. Some results on the information theoretic analysis of cryptosystems. In *Advances in cryptology (Santa Barbara, Calif., 1983)*, pages 303–356. Plenum, New York, 1984.

Johnson:1989:BDC

[Joh89] Michael Paul Johnson. Beyond DES: data compression

and the MPJ encryption algorithm. Thesis (M.S.), University of Colorado at Colorado Springs, Colorado Springs, CO, USA, 1989. viii + 127 pp.

Jones:1978:WWB

[Jon78a] R. V. (Reginald Victor) Jones. *The Wizard War: British Scientific Intelligence, 1939–1945*. Coward, McCann and Geoghegan, New York, NY, USA, 1978. ISBN 0-698-10896-5. xx + 556 + 16 pp. LCCN D810.C88 J66 1978. URL `https://en.wikipedia.org/wiki/Reginald_Victor_Jones`.

Jones:1978:MSW

[Jon78b] Reginald V. Jones. *Most secret war: [British scientific intelligence, 1939–1945]*. Hamilton, London, UK, 1978. ISBN 0-241-89746-7. xx + 556 + 16 pp. LCCN ????

Jones:1986:DEB

[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

[Jos85] H. (Henri) Jossé. *La cryptographie et ses applications à l'art militaire*. Libraire militaire de L. Baudoin, Paris, France, 1885. 103 pp. LCCN Z104 .J67 1885.

JCryptology:1988:JCJ

[Jou88] *Journal of cryptology: the journal of the International Association for Cryptologic Research*, page various, 1988. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/index.htm`. Springer International, New York, NY, USA. Appears three times a year.

Juenemann:1981:DES

[Jue81] Robert R. Juenemann. The Data Encryption Standard vs. exhaustive search. Report, Satellite Business Systems, McLean, VA, USA, February 5, 1981.

Jung:1987:IRC

[Jun87] Achim Jung. Implementing the RSA cryptosystem. *Computers and Security*, 6(4):342–350, August 1987. CODEN CPSEDU. ISSN 0167-4048.

Jung:1988:IRC

[Jun88] A. Jung. Implementing the RSA cryptosystem. *Computers and Security*, 7(5):510–511, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888902131`.

Jurgen:1986:SEI

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

86–87, January 1986. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Kahn:1963:PNU

[Kah63] David Kahn. *Plaintext in the new unabridged: an examination of the definitions on cryptology in Webster's Third New International Dictionary*. Crypto Press, New York, NY, USA, 1963. 35 pp.

Kahn:1966:MC

[Kah66] David Kahn. Modern cryptology. *Scientific American*, 215(1):38–46, July 1966. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL `http://www.nature.com/scientificamerican/journal/v215/n1/pdf/scientificamerican0766-38.pdf`.

Kahn:1967:CSSa

[Kah67a] David Kahn. *The codebreakers: the story of secret writing*. MacMillan Publishing Company, New York, NY, USA, 1967. xvi + 1164 pp. LCCN Z103 .K28. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1000.html`.

Kahn:1967:CSSb

[Kah67b] David Kahn. *The codebreakers: the story of secret writing*. Weidenfeld and Nicolson, London, UK, 1967. xvi + 1164 pp. LCCN Z103 .K28 1967.

Kahn:1974:C

[Kah74] David Kahn. *The Codebreakers*. Weidenfeld and Nicolson, London, UK, abridged edition, 1974. ISBN 0-02-560460-0, 0-297-76785-2. xvi + 576 pp. LCCN Z103 .K28 1974.

Kahn:1976:TC

[Kah76] David Kahn. Tapping computers. *New York Times*, ??(??): ??, April 3, 1976. CODEN NYTIAO. ISSN 0362-4331 (print), 1542-667X, 1553-8095.

Kahn:1979:CGP

[Kah79] David Kahn. Cryptology goes public. *Foreign affairs (Council on Foreign Relations)*, 58(1): 141–159, Fall 1979.

Kahn:1982:GLC

[Kah82] David Kahn. The grand lines of cryptology's development. *Computers and Security*, 1(3): 245–248, November 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404882900426`.

Kahn:1983:KCS

[Kah83] David Kahn. *Kahn on codes: secrets of the new cryptology*. MacMillan Publishing Company, New York, NY, USA, 1983. ISBN 0-02-560640-9. viii + 343 pp. LCCN Z103 .K29 1983.

Kahn:1984:COS

[Kah84] D. Kahn. Cryptology and the origins of spread spectrum. *IEEE Spectrum*, 21 (9):70–80, September 1984. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1009.html`.

Kahn:1996:CSS

[Kah96] David Kahn. *The codebreakers: the story of secret writing*. Scribner, New York, NY, USA, revised edition, 1996. ISBN 0-684-83130-9. xviii + 1181 pp. LCCN Z103 .K28 1996. See [Tuc66].

Kak:1983:EMP

[Kak83] Subhash C. Kak. Exponentiation modulo a polynomial for data security. *International Journal of Computer and Information Sciences*, 12(5):337–346, October 1983. CODEN IJCIAH. ISSN 0091-7036.

Kak:1984:MPK

[Kak84] S. C. Kak. On the method of puzzles for key distribution. *International Journal of Computer and Information Sciences*, 13(2):103–109, April 1984. CODEN IJCIAH. ISSN 0091-7036.

Kak:1985:EEC

[Kak85] Subhash C. Kak. Encryption and error-correction coding using D sequences. *IEEE Transactions on Computers*, 34(9): 803–809, 1985. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Kaliski:1984:AWA

[Kal84] Burton Stephen Kaliski, Jr. Analysis of Wyner's analog encryption scheme. Thesis (B.S.), Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA, 1984. 97 pp. Supervised by Ronald L. Rivest.

Kaliski:1985:WAE

[Kal85] Burt S. Kaliski. Wyner's analog encryption scheme: Results of a simulation. In Blakley and Chaum [BC85], pages 83–94. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=83`. 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.

Karger:1985:ADA

[Kar85] Paul A. Karger. Authentication and discretionary access control in computer networks. *Computer Networks and ISDN Systems*, 10(1):27–37, August 1985.

CODEN CNISE9. ISSN 0169-7552 (print), 1879-2324 (electronic).

Karger:1986:ADA

[Kar86] Paul A. Karger. Authentication and discretionary access control in computer networks. *Computers and Security*, 5(4): 314–324, December 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404886900520`.

Karger:1987:LDP

[Kar87] P. Karger. Limiting the damage potential of discretionary Trojan horses. In IEEE [IEE87c], pages 32–37. ISBN 0-8186-8771-1 (hardback), 0-8186-0771-8 (paperback), 0-8186-4771-X (microfiche). LCCN QA 76.9 A25 I43 1987. IEEE catalog number 87CH2416-6. Computer Society Order Number 771.

Kari:1989:CBP

[Kar89a] Jarkko Kari. A cryptosystem based on propositional logic. *Lecture Notes in Computer Science*, 381:210–219, 1989. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kari:1989:OCP

[Kar89b] Jarkko Kari. Observations concerning a public-key cryptosystem based on iterated morphisms. *Theoretical Computer Science*, 66(1):45–53, August 2, 1989. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Kasiski:1863:GDG

[Kas63] Friedrich Wilhelm Kasiski. *Die Geheimschriften und die Dechiffrirkunst, 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

[Kat77] Harry Katzan, Jr. *The Standard Data Encryption Algorithm*. Petrocelli Books, New York, NY, USA, 1977. ISBN 0-89433-016-0. viii + 134 pp. LCCN QA76.9 .A25K37.

Kawai:1987:LAI

[Kaw87] Satoru Kawai. Local authentication in insecure environments. *Information Processing Letters*, 25(3):171–174, May 29, 1987. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Klein:1989:STR

[KBD89] Shmuel T. Klein, Abraham Bookstein, and Scott Deerwester. Storing text retrieval systems on CD-ROM. compression and encryption considerations. *ACM Transactions on Information Systems*, 7(3): 230–245, July 1989. CODEN

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

Karp:1988:SDN

[KBN88] Bennett C. Karp, L. Kirk Barker, and Larry D. Nelson. The Secure Data Network System. *AT&T Technical Journal*, 67(3):19–27, May 1988. CODEN ATJOEM. ISSN 2376-676X (print), 8756-2324 (electronic).

Kam:1978:SDS

[KD78] John B. Kam and George I. Davida. A structured design of substitution-permutation encryption network. In *Foundations of secure computation (Workshop, Georgia Inst. Tech., Atlanta, Ga., 1977)*, pages 95–113. Academic Press, New York, NY, USA, 1978.

Kam:1979:SDS

[KD79] John B. Kam and George I. Davida. Structured design of substitution-permutation encryption networks. *IEEE Transactions on Computers*, 28(10): 747–753, 1979. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Kemp:1988:EEF

[Kem88] Elizabeth A. Kemp. Encryption in electronic funds transfer applications. Massey computer science report 88/2, Computer Science Department, Massey University, Palmerston North, NZ, December 1988. 16 pp.

Kemmerer:1989:AEP

[Kem89] Richard A. Kemmerer. Analyzing encryption protocols using formal verification techniques. Technical report TRCS 89-4, Department of Computer Science, College of Engineering, University of California, Santa Barbara, Santa Barbara, CA, USA, 1989. 23 pp.

Kerr:1975:PIC

[Ker75] Douglas S. Kerr, editor. *Proceedings of the International Conference on Very Large Data Bases, Framingham, MA, USA, September 22–24, 1975*. ACM Press, New York, NY 10036, USA, 1975. ISBN ???? ISSN 0278-2596. LCCN QA76.9.D3 I55 1975. US$15.00.

Kerr:1989:SNM

[Ker89] S. Kerr. A secret no more (security and encryption). *Datamation*, 35(13):53–55, July 1989. CODEN DTMNAT. ISSN 0011-6963.

Knoble:1979:EOW

[KFB79] H. D. Knoble, C. Forney, Jr., and F. S. Bader. An efficient one-way enciphering algorithm. *ACM Transactions on Mathematical Software*, 5(1):97–107, March 1979. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Kilian:1988:FCO

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In ACM [ACM88], pages 20–31. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988. URL `http://www.acm.org/pubs/articles/proceedings/stoc/62212/p20-kilian/p20-kilian.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/62212/p20-kilian/`. ACM order no. 508880.

Kak:1977:SEU

[KJ77] S. C. Kak and N. S. Jayant. On speech encryption using waveform scrambling. *The Bell System Technical Journal*, 56(5): 781–808, May–June 1977. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol56/bstj56-5-781.pdf`.

Kothari:1984:CMW

[KL84] S. Kothari and S. Lakshmivarahan. On the concealability of messages by the Williams public-key encryption scheme. *Computers and Mathematics with Applications*, 10(1):15–24, 1984. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic).

Kannan:1988:PFN

[KLL88] R. Kannan, A. K. Lenstra, and L. Lovász. Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers. *Mathematics of Computation*, 50(181):235–250, January 1988. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Kurosawa:1988:CSP

[KM88] K. Kurosawa and K. Matsu. Cryptographically secure pseudorandom sequence generator based on reciprocal number cryptosystem. *Electronics Letters*, 24(1):16–17, January 7, 1988. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8134`.

Konheim:1980:ICP

[KMM+80] Alan G. Konheim, Marian H. Mack, Robert K. McNeill, Bryant Tuckerman, and Gerald Waldbaum. The IPS cryptographic programs. *IBM Systems Journal*, 19(2):253–283, 1980. CODEN IBMSA7. ISSN 0018-8670.

Knoble:1979:AEO

[Kno79] H. D. Knoble. Algorithm 536: An efficient one-way enciphering algorithm [Z]. *ACM Transactions on Mathematical Software*, 5(1):108–111, March 1979. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Knuth:1969:SNM

[Knu69a] Donald E. Knuth. *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming*. Addison-Wesley, Reading, MA,

USA, 1969. ISBN 0-201-03802-1. xi + 624 pp. LCCN QA76.5 .K57. US$19.75. See pages 248–250.

Knuth:1969:SA

[Knu69b] Donald E. Knuth. *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming*. Addison-Wesley, Reading, MA, USA, 1969. ISBN 0-201-03802-1. xi + 624 pp. LCCN QA76.5 .K57. US$19.75.

Knuth:1973:FA

[Knu73] Donald E. Knuth. *Fundamental Algorithms*, volume 1 of *The Art of Computer Programming*. Addison-Wesley, Reading, MA, USA, second edition, 1973. ISBN 0-201-03809-9. xxi + 634 pp. LCCN QA76.6 .K641 1973.

Knuth:1980:DLC

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

Knuth:1985:DLC

[Knu85] Donald E. Knuth. Deciphering a linear congruential encryption. *IEEE Transactions on Information Theory*, IT-31(1):49–52, January 1985. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic). Russian translation, to appear.

Knuth:1987:CT

[Knu87] Donald E. Knuth. *N*-ciphered texts. *Word Ways*, 20(??):173–174, 191–192, 1987. ISSN 0043-7980.

Koblitz:1987:CNT

[Kob87a] Neal Koblitz. *A course in number theory and cryptography*, volume 114 of *Graduate texts in mathematics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1987. ISBN 0-387-96576-9. 208 pp. LCCN QA241 .K6721 1987. US$29.80.

Koblitz:1987:ECC

[Kob87b] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, January 1987. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Kochanski:1989:HSI

[Koc89] Martin Kochanski. How safe is it? (computer security). *BYTE Magazine*, 14(6):257–264, June 1989. CODEN BYTEDJ. ISSN 0360-5280.

Kolata:1977:NCC

[Kol77] Gina Bari Kolata. News and comment: Computer encryption and the National Security Agency connection. *Science*, 197(4302):438–440, July 29, 1977. CODEN SCIEAS. ISSN 0036-8075 (print), 1095-9203 (electronic). URL `http://science.sciencemag.org/content/197/4302/438/`.

Konheim:1981:CP

[Kon81] Alan G. Konheim. *Cryptography, a primer*. John Wiley and Sons, Inc., New York, NY, USA, 1981. ISBN 0-471-08132-9. xiv + 432 pp. LCCN Z103 .K66 1981. A Wiley-interscience publication.

Konheim:1985:CAE

[Kon85] Alan G. Konheim. Cryptanalysis of ADFGVX encipherment systems (extended abstract). In Blakley and Chaum [BC85], pages 339–341. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=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

[Kon89] Alan G. Konheim. Reviews: *Mathematical Cryptology for Computer Scientists and Mathematicians*, by Wayne Patterson; *A Course in Number Theory and Cryptography*, by Neal Koblitz. *American Mathematical Monthly*, 96(4):374–375, April 1989. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Koopman:1986:OES

[Koo86] Raymond F. Koopman. The orders of equidistribution of subsequences of some asymptotically random sequences. *Communications of the Association for Computing Machinery*, 29 (8):802–806, August 1986. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/6431.html`.

Koscielny:1983:PRD

[Kos83] Czeslaw Koscielny. *Programowa realizacja dzialan w cialach skonczonych do zastosowan w technice kodowania korekcyjnego i kryptografii*, volume 61. 11 of *Prace naukowe Instytutu Cybernetyki Technicznej Politechniki Wroclawskiej; Seria Monografie*. Wydawn. Politechniki Wroclawskiej, Wroclaw, Poland, 1983. ISBN ???? ISSN 0324-9786. 115 pp. LCCN QA76.9.A251 K6 1983. zl93.00. Title on p. [2] of cover: A software approach to computing in finite fields with applications to error-correcting coding technique and cryptography. Summary in English and Russian; legends and table of contents also in English. Bibliography: p. 109–110.

Kothari:1985:GLT

[Kot85] S. C. Kothari. Generalized linear threshold scheme. In

Blakley and Chaum [BC85], pages 231–241. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=231`. 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.

Koyama:1982:CUM

[Koy82a] Kenji Koyama. A cryptosystem using the master key for multi-address communication. *Systems-Comput.-Controls*, 13 (5):36–46 (1983), 1982. CODEN SYCCBB. ISSN 0096-8765.

Koyama:1982:MKR

[Koy82b] Kenji Koyama. A master key for the RSA public-key cryptosystem. *Systems-Comput.-Controls*, 13(1):63–70 (1983), 1982. CODEN SYCCBB. ISSN 0096-8765.

Koyama:1983:MKR

[Koy83] Kenji Koyama. A master key for the Rabin's public-key cryptosystem. *Systems-Comput.-Controls*, 14(6):49–57 (1984), 1983. CODEN SYCCBB. ISSN 0096-8765.

Kozaczuk:1984:EHGa

[Koz84a] Władysław Kozaczuk. *Enigma: how the German machine cipher was broken, and how it was read by the Allies in World War Two*. Arms and Armour, London, UK, 1984. ISBN 0-85368-640-8. xiv + 348 pp. LCCN D810.C88 K6813 1984b. Translation of: W kregu Enigmy.

Kozaczuk:1984:EHGb

[Koz84b] Władysław Kozaczuk. *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two*. Foreign intelligence book series. University Publications of America, Frederick, MD, USA, 1984. ISBN 0-89093-547-5. xiv + 348 pp. LCCN D810.C88 K6813 1984. US$24.00. Edited and translated by Christopher Kasparek, from the original Polish edition, *W kręgu Enigma*, Książka i Wiedza, Warsaw, 1979.

Kim:1989:PRP

[KP89] Su Hee Kim and Carl Pomerance. The probability that a random probable prime is composite. *Mathematics of Computation*, 53(188):721–741, October 1989. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Krause:1984:DEI

[Kra84] Lothar Krause. Data encryption in ISO, the international organization for standardization.

Computers and Security, 3(3): 234–236, August 1984. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404884900452`.

Kranakis:1986:PC

[Kra86] Evangelos Kranakis. *Primality and cryptography*. Wiley-Teubner series in computer science. John Wiley and Sons, Inc., New York, NY, USA, 1986. ISBN 0-471-90934-3. xv + 235 pp. LCCN TK5102.5 .K661 1986. US$38.00.

Kordes:1989:UMC

[KS89] F. L. G. Kordes and J. J. Schuurman. The use of MEBAS in creating a simulation environment for compression and encryption. Report NLR TP 89130 U, National Luchten Ruimtevaartlaboratorium, Amsterdam, The Netherlands, 1989. 69 pp.

Kuchlin:1987:PKE

[Küc87] W. Küchlin. Public key encryption. *SIGSAM Bulletin (ACM Special Interest Group on Symbolic and Algebraic Manipulation)*, 21(3):69–73, August 1987. CODEN SIGSBZ. ISSN 0163-5824 (print), 1557-9492 (electronic).

Kullback:1935:SMC

[Kul35] Solomon Kullback. *Statistical methods in cryptanalysis: technical paper*. War Dept., Office of the Chief Signal Officer: U.S. G.P.O., Washington, DC, USA, 1935. various pp.

Kullback:1938:SMC

[Kul38] 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

[Kul67] Solomon Kullback. *Statistical methods in cryptanalysis*. Number 14 in Technical literature series monograph. National Archives, Washington, DC, USA, revised edition, 1967. iii + 194 pp.

Kullback:1976:SMC

[Kul76] Solomon Kullback. *Statistical methods in cryptanalysis*, volume 4 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, revised edition, 1976. v + 206 pp. LCCN Z104 .K84.

Kearns:1989:CLL

[KV89] M. Kearns and L. G. Valiant. Cryptographic limitations on learning Boolean formulae and finite automata. In ACM-TOC'89 [ACM89c], pages 433–444. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989. URL `http://www.acm.org/pubs/articles/proceedings/stoc/73007/p433-kearns/p433-kearns.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/73007/p433-kearns/`.

Kasami:1982:KMS

[KYM82] Tadao Kasami, Saburo Yamamura, and Kenichi Mori. A key management scheme for end-to-end encryption and a formal verification of its security. *Systems-Comput.-Controls*, 13 (3):59–69 (1983), 1982. CODEN SYCCBB. ISSN 0096-8765.

Laffin:1964:CCS

[Laf64] John Laffin. *Codes and ciphers: secret writing through the ages*. Abelard-Schuman, ????, 1964. 164 pp.

Lagarias:1984:KPK

[Lag84a] J. C. Lagarias. Knapsack public key cryptosystems and Diophantine approximation (extended abstract). In *Advances in cryptology (Santa Barbara, Calif., 1983)*, pages 3–23. Plenum, New York, 1984.

Lagarias:1984:PAS

[Lag84b] J. C. Lagarias. Performance analysis of Shamir's attack on the basic Merkle–Hellman knapsack cryptosystem. *Lecture Notes in Computer Science*, 172:312–323, 1984. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lakshmivarahan:1983:APK

[Lak83] S. Lakshmivarahan. Algorithms for public key cryptosystems: theory and application. In *Advances in computers, Vol. 22*, volume 22 of *Adv. in Comput.*, pages 45–108. Academic Press, New York, NY, USA, 1983.

Lampson:1973:NCP

[Lam73] Butler W. Lampson. A note on the confinement problem. *Communications of the Association for Computing Machinery*, 16(10):613–615, October 1973. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1014.html`.

Lamport:1981:TNP

[Lam81] Leslie Lamport. Technical note: Password authentication with insecure communication. *Communications of the Association for Computing Machinery*, 24 (11):770–772, November 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Landers:1946:RPR

[Lan46] A. W. Landers. Recent publications: Reviews: *An Historical and Analytical Bibliography of the Literature of Cryptology*, by J. S. Galland. *American Mathematical Monthly*, 53(6):330–331, June/July 1946. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Langie:1981:CSS

[Lan81] Andre Langie. *Cryptography: a study on secret writings*, volume 38 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1981. ISBN 0-89412-061-1. vii + 192 pp. LCCN Z104 .L28 1981.

Translation of: De la cryptographie. Reprint of an unspecified previous ed. Bibliography: p. 158.

Landau:1989:SSC

[Lan89] Charles R. Landau. Security in a secure capability-based system. *Operating Systems Review*, 23(4):2–4, October 1989. CODEN OSRED8. ISSN 0163-5980.

Lassek:1985:CCA

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

Lauer:1981:CSC

[Lau81] Rudolph F. Lauer. *Computer simulation of classical substitution cryptographic systems*, volume 32 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1981. ISBN 0-89412-050-6. xi + 111 pp. LCCN Z104 .L38 1981.

Lee:1988:OSM

[LB88] P. J. Lee and E. F. Brickell. An observation on the security of McEliece's public-key cryptosystem. *Lecture Notes in Computer Science*, 330:275–280, 1988. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lee:1989:WBL

[LB89a] T. Paul Lee and R. E. Barkley. A watermark-based lazy buddy system for kernel memory allocation. In USENIX [USE89a], pages 1–13.

Lee:1989:WLB

[LB89b] T. Paul Lee and R. E. Barkley. A watermark-based lazy buddy system for kernel memory allocation. In USENIX Association [USE89b], pages 1–13. LCCN QA 76.76 O63 U83 1989.

Leary:1987:CSM

[Lea87] Penn Leary. *The Cryptographic Shakespeare: a monograph wherein the poems and plays attributed to William Shakespeare are proven to contain the enciphered name of the concealed author, Francis Bacon*. Westchester House, Omaha, NE, USA, 1987. ISBN 0-9617917-0-5. 272 pp. LCCN PR2944 .L38 1987.

Leclerc:1989:CRM

[Lec89] Matthias Leclerc. Chinesische Reste und moderne Kryptographie. (German) [Chinese remainders and modern cryptography]. *Mathematische Semesterberichte*, 36(2):257–267, 1989. CODEN ???? ISSN 0720-728X.

Leighton:1969:SCA

[Lei69] Albert C. Leighton. Secret communication among the Greeks and Romans. *Technology and Culture*, 10(2):139–154, April 1969. CODEN TECUA3. ISSN 0040-165X (print), 1097-3729 (electronic).

URL https://muse.jhu.edu/pub/1/article/892350/pdf.

Leighton:1979:BRA

[Lei79a] Albert C. Leighton. Book review: *An annotated bibliography of cryptography*: By David Shulman. Garland Reference Library of the Humanities, Vol. 37 New York/London (Garland Publishing Inc.). 1976. xvi + 372 pp. illus. $35.00. *Historia Mathematica*, 6(2): 213–218, May 1979. CODEN HIMADS. ISSN 0315-0860 (print), 1090-249X (electronic). URL http://www.sciencedirect.com/science/article/pii/0315086079900934.

Leighton:1979:BRB

[Lei79b] Albert C. Leighton. Book review: *An annotated bibliography of cryptography*: By David Shulman. Garland Reference Library of the Humanities, Vol. 37 New York/London (Garland Publishing Inc.). 1976. xvi + 372 pp. illus. $35.00. *Historia Mathematica*, 6(2): 213–218, May 1979. CODEN HIMADS. ISSN 0315-0860 (print), 1090-249X (electronic). URL http://www.sciencedirect.com/science/article/pii/0315086079900934.

Leiss:1980:NSS

[Lei80] E. Leiss. A note on a signature system based on probabilistic logic. *Information Processing Letters*, 11(2):110–113, October ??, 1980. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Lempel:1979:CT

[Lem79] Abraham Lempel. Cryptology in transition. *ACM Computing Surveys*, 11(4):285–303, December 1979. CODEN CMSVAN. ISSN 0010-4892.

Lennon:1978:CAI

[Len78] Richard E. Lennon. Cryptography architecture for information security. *IBM Systems Journal*, 17(2):138–150, 1978. CODEN IBMSA7. ISSN 0018-8670.

Lenstra:1987:FIE

[Len87] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Mathematics*, 126 (3):649–673, 1987. CODEN ANMAAH. ISSN 0003-486X (print), 1939-8980 (electronic). URL http://www.jstor.org/stable/1971363.

Levine:1958:VMS

[Lev58] Jack Levine. Variable matrix substitution in algebraic cryptography. *American Mathematical Monthly*, 65(3):170–179, March 1958. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Levine:1961:SAH

[Lev61a] Jack Levine. Some applications of high-speed computers to the case $n = 2$ of algebraic cryptography. *Mathematics of Computation*, 15(75):254–260, July 1961. CODEN MCM-

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

Levine:1961:SECa

[Lev61b] Jack Levine. Some elementary cryptanalysis of algebraic cryptography. *American Mathematical Monthly*, 68(5):411–418, May 1961. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Levine:1961:SECb

[Lev61c] Jack Levine. *Some elementary cryptanalysis of algebraic cryptography*. Mathematical Association of America, Buffalo, NY, USA, 1961. 411–418 pp. Reprint from American Mathematical Monthly, vol. 68, no. 5, May 1961.

Levine:1983:USC

[Lev83] Jack Levine. *United States cryptographic patents, 1861–1981*. Cryptologia, Terre Haute, IN, USA, 1983. ISBN 0-9610560-0-2. 69 pp. LCCN T223.Z1 .L48.

Levin:1985:OWF

[Lev85] L. A. Levin. One-way functions and pseudorandom generators. In ACM [ACM85], pages 363–365. ISBN 0-89791-151-2 (paperback). LCCN QA 76.6 A13 1985. URL `http://www.acm.org/pubs/articles/proceedings/stoc/22145/p363-levin/p363-levin.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/22145/p363-levin/`. ACM order no. 508850.

Lewin:1978:UGW

[Lew78] Ronald Lewin. *Ultra goes to war: the first account of World War II's greatest secret based on official documents*. McGraw-Hill, New York, NY, USA, 1978. ISBN 0-07-037453-8. 397 + 6 pp. LCCN D810.S7 L43 1978; D810.S7L43. US$12.95.

Lewin:1982:AMC

[Lew82] Ronald Lewin. *The American magic: codes, ciphers, and the defeat of Japan*. Farrar Straus Giroux, New York, NY, USA, 1982. ISBN 0-374-10417-4. xv + 332 pp. LCCN D810.C88 .L48.

Lexar:1976:END

[Lex76] Lexar Corporation. An evaluation of the NBS Data Encryption Standard. Unpublished report, Lexar Corporation, 11611 San Vicente Boulevard, Los Angeles, CA, USA, 1976.

Landwehr:1984:SMM

[LHM84] Carl E. Landwehr, Constance L. Heitmeyer, and John McLean. A security model for military message system. *ACM Transactions on Computer Systems*, 2 (3):198–222, August 1984. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

Lidl:1985:CBP

[Lid85] R. Lidl. On cryptosystems based on polynomials and finite fields. *Lecture Notes in Computer Science*, 209:10–15, 1985.

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

Lieberherr:1981:UCD

[Lie81] K. Lieberherr. Uniform complexity and digital signatures. *Theoretical Computer Science*, 16(1):99–110, October 1981. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

RFC0989

[Lin87] J. Linn. RFC 989: Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication procedures, February 1, 1987. URL `ftp://ftp.internic.net/rfc/rfc1040.txt`; `ftp://ftp.internic.net/rfc/rfc1113.txt`; `ftp://ftp.internic.net/rfc/rfc989.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc1040.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc1113.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc989.txt`. Obsoleted by RFC1040, RFC1113 [Lin88, Lin89]. Status: UNKNOWN.

RFC1040

[Lin88] J. Linn. RFC 1040: Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication procedures, January 1, 1988. URL `ftp://ftp.internic.net/rfc/rfc1040.txt`; `ftp://ftp.internic.net/rfc/rfc1113.txt`; `ftp://ftp.internic.net/rfc/rfc989.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc1040.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc1113.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc989.txt`. Obsoleted by RFC1113 [Lin89]. Obsoletes RFC0989 [Lin87]. Status: UNKNOWN.

RFC1113

[Lin89] J. Linn. RFC 1113: Privacy enhancement for Internet electronic mail: Part I — message encipherment and authentication procedures, August 1, 1989. URL `ftp://ftp.internic.net/rfc/rfc1040.txt`; `ftp://ftp.internic.net/rfc/rfc1113.txt`; `ftp://ftp.internic.net/rfc/rfc1421.txt`; `ftp://ftp.internic.net/rfc/rfc989.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc1040.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc1113.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc1421.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc989.txt`. Obsoleted by RFC1421 [Lin93]. Obsoletes RFC0989, RFC1040 [Lin87, Lin88]. Status: HISTORIC.

RFC1421

[Lin93] J. Linn. RFC 1421: Privacy enhancement for Internet electronic mail: Part I: Message encryption and authentication procedures, February 1993. URL `ftp://ftp.internic.net/rfc/rfc1113.txt`; `ftp://ftp.internic.`

net/rfc/rfc1421.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc1113.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc1421.txt. Obsoletes RFC1113 [Lin89]. Status: PROPOSED STANDARD.

Litant:1987:BRC

[Lit87] Thomas F. Litant. Book review: *Computer Security: the Practical Issues in a Troubled World*, (Elsevier Science Publishers, Amsterdam 1985). *Operating Systems Review*, 21(1): 3–5, January 1987. CODEN OSRED8. ISSN 0163-5980.

Laih:1989:NTS

[LLH89] Chi Sung Laih, Jau Yien Lee, and Lein Harn. A new threshold scheme and its application in designing the conference key distribution cryptosystem. *Information Processing Letters*, 32 (3):95–99, August 24, 1989. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Langie:1922:C

[LM22] André Langie and James Cruickshank Henderson Macbeth. *Cryptography*. Constable and Company Limited, London, UK, 1922. vii + 1 + 192 pp. LCCN Z 104 L26dE. Bibliography: p.158.

Luccio:1980:CMC

[LM80] F. Luccio and S. Mazzone. A cryptosystem for multiple communication. *Information Processing Letters*, 10(4–5):180–183, July 5, 1980. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See notes [Mei81, Hel81].

Lidl:1984:PPR

[LM84] Rudolf Lidl and Winfried B. Müller. Permutation polynomials in RSA-cryptosystems. In *Advances in cryptology (Santa Barbara, Calif., 1983)*, pages 293–301. Plenum, New York, 1984.

Leighton:1985:HBC

[LM85] Albert C. Leighton and Stephen M. Matyas. The history of book ciphers. In Blakley and Chaum [BC85], pages 101–113. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=101. 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.

Lagarias:1985:SLD

[LO85] J. C. Lagarias and A. M. Odlyzko. Solving low-density subset sum problems. *Journal of the Association for Computing Machinery*, 32(1):229–246, January 1985. CODEN

JACOAH. ISSN 0004-5411. URL http://www.acm.org/pubs/toc/Abstracts/0004-5411/2461.html. Preliminary version in *Proc. 24th IEEE Foundations Computer Science Symp.*, pp. 1–10, 1983.

Lomet:1983:HPU

[Lom83] David B. Lomet. A high performance, universal, key associative access method. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 13(4):120–133, May 1983. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Luciano:1987:CCC

[LP87] Dennis Luciano and Gordon Prichett. Cryptology: From Caesar ciphers to public-key cryptosystems. *College Mathematics Journal*, 18(1):2–17, January 1987. CODEN ???? ISSN 0746-8342 (print), 1931-1346 (electronic). URL http://www.tandfonline.com/doi/abs/10.1080/07468342.1987.11973000.

Luby:1986:PRP

[LR86] M. Luby and C. Rackoff. Pseudo-random permutation generators and cryptographic composition. In ACM [ACM86], pages 356–363. ISBN 0-89791-193-8. LCCN QA 76.6 A13 1986. URL http://www.acm.org/pubs/articles/proceedings/stoc/12130/p356-luby/p356-luby.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/12130/p356-luby/. ACM order number 508860.

Lagarias:1988:UEP

[LR88a] Jeffrey C. Lagarias and James A. Reeds. Unique extrapolation of polynomial recurrences. *SIAM Journal on Computing*, 17(2): 342–362, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Luby:1988:HCP

[LR88b] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17(2): 373–386, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Lange:1925:TC

[LS25] André Lange and E. A. Soudart. *Traité de cryptographie. (French) [Treatise on cryptography]*. Librairie Félix Alcan, Paris, France, 1925. xii + 366 + vi pp. LCCN Z104 .L26 1925.

Lange:1981:TC

[LS81] André Lange and E. A. Soudart. *Treatise on cryptography*, volume 36 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1981. ISBN 0-89412-055-7 (paperback). xvi + 168 pp. LCCN Z104.L2613 1981. Translation

of: Traite de cryptographie / par André Lange et E.-A. Soudart. "Plus many problems in French for the solver".

Lu:1989:SCI

[LS89] W. P. Lu and M. K. Sundareshan. Secure communication in Internet environments: a hierarchical key management scheme for End-to-End encryption. *IEEE Transactions on Communications*, 37(10):1014–1023, October 1, 1989. CODEN IECMBT. ISSN 0090-6778 (print), 1558-0857 (electronic).

Lamport:1982:BGP

[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.

Leung:1985:SCT

[LT85] A. K. Leung and S. E. Tavares. Sequence complexity as a test for cryptographic systems. In Blakley and Chaum [BC85], pages 468–474. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=468`. 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.

Lioen:1988:OMA

[LtW88a] W. Lioen, H. te Riele, and D. Winter. Optimization of the MPQS-factoring algorithm on the Cyber 205 and the NEC SX-2. *Supercomputer*, 5(4):42–50, July 1988. CODEN SPCOEL. ISSN 0168-7875.

Lioen:1988:OMF

[LtW88b] W. Lioen, H. te Riele, and D. Winter. Optimization of the MPQS-factoring algorithm on the Cyber 205 and the NEC SX-2. *Supercomputer*, 5(4):42–50, July 1988. CODEN SPCOEL. ISSN 0168-7875.

Lu:1979:EGC

[Lu79] Shyue Ching Lu. The existence of good cryptosystems for key rates greater than the message redundancy. *IEEE Transactions*

on Information Theory, 25(4): 475–477, 1979. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Lu:1980:AEG

[Lu80] Shyue Ching Lu. Addition to: "The existence of good cryptosystems for key rates greater than the message redundancy" [IEEE Trans. Inform. Theory **25** (1979), no. 4, 475–477; MR 80g:94069]. *IEEE Transactions on Information Theory*, 26(1): 129, 1980. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Long:1988:DLH

[LW88] Douglas L. Long and Avi Wigderson. The discrete logarithm hides $O(\log n)$ bits. *SIAM Journal on Computing*, 17(2): 363–372, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Ma:1979:RAD

[Ma79] Robert Ma. Review and analysis of the Data Encryption Standard. Master of science, plan ii., Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, Berkeley, CA, USA, 1979. 70 pp.

Meijer:1981:DSS

[MA81] Henk Meijer and Selim G. Akl. Digital signature schemes. Technical report 81-120, Department of Computing and Information Science, Queen's University, Kingston, ON, Canada, 1981. 10 pp.

MacPherson:1987:CUN

[Mac87] B. Nelson MacPherson. The compromise of US Navy cryptanalysis after the Battle of Midway. *Intelligence and National Security*, 2(2):320–??, 1987. ISSN 0268-4527 (print), 1743-9019 (electronic).

Mandelbrot:1960:BRJa

[Man60] Benoît Mandelbrot. Book review: John Chadwick, *The Decipherment of Linear B* (1958) Cambridge University Press. *Information and Control*, 3 (1):95–96, March 1960. CODEN IFCNA4. ISSN 0019-9958 (print), 1878-2981 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0019995860903478`.

Marsh:1970:CSS

[Mar70a] D. C. B. Marsh. *Cryptology as a senior seminar topic.* Mathematical Association of America, Buffalo, NY, USA, 1970. 761–764 pp. Reprint from American Mathematical Monthly, vol. 77, no. 7, August-September, 1970.

Marsh:1970:MEC

[Mar70b] D. C. B. Marsh. Mathematical education: Cryptology as a senior seminar topic. *American Mathematical Monthly*, 77 (7):761–764, August/September 1970. CODEN AMMYAE.

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

Marion:1976:ANB

[Mar76] Bruce Phillip Marion. Analysis of National Bureau of Standards Data Encryption Algorithm. Thesis (Engineer), Department of Electrical Engineering, Stanford University, Stanford, CA, USA, 1976. v + 46 pp.

Massey:1983:LFC

[Mas83] J. L. Massey. Logarithms in finite cycle groups – cryptographic issues. In Edward C. van der Meulen, editor, *Proceedings of the Fourth Symposium on Information Theory in the Benelux: held at the Brembergcentrum, Haasrode, Belgium, May 26–27, 1983*, pages 17–25. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1983. ISBN 90-334-0690-X. LCCN Q350 S988 1983.

Mastrovito:1989:VDM

[Mas89] 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

[Mat79] Stephen M. Matyas. Digital signatures — an overview. *Computer Networks: The International Journal of Distributed Informatique*, 3(2):87–94, April 1979. CODEN CNETDP. ISSN 0376-5075.

Mauborgne:1914:APC

[Mau14] Joseph O. Mauborgne. An advanced problem in cryptography and solution. Technical report, Army Service School's Press, Ft. Leavenworth, KS, USA, 1914. 21 pp.

Milner-Barry:1986:ADL

[MB86] 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

[McC75] John McCarthy. ACM Forum: Proposed criterion for a cipher to be probable-word-proof. *Communications of the Association for Computing Machinery*, 18(2):131–132, February 1975. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [FH74].

McIvor:1985:SC

[McI85] R. McIvor. Smart cards. *Scientific American*, 253(5):130–137, November 1985. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Meador:1920:KCE

[Mea20] J. E. D. Meador. Keeping the camera on an even keel, tele-

phoning in cipher. *Scientific American*, 123(5):107, July 31, 1920. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL `http://www.nature.com/scientificamerican/journal/v123/n5/pdf/scientificamerican0731-107a.pdf`.

Meijer:1981:NCM

[Mei81] H. Meijer. A note on "A cryptosystem for multiple communication" [Inform. Process. Lett. **10**(4–5), 5 July 1980, pp. 180–183]. *Information Processing Letters*, 12(4):179–181, August 13, 1981. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [LM80, Hel81].

Meijer:1983:CCC

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

Meijer:1985:MEN

[Mei85] Henk Meijer. Multiplication-permutation encryption networks. Technical report 85-171, Department of Computing and Information Science, Queen's University, Kingston, Ont., Canada, 1985. 15 pp.

Mendelsohn:1939:CC

[Men39] Charles Jastrow Mendelsohn. *Cardan on cryptography*. Yeshiva College, New York, NY, USA, 1939. 157–168 pp. LCCN ???? Reprinted from Scripta mathematica, Vol. 6, No. 3, October, 1939. J. S. Galland, Bibliography of ... cryptology, 1945, p. 124.

Mendelsohn:1989:CWI

[Men89] John Mendelsohn, editor. *Covert warfare: intelligence, counterintelligence, and military deception during the World War II era*. Garland, New York, NY, USA, 1989. ISBN 0-8240-7950-7 (vol. 1). ???? pp. LCCN D810.S7 C66 1989. US$60.00.

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

[Mer78] Ralph C. Merkle. Secure communications over insecure channels. *Communications of the Association for Computing Machinery*, 21(4):294–299, April 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Merkle:1980:PPK

[Mer80] R. C. Merkle. Protocols for public key cryptosystems. In IEEE [IEE80], page ?? LCCN QA76.9.A25S95 1980.

Merkle:1982:PPK

[Mer82a] Ralph C. Merkle. Protocols for public key cryptosystems. In *Secure communications and asymmetric cryptosystems*, volume 69 of *AAAS Sel. Sympos. Ser.*, pages 73–104. Westview, Boulder, CO, 1982.

Merkle:1982:SAP

[Mer82b] Ralph C. (Ralph Charles) Merkle. *Secrecy, authentication, and public key systems*, volume 18 of *Computer science. Systems programming*. UMI Research Press, Ann Arbor, MI, USA, 1982. ISBN 0-8357-1384-9. 104 pp. LCCN QA76.9.A25 M47 1982. Revision of the author's thesis (Ph.D.—Stanford University, 1979).

Merkle:1988:DSB

[Mer88] Ralph C. Merkle. A digital signature based on a conventional encryption function. In Carl Pomerance, editor, *Advances in Cryptology — CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*, pages 369–378. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988. ISBN 3-540-48184-2.

Merkle:1989:CDS

[Mer89] Ralph C. Merkle. A certified digital signature. *Lecture Notes in Computer Science*, 435:218–238, 1989. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `https://link.springer.com/chapter/10.1007/0-387-34805-0_21`.

Meyer:1973:DCC

[Mey73] C. H. Meyer. Design considerations for cryptography. *AFIPS Conference Proceedings*, 42(??): 603–606, ???? 1973.

Merkle:1978:HIS

[MH78] Ralph Merkle and Martin E. Hellman. Hiding information and signatures in trap door knapsacks. *IEEE Transactions on Information Theory*, 24(5): 525–530, 1978. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Merkle:1981:SME

[MH81] Ralph C. Merkle and Martin E. Hellman. On the security of multiple encryption. *Communications of the Association for Computing Machinery*, 24(7): 465–467, July 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Matsumoto:1988:PQP

[MI88] Tsutomu Matsumoto and Hideki Imai. Public quadratic polynomial-tuples for efficient signature-verification and message encryption. In Gunther [Gun88b], pages 419–453. CODEN LNCSD9. ISBN 0-387-50251-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.330; QA76.9.A25 E9641 1988. Sponsored by the International Association for Cryptologic Research.

Michener:1988:TSK

[Mic88] John R. Michener. A tool for secret key cryptography. *Dr. Dobb's Journal of Software Tools*, 13(8):50–52, 55, 96, August 1988. CODEN DDJOEB. ISSN 0888-3076.

Millikin:1943:ECCa

[Mil43a] Donald D. Millikin. *Elementary cryptography and cryptanalysis*, volume 56 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1943. ISBN 0-89412-173-1 (soft cover), 0-89412-174-X (library bound). vii + 132 pp. LCCN ????

Millikin:1943:ECCb

[Mil43b] Donald D. Millikin. *Elementary cryptography and cryptanalysis*. New York University Bookstore, New York, NY, USA, second edition, 1943. vii + 132 + 1 + 28 pp.

Millikin:1943:ECCc

[Mil43c] Donald D. Millikin. *Elementary cryptography and cryptanalysis*. Aegean Park Press, Laguna Hills, CA, USA, third edition, 1943. vii + 132 pp.

Miller:1976:RHT

[Mil76] G. L. Miller. Reimann's hypothesis and tests for primality. *Journal of Computer and System Sciences*, 13:300–317, 1976. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic).

Miller:1985:PES

[Mil85] Jay I. Miller. A private-key encryption system based on plane geometry. Thesis (M.S. in Computer Science), University of Wisconsin-Milwaukee, Milwaukee, WI, USA, 1985. iv + 33 + 115 pp.

Miller:1986:UEC

[Mil86] V. S. Miller. Uses of elliptic curves in cryptography. In Williams [Wil86b], pages 417–426. CODEN LNCSD9. ISBN 0-387-16463-4 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1985; QA267.A1 L43 no.218. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0218.htm; http://www.springerlink.com/content/978-0-387-16463-2; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=218.

Millen:1987:CCC

[Mil87a] Jonathan K. Millen. Covert channel capacity. In IEEE [IEE87c], pages 60–66. ISBN 0-8186-8771-1 (hardback), 0-8186-0771-8 (paperback), 0-8186-4771-X (microfiche). LCCN QA 76.9 A25 I43 1987. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1016.html. IEEE catalog number 87CH2416-6. Computer Society Order Number 771.

Mills:1987:RDP

[Mil87b] D. L. Mills. RFC 1004: Distributed-protocol authentication scheme, April 1, 1987. URL ftp://ftp.internic.net/rfc/rfc1004.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc1004.txt. Status: EXPERIMENTAL.

Mitchell:1976:EAD

[Mit76] James Melvin Mitchell. Encryption algorithm for data security based on a polyalphabetic substitution scheme and a pseudo-random number generator. Thesis (M.S.), University of Tennessee, Knoxville, Knoxville, TN, USA, 1976. v + 83 pp.

Mitchell:1989:MDS

[Mit89] C. Mitchell. Multi-destination secure electronic mail. *The Computer Journal*, 32(1):13–15, February 1989. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/32/1/13.full.pdf+html; http://www3.oup.co.uk/computer_journal/hdb/Volume_32/Issue_01/tiff/13.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_32/Issue_01/tiff/14.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_32/Issue_01/tiff/15.tif.

Monge:1967:NMC

[ML67] Alf Monge and O. G. Landsverk. *Norse medieval cryptography in runic carvings*. Norseman Press, Glendale, CA, USA, 1967. 224 pp. LCCN E105 .M65. Includes bibliographies.

Maulucci:1987:HAC

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

25th Anniversary of Committee X3; The Code-Breaking Computers of 1944. *Annals of the History of Computing*, 9(3/4):345–356, July/September 1987. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1987/pdf/a3345.pdf`; `http://www.computer.org/annals/an1987/a3345abs.htm`.

Matyas:1978:GDI

[MM78] Stephen M. Matyas and Carl H. Meyer. Generation, distribution, and installation of cryptographic keys. *IBM Systems Journal*, 17(2):126–137, 1978. CODEN IBMSA7. ISSN 0018-8670.

Meyer:1982:CND

[MM82] Carl H. Meyer and Stephen M. Matyas. *Cryptography: a new dimension in computer data security: a guide for the design and implementation of secure systems*. John Wiley and Sons, Inc., New York, NY, USA, 1982. ISBN 0-471-04892-5. xxi + 755 pp. LCCN Z103 .M55. US$39.95.

Moler:1983:SVA

[MM83] Cleve Moler and Donald Morrison. Singular value analysis of cryptograms. *American Mathematical Monthly*, 90(2):78–87, February 1983. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Meadows:1987:MSA

[MM87] C. Meadows and D. Mutchler. Matching secrets in the absence of a continuously available trusted authority. *IEEE Transactions on Software Engineering*, SE-13(2):289–292, February 1987. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1702207`.

Muller:1981:SRP

[MN81] Winfried B. Müller and Wilfried Nöbauer. Some remarks on public-key cryptosystems. *Studia Sci. Math. Hungar.*, 16 (1-2):71–76, 1981. CODEN SSMHAX. ISSN 0081-6906.

Muller:1986:CDS

[MN86] Winfried B. Müller and Rupert Nöbauer. Cryptanalysis of the Dickson-scheme. *Lecture Notes in Computer Science*, 219:50–61, 1986. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Matsumoto:1982:DTL

[MOI82] Tsutomu Matsumoto, Tomoko Okada, and Hideki Imai. Directly transformed link encryption. *Systems-Comput.-Controls*, 13(6):36–44 (1983), 1982. CODEN SYCCBB. ISSN 0096-8765.

Montgomery:1985:MMT

[Mon85] Peter L. Montgomery. Modular multiplication without trial division. *Mathematics*

of Computation, 44(170):519–521, April 1985. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/journals/mcom/1985-44-170/S0025-5718-1985-0777282-X/`.

Morland:1666:NMC

[Mor66] Sir Samuel Morland. *A New Method of Cryptography*. ????, ????, 1666. 12 pp. Microfilm in Folger Shakespeare Library, Washington, DC, USA.

Morrice:1692:EB

[Mor92] Roger Morrice. *Entring Book*. ????, ????, 1692. 1500 pp. URL `http://www.hist.cam.ac.uk/seminars_events/events/roger-morrice.html; http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2003/08/29/ndiary29.xml`. Three volumes.

Morrison:1983:SEA

[Mor83] D. R. Morrison. Subtractive encryptors: alternatives to the DES. *ACM SIGACT News*, 15 (1):67–77, Winter–Spring 1983. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Morain:1988:IGP

[Mor88] F. Morain. Implementation of the Goldwasser-Killian-Atkin primality testing algorithm. Technical report, Institut de la Recherche en Informatique et Automatique, now Institut National de Recherche en Informatique et Automatique (INRIA), Domaine de Voluceau, Rocquencourt, B.P. 105, 78153 Le Chesnay Cedex, France, 1988. ?? pp. Project ALGO, INRIA.

Mora:1989:AAA

[Mor89] Teo Mora, editor. *Applied algebra, algebraic algorithms, and error-correcting codes: 6th international conference, AAECC-6, Rome, Italy, July 4–8, 1988: proceedings*, volume 357 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1989. CODEN LNCSD9. ISBN 0-387-51083-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA268 .A35 1988. US$36.00 (USA).

Mullin:1988:ONB

[MOVW89] R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone, and R. M. Wilson. Optimal normal bases in GF(p^n). *Discrete Applied Mathematics*, 22(2):149–161, 1988–1989. CODEN DAMADU. ISSN 0166-218X.

Mevis:1986:SCP

[MP86] Howard Mevis and Janet Plant. *Satellite communications: a practical guide to satellite TV encryption with tips on installing decoders, solving reception problems, and upgrading TVROs*. American Hospital Association, Media Center, Chicago, IL, USA, 1986. 25 pp.

Mori:2002:CSD

[MPS02] G. Mori, F. Paterno, and C. Santoro. CTTE: support for developing and analyzing task models for interactive system design. *IEEE Transactions on Software Engineering*, 28(8):797–813, August 2002. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1027801`.

Micali:1987:NSP

[MRS87] Silvio Micali, Charles Rackoff, and Bob Sloan. The notion of security for probabilistic cryptosystems (extended abstract). *Lecture Notes in Computer Science*, 263:381–392, 1987. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Micali:1988:NSP

[MRS88] Silvio Micali, Charles Rackoff, and Bob Sloan. The notion of security for probabilistic cryptosystems. *SIAM Journal on Computing*, 17(2):412–426, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Mitchell:1989:RHF

[MRW89] Chris Mitchell, Dave Rush, and Michael Walker. A remark on hash functions for message authentication. *Computers and Security*, 8(1):55–58, February 1, 1989. CODEN CPSEDU. ISSN 0167-4048.

Macalister:1976:SLI

[MS76] Robert Alexander Stewart Macalister and John Sampson. *The secret languages of Ireland: Ogham, Hisperic, Bearlagair na Saer, Bog-Latin, and cryptography, with special reference to the origin and nature of the Shelta language; partly based upon collections and manuscripts of the late John Sampson; with an English-jargon vocabulary*. APA-Philo Press, Amsterdam, The Netherlands, 1976. ISBN 90-6022-276-8. x + 284 pp. LCCN PM9001 .M2 1976. Reprint of the 1937 ed. published by the Cambridge University Press, Cambridge, England.

McEliece:1981:SSR

[MS81] R. J. McEliece and D. V. Sarwate. On sharing secrets and Reed–Solomon codes. *Communications of the Association for Computing Machinery*, 24(9): 583–584, September 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Muller-Schloer:1983:MBC

[MS83] C. Müller-Schloer. A microprocessor-based cryptoprocessor. *IEEE Micro*, 3(5):5–15, September/October 1983. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Moore:1987:CSK

[MS87] J. H. Moore and G. J. Simmons. Cycle structure of the DES

for keys having palindromic (or antipalindromic) sequences of round keys. *IEEE Transactions on Software Engineering*, SE-13(2):262–273, February 1987. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1702205`.

Meyer:1972:PCC

[MT72] C. H. Meyer and W. L. Tuchman. Pseudorandom codes can be cracked. *Electronic Design*, 20(23):74–76, November 9, 1972. CODEN ELODAW. ISSN 0013-4872 (print), 1944-9550 (electronic).

Mullender:1986:DCD

[MT86] S. J. Mullender and A. S. Tanenbaum. The design of a capability-based distributed operating system. *The Computer Journal*, 29(4):289–299, August 1986. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/289.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/290.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/291.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/292.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/293.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/294.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/295.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/296.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/297.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/298.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/299.tif`.

Marayati:1987:AWA

[MTA87] Muhammad Marayati, Muhammad Hassan Tayyan, and Yahya Mir 'Alam. *'Ilm al-ta'miyah wa-istikhraj al-mu'amma 'inda al-'Arab*. Majma' al-Lughah al-'Arabiyah bi-Dimashq, Damascus, Syria, 1987. various pp. LCCN Z103.4.A65 M37 1987. Abstract in English. Title on added t.p.: Origins of Arab cryptography and cryptanalysis. Contents: al-juz' 1. Dirasat wa-tahqiq li-rasa'il al-Kindi wa-Ibn 'Adlan wa-Ibn al-Durayhim.

Mackinnon:1985:OAA

[MTMA85] S. J. Mackinnon, P. D. Taylor, H. Meijer, and S. G. Akl. An optimal algorithm for assigning cryptographic keys to control access in a hierarchy.

IEEE Transactions on Computers, C-34(9):797–802, September 1985. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1676635`.

Muftic:1988:SMC

[Muf88] Sead Muftic. Security mechanisms for computer networks. current results of the CEC COST-11 ter project. *Computer Networks and ISDN Systems*, 15(1):67–71, 1988. CODEN CNISE9. ISSN 0169-7552.

Mulherin:1981:FDE

[Mul81] Michael Hugh Mulherin. A file data encryption system using Galois fields. Thesis (M.Sc.Cs.), University of New Brunswick, Ottawa, ON, Canada, 1981. 174 pp. 2 microfiche(s) (174 fr.).

Mullin:1984:NMP

[Mul84] Albert A. Mullin. A note on the mathematics of public-key cryptosystems. *Computers and Security*, 3(1):45–47, February 1984. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404884900269`.

Mulligan:1989:UMA

[Mul89a] Timothy Mulligan, editor. *ULTRA, MAGIC, and the Allies*, volume 1 of *Covert warfare*. Garland, New York, NY, USA, 1989. ISBN 0-8240-7950-7. (various) pp. LCCN D810.S7 C66 1989 vol. 1; D810.C88. US$60.00.

Mullin:1989:LEN

[Mul89b] 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 AMMYAE. 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

[Mur87] J. T. Muraszko, editor. *Colloquium on Vehicle Route Guidance, Navigation and Location Systems (Wednesday, 11 February 1987: London, England)*. IEE, London, UK, 1987. LCCN TE228 .C66 1987. Digest no.: 1987/21.

Merwin:1979:NCC

[MZS79] Richard E. Merwin, Jacqueline T. Zanca, and Merlin. Smith, editors. *1979 National Computer Conference: June 4–7, 1979, New York, New York*, volume 48 of *AFIPS Conference proceedings*. AFIPS Press, Montvale, NJ, USA, 1979.

Naik:1989:CDS

[Nai89] Varsha Naik. Cryptology in data security environment: what should be the new trend? Technical report, ????, ????, 1989. 63 pp.

Nanovic:1936:SWI

[Nan36] John Leonard Nanovic. *Secret writing: an introduction to cryptograms, ciphers and codes*. D. Kemp and Co, New York, NY, USA, 1936. x + 117 + 1 pp. LCCN Z104 .N3. See also reprint [Nan74].

Nanovic:1974:SWI

[Nan74] John L. (John Leonard) Nanovic. *Secret writing: an introduction to cryptograms, ciphers, and codes*. Dover Publications, Inc., New York, NY, USA, 1974. ISBN 0-486-23062-7. x + 117 pp. LCCN Z104.N35 1974. Reprint of the 1936 edition [Nan36].

NBS:1977:DES

[Nat77] National Bureau of Standards. *Data Encryption Standard*. U. S. Department of Commerce, Washington, DC, USA, January 1977. 18 pp.

NBS:1980:MO

[Nat80] National Bureau of Standards. *DES Modes of Operation*. U. S. Department of Commerce, Washington, DC, USA, December 1980. 16 pp.

NCSOTS:1984:ISR

[Nat84] National Communications System (U.S.). Office of Technology and Standards. Interoperability and security requirements for use of the Data Encryption Standard in the physical layer of data communications. Federal standard 1026, General Services Administration, Office of Information Resources Management, Washington, DC, USA, August 3, 1984. various pp.

NIST:1985:FPSa

[Nat85a] National Institute of Standards and Technology. *FIPS PUB 112: Standard for Password Usage*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, May 30, 1985. URL `http://www.itl.nist.gov/fipspubs/fip112.htm`.

NIST:1985:FPSb

[Nat85b] National Institute of Standards and Technology. *FIPS PUB 113: Standard for Computer Data Authentication*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, May 30, 1985. URL `http://www.itl.nist.gov/fipspubs/fip113.htm`.

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

[NBS76] NBS. The NBS workshop on cryptography in support of computer security. Unpublished memorandum, U.S. National Bureau of Standards, Gaithersburg, MD, USA, September 1976.

Nilsson:1978:OST

[NBWH78] Arne Nilsson, Rolf Blom, Harald Wesemeyer, and S. Hellstrom. On overflow systems in telephone networks: general service times in the secondary group. *Ericsson technics*, 34(2): 48–128, 1978.

Neat:1975:NCC

[Nea75] Charlie Edmund Neat. *A new computer cryptography: the Expanded Character Set (ECS) cipher*. PhD thesis, Engineering, University of California, Los Angeles, Los Angeles, CA, USA, 1975. xxi + 203 pp.

Niederreiter:1986:KTC

[Nie86] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform.*, 15 (2):159–166, 1986. CODEN PUTIAI. ISSN 0370-2529.

Niederreiter:1988:SNC

[Nie88] Harald Niederreiter. Some new cryptosystems based on feedback shift register sequences. *Math. J. Okayama Univ.*, 30: 121–149, 1988. CODEN MJOKAP. ISSN 0030-1566.

NIST:1985:FPC

[NIS85] NIST. *FIPS PUB 113: Computer Data Authentication*. National Institute of Standards and Technology (formerly National Bureau of Standards), Gaithersburg, MD, USA, May 30, 1985. ?? pp.

Nissan:1989:AIM

[Nis89] Ephraim Nissan. Artificial intelligence for a metatheory of interpretation. (A knowledge-analysis of Bernardini Marzolla's Indoglottal interpretation of Etruscan: For a metamodel of interpretation). Technical Report Report, 133 p. (available from the author), CMS, Univ. of Greenwich, Woolwich, London, UK, 1989.

Nakamura:1988:DRM

[NM88] Yasuhiro Nakamura and Kineo Matsui. Dual reduction method of random keys for encryption by graph transformation. *Mem. Nat. Defense Acad.*, 28(1):39–51, 1988. CODEN MDPCAW. ISSN 0388-4112.

Nobauer:1984:CRS

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

255–264. ISBN 3-209-00591-5, 3-519-02762-3. LCCN ????

Nobauer:1985:CRS

[Nöb85] Rupert Nöbauer. Cryptanalysis of the Rédei-scheme. In *Contributions to general algebra, 3 (Vienna, 1984)*, pages 255–264. Hölder-Pichler-Tempsky, Vienna, Austria, 1985.

Nobauer:1988:CPK

[Nöb88] Rupert Nöbauer. Cryptanalysis of a public-key cryptosystem based on Dickson-polynomials. *Mathematica Slovaca*, 38(4):309–323, 1988. CODEN MASLDM. ISSN 0139-9918.

Norman:1973:SWB

[Nor73] Bruce Norman. *Secret warfare: the battle of codes and ciphers*. David and Charles, Newton Abbot, UK, 1973. ISBN 0-7153-6223-2. 187 pp. LCCN Z103 .N67.

Needham:1978:UEAa

[NS78a] R. M. (Roger Michael) Needham and Michael D. Schroeder. Using encryption for authentication in large networks of computers. Technical Report CSL-78-4, Xerox Palo Alto Research Center, Palo Alto, CA, USA, 1978. ?? pp. Reprinted June 1982.

Needham:1978:UEAb

[NS78b] Roger M. Needham and Michael D. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the Association for Computing Machinery*, 21 (12):993–999, December 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Needham:1987:AR

[NS87] R. M. Needham and M. D. Schroeder. Authentication revisited. *Operating Systems Review*, 21(1):7, January 1987. CODEN OSRED8. ISSN 0163-5980.

Neuman:1988:AUE

[NS88] B. Clifford Neuman and Jennifer G. Steiner. Authentication of unknown entities on an insecure network of untrusted workstations. In USENIX Association [USE88b], pages 10–11. LCCN QA76.8.U65 U55 1988(1)-1990(2)//. Abstract only.

Norris-Saucedo:1989:DAD

[NS89] Steven Joseph Norris-Saucedo. Development and application of data encryption using a data shuffling technique. Thesis (M.S.), Department of Electrical Engineering, University of Colorado at Denver, Denver, CO, USA, 1989. vii + 94 pp.

Nemetz:1988:RLS

[NU88] T. Nemetz and J. Ureczky. A random linear secret-key encryption. In *Probability theory and mathematical statistics with applications (Visegrád,*

1985), pages 171–180. D. Reidel, Dordrecht, Boston, Lancaster, Tokyo, 1988.

Naor:1989:UOW

[NY89a] M. Naor and M. Yung. Universal one-way hash functions and their cryptographic applications. In ACM-TOC'89 [ACM89c], pages 33–43. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989. URL `http://www.acm.org/pubs/articles/proceedings/stoc/73007/p33-naor/p33-naor.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/73007/p33-naor/`.

Naor:1989:UOH

[NY89b] Moni Naor and Moti Yung. Universal one-way hash functions and their cryptographic applications. In ACM-TOC'89 [ACM89c], pages 33–43. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989.

Oakley:1978:RPC

[Oak78] Howard T. Oakley. *The Riverbank publications on cryptology.* ????, Washington, DC, USA, 1978. 324–330 pp.

OConnell:1981:CDE

[O'C81] Richard O'Connell. *Cryptoease: a data encryption dictionary.* Atlantis Editions, Philadelphia, PA, USA, 1981. 33 pp.

Odlyzko:1984:CAM

[Odl84] Andrew M. Odlyzko. Cryptanalytic attacks on the multiplicative knapsack cryptosystem and on Shamir's fast signature scheme. *IEEE Transactions on Information Theory*, IT-30(4):594–601, 1984. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic). URL `http://www.research.att.com/~amo/doc/arch/knapsack.attacks.pdf; http://www.research.att.com/~amo/doc/arch/knapsack.attacks.ps; http://www.research.att.com/~amo/doc/arch/knapsack.attacks.troff`.

Odlyzko:1985:DLF

[Odl85] A. M. Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. In Beth et al. [BCI85], pages 224–314. CODEN LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E951 1984. URL `http://www.research.att.com/~amo/doc/arch/discrete.logs.pdf; http://www.research.att.com/~amo/doc/arch/discrete.logs.ps; http://www.research.att.com/~amo/doc/arch/discrete.logs.troff`. Held at the University of Paris, Sorbonne.

Odlyzko:1987:CCD

[Odl87a] A. M. Odlyzko. On the complexity of computing discrete logarithms and factoring integers. In Cover and Gopinath [CG87], pages 113–116. ISBN 0-387-96621-8. LCCN TK5102.5 .O243 1987.

US$25.00. URL http://www.research.att.com/~amo/doc/arch/factoring.logs.pdf; http://www.research.att.com/~amo/doc/arch/factoring.logs.ps; http://www.research.att.com/~amo/doc/arch/factoring.logs.troff.

Odlyzko:1987:ACC

[Odl87b] Andrew Michael Odlyzko, editor. *Advances in cryptology: CRYPTO '86: proceedings*, volume 263 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1987. CODEN LNCSD9. ISBN 3-540-18047-8, 0-387-18047-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1986. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0263.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=263. Conference held at the University of California, Santa Barbara, Aug. 11–15, 1986.

Okamoto:1988:DMS

[Oka88] Tatsuaki Okamoto. A digital multisignature scheme using bijective public-key cryptosystems. *ACM Transactions on Computer Systems*, 6 (4):432–441, November 1988. CODEN ACSYEC. ISSN 0734-2071. URL http://www.acm.org:80/pubs/citations/journals/tocs/1988-6-4/p432-okamoto/.

Oldehoeft:1984:SSU

[OM84] Arthur E. Oldehoeft and Robert McDonald. A software scheme for user-controlled file encryption. *Computers and Security*, 3 (1):35–41, February 1984. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404884900245.

ONeil:1986:ETM

[O'N86] Patrick E. O'Neil. The Escrow transactional method. *ACM Transactions on Database Systems*, 11(4):405–430, December 1986. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL http://www.acm.org/pubs/articles/journals/tods/1986-11-4/p405-o_neil/p405-o_neil.pdf; http://www.acm.org/pubs/citations/journals/tods/1986-11-4/p405-o_neil/; http://www.acm.org/pubs/toc/Abstracts/tods/7265.html.

Otway:1987:ETM

[OR87] Dave Otway and Owen Rees. Efficient and timely mutual authentication. *Operating Systems Review*, 21(1):8–10, January 1987. CODEN OSRED8. ISSN 0163-5980.

Orton:1987:VIP

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

S. E. Tavares. VLSI implementation of public-key encryption algorithms. In *Advances in cryptology—CRYPTO '86 (Santa Barbara, Calif., 1986)*, volume 263 of *Lecture Notes in Comput. Sci.*, pages 277–301. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1987.

OShea:1988:CDU

[O'S88] G. O'Shea. Controlling the dependency of user access control mechanisms on correctness of user identification. *The Computer Journal*, 31(6):503–509, December 1988. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Ong:1985:ESS

[OSS85] H. Ong, C. P. Schnorr, and A. Shamir. Efficient signature schemes based on polynomial equations (preliminary version). In Blakley and Chaum [BC85], pages 37–46. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=37`. 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.

Ozarow:1984:WTC

[OW84] Lawrence H. Ozarow and Aaron D. Wyner. Wire-tap channel II. *ATT Bell Lab. tech. j*, 63(10 part 1):2135–2157, 1984. CODEN ABLJER. ISSN 0748-612X (print), 2376-7162 (electronic).

Parthasarathy:1985:DSG

[Par85] Aiyaswamy Parthasarathy. Digital signature generator for cryptographic applications. Thesis (M.S.), South Dakota School of Mines and Technology, Rapid City, SD, USA, 1985. 148 pp.

Patterson:1987:MCC

[Pat87] Wayne Patterson. *Mathematical cryptology for computer scientists and mathematicians*. Rowman and Littlefield, Totowa, NJ, USA, 1987. ISBN 0-8476-7438-X. xxii + 312 pp. LCCN Z103 .P351 1987. US$29.50.

Preneel:1989:CHB

[PBGV89] Bart Preneel, Antoon Bosselaers, Rene Govaerts, and Joos Vandewalle. Collision-free hashfunctions based on blockcipher algorithms. In *Proceedings 1989 International Carnahan Conference on Security Technology (Oct 3–5 1989: Zurich, Switzerland)*, pages 203–210. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA,

1989. IEEE catalog number 89CH2774-8.

Pearcey:1980:EDS

[Pea80] T. (Trevor) Pearcey. *Encryption in data systems and communication*. Caulfield Institute of Technology. Computer Abuse Research and Bureau (CITCARB), Caulfield, Victoria, Australia, 1980. ISBN 0-909176-14-0. 99 pp. LCCN ????

Pelta:1960:SP

[Pel60] Harold N. Pelta. Selfcipher: Programming. *Communications of the Association for Computing Machinery*, 3(2):83, February 1960. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Perret:1890:RCS

[Per90] P.-M. Perret. Les règles de Cicco Simonetta pour le déchiffrement des écritures secrètes (4 juillet 1474). (French) [the rules of Cicco Simonetta for decryption of secret writings (4 July 1474)]. *Bibliothèque de lÉcole des chartes*, 51:516–525, 1890. ISSN 0373-6237 (print), 1953-8138 (electronic). URL `http://www.jstor.org/stable/43000437`.

Peralta:1985:TRN

[Per85] Rene Caupolican Peralta. *Three results in number theory and cryptography: a new algorithm to compute square roots modulo a prime number; On the bit complexity of the discrete logarithm; A framework for the study of cryptoprotocols*. Thesis (Ph.D.), Department of Computer Science, University of California, Berkeley, Berkeley, CA, USA, December 1985. 52 pp.

Perry:1988:EBG

[Per88] Tekla S. Perry. Electronic banking goes to market. *IEEE Spectrum*, 25(2):46–49, February 1988. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Pfleeger:1989:SC

[Pfl89] Charles P. Pfleeger. *Security in computing*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 1989. ISBN 0-13-798943-1. xxi + 538 pp. LCCN QA76.9.A25 P45 1989.

Pohlig:1978:IAC

[PH78] S. C. Pohlig and M. E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Transactions on Information Theory*, 24(1): 106–111, ???? 1978. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Pichler:1986:ACE

[Pic86] Franz Pichler, editor. *Advances in cryptology: Eurocrypt 85: proceedings of a workshop on the theory and application of cryptographic techniques, Linz, Austria, April, 1985*, volume 219 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg,

Germany / London, UK / etc., 1986. CODEN LNCSD9. ISBN 0-387-16468-5 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E961 1985. "The workshop was sponsored by International Association for Cryptologic Research ... [et al.]"–T.p. verso.

Pierce:1977:SSP

[Pie77] Clayton C. Pierce. *Secret and secure: privacy, cryptography, and secure communication*. Pierce, Ventura, CA, USA, 1977. iv + 84 pp. LCCN Z103.P531.

Popek:1979:ESC

[PK79] Gerald J. Popek and Charles S. Kline. Encryption and secure computer networks. *ACM Computing Surveys*, 11(4):331–356, December 1979. CODEN CMSVAN. ISSN 0010-4892.

Pless:1975:ESC

[Ple75] Vera Pless. Encryption schemes for computer confidentially [sic]. MAC technical memorandum 63, Massachusetts Institute of Technology, Project MAC, Cambridge, MA, USA, 1975. 19 pp. Research done under ARPA Order no.2095, ONR Contract no. N00014-70-A-0362-0006 and IBM Contract 82280.

Pless:1977:ESC

[Ple77] Vera S. Pless. Encryption schemes for computer confidentiality. *IEEE Transactions on Computers*, C-26(11):1133–1136, 1977. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Plimmer:1998:MIW

[Pli98] Beryl Plimmer. Machines invented for WW II code breaking. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 30(4): 37–40, December 1998. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Plumstead:1982:ISG

[Plu82] Joan Boyar Plumstead. Inferring a sequence generated by a linear congruence. In IEEE [IEE82a], pages 153–159. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA76.6 .S95 1982. IEEE catalog no. 82CH1806-9. IEEE Computer Society order no. 440.

Plumstead:1983:ISP

[Plu83] Joan Boyar Plumstead. *Inferring Sequences Produced by Pseudo-Random Number Generators*. Ph.D. dissertation, Department of Computer Science, University of California, Berkeley, Berkeley, CA, USA, June 1983. ii + 56 pp.

Payne:1978:OEN

[PM78] W. H. Payne and K. L. McMillen. Orderly enumeration of nonsingular binary matrices applied to text encryption. *Communications of the Association for Computing Machin-*

ery, 21(4):259–263, April 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Pollard:1974:TFP

[Pol74] J. Pollard. Theorems on factorization and primality testing. *Proceedings of the Cambridge Philosophical Society. Mathematical and physical sciences*, 76:521–528, 1974. CODEN PCPSA4. ISSN 0008-1981.

Pollard:1978:MCM

[Pol78] J. M. Pollard. Monte Carlo methods for index computation (mod$p$). *Mathematics of Computation*, 32(143):918–924, July 1978. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Pomerance:1988:ACC

[Pom88] Carl Pomerance, editor. *Advances in cryptology — CRYPTO '87: proceedings*, volume 293 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988. CODEN LNCSD9. ISBN 0-387-18796-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1987; QA267.A1 L43 no.293. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0293.htm; http://www.springerlink.com/openurl.asp?genre=issue&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.

Ponting:1989:TCB

[Pon89] Bob Ponting. Three companies break Adobe encryption scheme. *InfoWorld*, 11(9):8, February 2, 1989. CODEN INWODU. ISSN 0199-6649. URL `https://books.google.com/books?id=IToEAAAAMBAJ&pg=PT7`.

Popentiu:1989:SRK

[Pop89] Fl. Popenţiu. A survey of recent knapsack cryptosystems. *Bul. Inst. Politehn. Bucureşti Ser. Electron.*, 51:83–90, 1989.

Porges:1952:MNC

[Por52] Arthur Porges. Mathematical notes: a continued fraction cipher. *American Mathematical Monthly*, 59(4):236, April 1952. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Porter:1984:CNS

[Por84] Sig Porter. Cryptology and number sequences: Pseudorandom, random, and perfectly random. *Computers and Security*, 3(1):43–44, February 1984. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404884900257`.

Posch:1989:AEA

[PP89] K. C. Posch and R. Posch. Approaching encryption at ISDN speed using partial parallel modulus multiplication. IIG report 276, Institutes for Information Processing Graz, Graz, Austria, November 1989. 9 pp.

Peleg:1979:BSC

[PR79] Shmuel Peleg and Azriel Rosenfeld. Breaking substitution ciphers using a relaxation algorithm. *Communications of the Association for Computing Machinery*, 22(11):598–605, November 1979. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Pieprzyk:1985:DPK

[PR85a] Józef P. Pieprzyk and Dominik A. Rutkowski. Design of public key cryptosystems using idempotent elements. *Computers and Security*, 4(4):297–308, December 1985. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404885900483`.

Pieprzyk:1985:MDI

[PR85b] Józef P. Pieprzyk and Dominik A. Rutkowski. Modular design of information encipherment for computer systems. *Computers and Security*, 4(3): 211–218, September 1985. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404885900306`.

Pratt:1939:SUS

[Pra39] Fletcher Pratt. *Secret and urgent: the story of codes and ciphers*. Robert Hale, London, UK, 1939. 282 pp. LCCN Z104 .P92 1939.

Pritchard:1980:DE

[Pri80] John Arthur Thomas (John A. T.) Pritchard. *Data encryption*. National Computing Centre, Manchester, UK, 1980. ISBN 0-85012-253-8. 126 (or 118??) pp. LCCN QA76.9.A25 P7.

Price:1983:ABR

[Pri83] W. L. Price. *Annotated bibliography of recent publications on data security and cryptography*, volume 35/83 of *NPL-DITC*. National Physical Laboratory, Teddington, Middlesex, UK, sixth edition, 1983. ii + 29 pp. LCCN Z103.A1 P74 1983a. Reprinted by permission of the Controller of Her Britannic Majesty's Stationery Office. "PB84-169168." Photocopy. Springfield, VA: National Technical Information Service, [1983?]. 28 cm.

Pronzini:1980:MCC

[Pro80] Bill Pronzini. *Mummy!: a chrestomathy of crypt-ology*. Arbor House, New York, NY, USA, 1980. ISBN 0-87795-271-X. xii + 273

pp. LCCN PN 6120.95 M77 M86 1980. US$10.95. Contents: Doyle, A.C. Lot no. 249.–Poe, E.A. Some words with a mummy.–Benson, E.F. Monkeys.–Wollheim, D.A. Bones.–Williams, T. The vengeance of Nitocris.–Gautier, T. The mummy's foot.–Bloch, R. The eyes of the mummy.–Powell, T. Charlie.–Hoch, E.D. The weekend magus.–Lansdale, J.R. The princess.–Mayhar, A. The eagle-claw rattle.–Grant, C.L. The other room.–Malzberg, B.N. Revelation in seven stages.–Bibliography.

Proctor:1985:SSC

[Pro85] Norman Proctor. A self-synchronizing cascaded cipher system with dynamic control of error propagation. In Blakley and Chaum [BC85], pages 174–190. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=174`. 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.

Pomerance:1988:PAF

[PST88] Carl Pomerance, J. W. Smith, and Randy Tuler. A pipeline architecture for factoring large integers with the quadratic sieve algorithm. *SIAM Journal on Computing*, 17(2):387–403, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Pomerance:1980:P

[PSW80] Carl Pomerance, J. L. Selfridge, and Samuel S. Wagstaff, Jr. The pseudoprimes to $25 \cdot 10^9$. *Mathematics of Computation*, 35(151):1003–1026, July 1980. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Press:1989:CRC

[PT89] William H. Press and Saul A. Teukolsky. Cyclic redundancy checks for data integrity or identity. *Computers in Physics*, 3(4):88–??, July 1989. CODEN CPHYE2. ISSN 0894-1866 (print), 1558-4208 (electronic). URL `https://aip.scitation.org/doi/10.1063/1.4822859`.

Purdy:1974:HSL

[Pur74] George B. Purdy. A high security log-in procedure. *Communications of the Association for Computing Machinery*, 17(8):442–445, August 1974. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

URL https://dl.acm.org/doi/10.1145/361082.361089.

Puteanus:1627:EPC

[Put27] Erycius Puteanus. *ErycI Puteani Cryptographia Tassiana, sive, Clandestina scripti*. Typis Cornelii Coenesteynii, Louvanii, 1627. 18 + 2 pp. LCCN Z103.5 .P88 1627.

Pluimakers:1986:ACS

[PvL86] G. M. J. Pluimakers and J. van Leeuwen. Authentication: a concise survey. *Computers and Security*, 5(3):243–250, September 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404886900155.

Pfitzmann:1986:NUO

[PW86a] A. Pfitzmann and M. Waidner. Networks without user observability — design options. In Pichler [Pic86], page ???? CODEN LNCSD9. ISBN 0-387-16468-5 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E961 1985. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1020.html. "The workshop was sponsored by International Association for Cryptologic Research ... [et al.]"–T.p. verso.

Power:1986:AHE

[PW86b] June M. Power and Steve R. Wilbur. Authentication in a heterogeneous environment. *Computers and Security*, 5 (2):167, June 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404886901458.

Pfitzmann:1987:NUO

[PW87a] Andreas Pfitzmann and Michael Waidner. Networks without user observability. *Computers and Security*, 6(2): 158–166, April 1987. CODEN CPSEDU. ISSN 0167-4048. URL http://www.semper.org/sirene/publ/PfWa_86anonyNetze.html.

Power:1987:AHE

[PW87b] June M. Power and Steve R. Wilbur. Authentication in a heterogeneous environment. *Computers and Security*, 6(1): 41–48, February 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404887901246.

Quisquater:1989:BHF

[QG89] J. J. Quisquater and M. Girault. $2n$-bit hash-functions using n-bit symmetric block cipher algorithms. In Quisquater and Vandewalle [QV89], page ?? ISBN 0-387-53433-4 (New York), 3-540-53433-4 (Berlin). LCCN QA76.9.A25 E964 1989. DM98.00.

Qin:1988:RSS

[QSA88] Bin Qin, Howard A. Sholl, and Reda A. Ammar. RTS: a system to simulate the real time cost behaviour of parallel computations. *Software—Practice and Experience*, 18(10):967–985, October 1988. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Quisquater:1989:ACE

[QV89] Jean-Jacques Quisquater and Joos Vandewalle, editors. *Advances in Cryptology–EUROCRYPT '89: Workshop on the Theory and Application of Cryptographic Techniques, Houthalen, Belgium, April 10–13, 1989: Proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1989. ISBN 0-387-53433-4 (New York), 3-540-53433-4 (Berlin). LCCN QA76.9.A25 E964 1989. DM98.00.

Rabin:1977:DS

[Rab77] M. O. Rabin. Digitalized signatures. In Richard A. DeMillo et al., editors, *Foundations of Secure Computation: Papers presented at a 3 day workshop held at Georgia Institute of Technology, Atlanta, October 1977*, pages x + 404. Academic Press, New York, NY, USA, 1977. ISBN 0-12-210350-5. LCCN QA76.9.A25 F66.

Rabin:1981:HES

[Rab81] Michael O. Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Aiken Computation Laboratory, Harvard University, Cambridge, MA, USA, 1981. URL `http://eprint.iacr.org/2005/187.pdf`.

Rabin:1989:EDI

[Rab89] Michael O. Rabin. Efficient dispersal of information for security, load balancing, and fault tolerance. *Journal of the Association for Computing Machinery*, 36(2):335–348, April 1989. CODEN JACOAH. ISSN 0004-5411. URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/62050.html`.

Rand:1955:MRD

[Ran55] Rand Corporation. *A Million Random Digits With 100,000 Normal Deviates*. Free Press, Glencoe, IL, USA, 1955. ISBN 0-02-925790-5. xxv + 400 + 200 pp. LCCN QA276.5 .R3. Reprinted in 1966 and 2001 [Ran01]. See also [Tip27].

Randell:1982:CGC

[Ran82a] Brian Randell. Colossus: Godfather of the computer (1977). In *The Origins of Digital Computers: Selected Papers* [Ran82b], pages 349–354. ISBN 0-387-11319-3, 3-540-11319-3. LCCN TK7885.A5 O741 1982.

Randell:1982:ODC

[Ran82b] Brian Randell, editor. *The Origins of Digital Computers: Selected Papers*. Texts and

monographs in computer science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., third edition, 1982. ISBN 0-387-11319-3, 3-540-11319-3. xvi + 580 pp. LCCN TK7885.A5 O741 1982.

Rand:2001:MRD

[Ran01] Rand Corporation. *A Million Random Digits With 100,000 Normal Deviates*. Rand Corporation, Santa Monica, CA, USA, 2001. ISBN 0-8330-3047-7. xxv + 400 + 200 pp. LCCN QA276.25 .M55 2001. See also [Ran55].

Rao:1984:JEE

[Rao84] T. R. N. Rao. Joint encryption and error correction schemes. *ACM SIGARCH Computer Architecture News*, 12(3):240–241, June 1984. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Rhodes-Burke:1982:RSA

[RB82] Robert Rhodes-Burke. Retrofitting for signature analysis simplified. *Hewlett-Packard Journal: technical information from the laboratories of Hewlett-Packard Company*, 33(1):9–16, January 1982. CODEN HPJOAX. ISSN 0018-1153.

Rabin:1989:VSS

[RBO89] T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In ACM [ACM89a], pages 73–85. ISBN 0-89791-326-4. LCCN QA 76.9 D5 A26 1989.

Reeds:1979:CMC

[Ree79] James Reeds. Cracking a multiplicative congruential encryption algorithm. In *Information linkage between applied mathematics and industry (Proc. First Annual Workshop, Naval Postgraduate School, Monterey, Calif., 1978)*, pages 467–472. Academic Press, New York, NY, USA, 1979.

Reischuk:1985:NSB

[Rei85] R. Reischuk. A new solution to the Byzantine generals problem. *Information and Control*, pages 23–42, 1985. CODEN IFCNA4. ISSN 0019-9958 (print), 1878-2981 (electronic).

Rejewski:1977:ATP

[Rej77] Marian Rejewski. An application of the theory of permutations in breaking the Enigma cipher. *Applications of Mathematicae, Polish Academy of Sciences*, 16(??):543–559, ???? 1977.

Rejewski:1981:HPM

[Rej81] Marian Rejewski. How Polish mathematicians deciphered the Enigma. *Annals of the History of Computing*, 3(3):213–234, July/September 1981. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1981/pdf/a3213.pdf; http://www.computer.org/annals/an1981/a3213abs.htm`. Afterwords by Cipher

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

Rejewski:19xx:EMH

[Rejxx] Marian Rejewski. Enigma (1930–40). method and history of solving the German machine cipher. Unpublished manuscript in Polish, 19xx.

Rowlett:1935:FAP

[RF35] Frank B. Rowlett and William F. Friedman. *Further applications of the principles of indirect symmetry of position in secondary alphabets: technical paper*. United States Government Printing Office, Washington, DC, USA, 1935. ???? pp.

Richards:1974:SWP

[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.

Rihaczek:1987:T

[Rih87] Karl Rihaczek. Teletrust. *Computer Networks and ISDN Systems*, 13(3):235–239, 1987. CODEN CNISE9. ISSN 0169-7552.

Ritchie:19xx:DCW

[Ritxx] Dennis M. Ritchie. Dabbling in the cryptographic world — A story. This undated note describes the interesting history behind the non-publication of a paper [RRM78] on the Hagelin cypher machine (M-209), submitted to the journal Cryptologia, because of shadowy suggestions of a "retired gentleman from Virginia"., 19xx. URL `http://www.cs.bell-labs.com/~dmr/crypt.html`.

Rivest:1974:HCA

[Riv74a] R. L. Rivest. On hash-coding algorithms for partial-match retrieval. In IEEE [IEE74], pages 95–103.

Rivest:1974:AAR

[Riv74b] Ronald L. Rivest. Analysis of associative retrieval algorithms. Technical Report TR.54, Institut de la Recherche en Informatique et Automatique, now Institut National de Recherche en Informatique et Automatique (INRIA), Domaine de Voluceau — Rocquencourt — B.P. 105, 78153 Le Chesnay Cedex, France, February 1974. ?? pp. Also published in/as: Stanford CSD report 74-415. Also published

in/as: SIAM Journal for Computing, Springer-Verlag (Heidelberg, FRG and New York NY, USA)-Verlag, 1976, with mod. title.

Rivest:1979:CRC

[Riv79] Ronald L. Rivest. Critical remarks on: "Critical remarks on some public-key cryptosystems" [BIT **18**(4), 1978, pp. 493–496; MR 80b:94033] by Tore Herlestam. *BIT*, 19(2): 274–275, June 1979. CODEN NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=19&issue=2&spage=274`. See [Her78].

Rivest:1980:DSC

[Riv80] R. L. Rivest. A description of a single-chip implementation of the RSA cipher. *Lambda: the magazine of VLSI design*, 1 (3):14–18, Fourth Quarter 1980. CODEN VDESDP. ISSN 0273-8414.

Rivest:1985:RCP

[Riv85] Ronald L. Rivest. RSA chips (past/present/future). In Beth et al. [BCI85], pages 159–163. CODEN LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). 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.

Rivest:1987:EDR

[Riv87] Ronald L. Rivest. The eary days of RSA: History and lessons. In Ashenhurst [Ash87], page ?? ISBN 0-201-07794-9. LCCN QA76.24 .A33 1987. ACM Turing Award lecture.

Reeds:1985:NPR

[RM85] J. A. Reeds and J. L. Manferdelli. DES has no per round linear factors. In Blakley and Chaum [BC85], pages 377–389. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=377`. 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.

Rao:1987:PKA

[RN87] T. R. N. Rao and Kil-Hyun Nam. Private-key algebraic-coded cryptosystems. *Lecture Notes in Computer Science*, 263:35–48, 1987. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rao:1989:PKA

[RN89] T. R. N. Rao and Kil-Hyun Nam. Private-key algebraic-code encryptions. *IEEE Transactions on Information Theory*, IT-35(4):829–833, 1989. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Rohwer:1975:GIM

[Roh75] Jurgen Rohwer. *Geleitzugschlachten im Marz 1943: Führungsprobleme im Höhepunkt der Schlacht im Atlantik. (German) [Convoy in March 1943: implementation problems in the climax of the Battle of the Atlantic].* Motorbuch, Stuttgart, Germany, 1975. ISBN 3-87943-383-6. 356 pp. LCCN ???? See also English translation [Roh77].

Rohwer:1977:CCB

[Roh77] Jürgen Rohwer. *The critical convoy battles of March 1943: the battle for HX.229/SC122.* Naval Institute Press, Annapolis, MD, USA, 1977. ISBN 0-87021-818-2. 256 + 32 pp. LCCN D770 .R59313. Revised English translation by Derek Masters of the German original [Roh75].

Routh:1984:PAA

[Rou84] Richard LeRoy Routh. A proposal for an architectural approach which apparently solves all known software-based internal computer security problems. *Operating Systems Review*, 18 (3):31–39, July 1984. CODEN OSRED8. ISSN 0163-5980.

Roy:1986:CBI

[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.).

Ringeisen:1986:ADM

[RR86] Richard D. Ringeisen and Fred S. Roberts, editors. *Applications of discrete mathematics. Proceedings of the Third SIAM Conference on Discrete Mathematics held at Clemson University, Clemson, South Carolina, May 14–16, 1986.* Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1986. ISBN 0-89871-219-X. LCCN QA76.9.M35C65 1986.

Reeds:1978:HCM

[RRM78] J. Reeds, D. Ritchie, and R. Morris. The Hagelin cypher machine (M-209): Cryptanalysis from ciphertext alone. Submitted to the journal Cryptologia, but never published. For the story behind the suppression of publication, see [Ritxx]. Internal technical memoranda TM 78-1271-10, TM 78-1273-2., 1978.

Rivest:1983:RET

[RS83] Ronald L. Rivest and Alan T. Sherman. Randomized encryption techniques. Technical report MIT/LCS/TM-234, Massachusetts Institute of Technol-

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

Rivest:1984:HEE

[RS84] Ronald L. Rivest and Adi Shamir. How to expose an eavesdropper. *Communications of the Association for Computing Machinery*, 27(4):393–395, April 1984. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Rivest:1978:MOD

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the Association for Computing Machinery*, 21(2):120–126, February 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). The basics of trap-door functions and the famous RSA public key cryptosystem are presented in this paper.

Rivest:1982:MOD

[RSA82] Ronald Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public key cryptosystems. In *Secure communications and asymmetric cryptosystems*, volume 69 of *AAAS Sel. Sympos. Ser.*, pages 217–239. Westview, Boulder, CO, 1982.

Rivest:1983:MOD

[RSA83] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the Association for Computing Machinery*, 26 (1):96–99, January 1983. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Reif:1988:EPP

[RT88] J. H. Reif and J. D. Tygar. Efficient parallel pseudorandom number generation. *SIAM Journal on Computing*, 17(2):404–411, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Raleigh:1988:CDP

[RU88] T. M. Raleigh and R. W. Underwood. CRACK: a distributed password advisor. In USENIX [USE88a], pages 12–13. LCCN QA76.8.U65 U55 1988(1)-1990(2)//. Abstract only.

Rubin:1979:DSC

[Rub79] F. Rubin. Decrypting a stream cipher based on J–K flip-flops. *IEEE Transactions on Computers*, C-28(7):483–487, July 1979. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1675392`.

Rudolph:1982:HTI

[Rud82] James G. Rudolph, editor. *High technology in the information industry: digest of papers/Compcon spring 82, February 22–25; twenty-fourth IEEE computer society international conference, Jack Tar Hotel, San Francisco, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1982. ISBN ???? LCCN TK7885.A1 C53 1982. IEEE catalog number 82CH1739-2.

Ruggiu:1985:CCT

[Rug85] G. Ruggiu. Cryptology and complexity theories. In Beth et al. [BCI85], pages 3–9. CODEN LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). 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.

Russell:1927:CMS

[Rus27] Henry Norris Russell. Cipher messages of the stars. *Scientific American*, 137(2): 118–119, August 1927. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL `http://www.nature.com/scientificamerican/journal/v137/n2/pdf/scientificamerican0827-118.pdf`.

Reeds:1984:FSU

[RW84] James A. Reeds and Peter J. Weinberger. File security and the UNIX system `crypt` command. *ATT Bell Lab. tech. j*, 63(8 part 2):1673–1683, October 1984. CODEN ABLJER. ISSN 0748-612X (print), 2376-7162 (electronic). Reprinted in [AT&T86, pp. 93–103].

Rytter:1986:SCU

[Ryt86] Wojciech Rytter. The space complexity of the unique decipherability problem. *Information Processing Letters*, 23(1):1–3, July 20, 1986. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

S:1873:COD

[S.73] H. S. *Cryptographie, ou, Divers systèmes d'écrire secrète spécialement pour l'usage des cartes postales: combinations alphabétiques, correspondance chiffrée, écriture par signes: divers procédés pour la fabrication d'encres sympathiques*. G. Jousset, Paris, France, 1873. 8 pp. LCCN Z104 .H16 1873.

Sacco:1936:MC

[Sac36] Luigi Sacco. *Manuale di crittografia. (Italian) [Manual of cryptography]*. Tipografia Santa Barbara, Roma, Italia, second edition, 1936. viii + 247 + 8 pp.

Sacco:1947:MC

[Sac47] Luigi Sacco. *Manuale di crittografia. (Italian) [Manual of cryptography]*. Istituto Poligrafico Dello Stato, Roma, Italia, third edition, 1947. xii + 374 pp.

Sacco:1951:MCF

[Sac51] Luigi Sacco. *Manuel de cryptographie. (French) [Manual of cryptography]*. Payot, Paris, France, 1951. ???? pp.

Sacco:1977:MC

[Sac77] Luigi Sacco. *Manual of cryptography*, volume 14 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1977. ISBN 0-89412-016-6. x + 193 pp. LCCN Z104 .S313 1977. Translation of: Manuale di crittografia. Bibliography: p. viii.

Saks:1989:RNP

[Sak89] Michael Saks. A robust noncryptographic protocol for collective coin flipping. *SIAM Journal on Discrete Mathematics*, 2(2):240–244, May 1989. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Saltzer:1973:PCI

[Sal73] Jerome H. Saltzer. Protection and control of information sharing in Multics. *Operating Systems Review*, 7(4):119, October 1973. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Saltzer:1978:DS

[Sal78] Jerome H. Saltzer. On digital signatures. *Operating Systems Review*, 12(2):12–14, April 1978. CODEN OSRED8. ISSN 0163-5980.

Salomaa:1985:PKC

[Sal85] Arto Salomaa. On a public-key cryptosystem based on parallel rewriting. In *Parcella '84 (Berlin, 1984)*, volume 25 of *Math. Res.*, pages 209–214. Akademie-Verlag, Berlin, 1985.

Salomaa:1988:PKC

[Sal88] Arto Salomaa. A public-key cryptosystem based on language theory. *Computers and Security*, 7(1):83–87, February 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/016740488890507X`.

Sansom:1986:BRC

[San86] Robert Sansom. Book review: *Computer Security: A Global Challenge — Proceedings of the Second IFIP International Conference on Computer Security, IFIP/Sec'84, Toronto, Ontario, Canada, 10–12 September, 1984*: (Elsevier Science Publishing Co. 1984). *Operating Systems Review*, 20(3):9, July 1986. CODEN OSRED8. ISSN 0163-5980.

Sandhu:1988:CIT

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

tree hierarchy for access control. *Information Processing Letters*, 27(2):95–98, February 29, 1988. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Sarton:1928:BRBn

[Sar28] George Sarton. Book review: *The Cipher of Roger Bacon* by William Romaine Newbold; Roland Grubb Kent. *Isis*, 11(1): 141–145, September 1928. CODEN ISISA4. ISSN 0021-1753 (print), 1545-6994 (electronic). URL `http://www.jstor.org/stable/224770`.

Satyanarayanan:1989:ISL

[Sat89] M. Satyanarayanan. Integrating security in a large distributed system. *ACM Transactions on Computer Systems*, 7 (3):247–280, August 1989. CODEN ACSYEC. ISSN 0734-2071. URL `http://www.acm.org:80/pubs/citations/journals/tocs/1989-7-3/p247-satyanarayanan/`.

Saunders:1989:IDE

[Sau89] Barry Ferguson Saunders. Insection and decryption: Edgar Poe's *The gold bug* and the diagnostic gaze. Thesis (M.A.), University of North Carolina at Chapel Hill, Chapel Hill, NC, USA, 1989. x + 116 pp.

Sawirudin:1955:PND

[Saw55] Sawirudin. *Pegawai negeri dan PGP baru*. Badan Penerbitan Dewan Nasional SOBSI, Djakarta, cet. 1. edition, 1955. 93 pp.

Schaumuller-Bichl:1982:ADE

[SB82] Ingrid Schaumuller-Bichl. *Zur Analyse des Data Encryption: Standard und Synthese verwandter Chiffriersysteme*. PhD thesis, Johannes Kepler-Universität Linz, Linz, Austria, 1982. 168 pp. Summary in English. Published by VWGO, Wien, Austria.

Sorkin:1984:MCC

[SB84] Arthur Sorkin and C. James Buchanan. Measurement of cryptographic capability protection algorithms. *Computers and Security*, 3(2): 101–116, May 1984. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/016740488490052X`.

Serpell:1985:PES

[SBC85] S. C. Serpell, C. B. Brookson, and B. L. Clark. A prototype encryption system using public key. In Blakley and Chaum [BC85], pages 3–9. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=3`. 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.

Smillie:1985:RFM

[SBET85] K. W. Smillie, F. L. Bauer, Ralph Erskine, and Henry S. Tropp. Reviews: O. I. Franksen, Mr. Babbage's Secret; F. H. Hinsley, British Intelligence in the Second World War; T. M. Thompson, From Error-Correcting Codes Through Sphere Packings to Simple Groups; capsule reviews. *Annals of the History of Computing*, 7(2):185–191, April/June 1985. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1985/pdf/a2185.pdf; http://www.computer.org/annals/an1985/a2185abs.htm`.

Chen:1985:RGE

[sC85] Su shing Chen. On rotation group and encryption of analog signals. In Blakley and Chaum [BC85], pages 95–100. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=95`. 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.

Scacchitti:1986:CT

[Sca86] Fred A. Scacchitti. The cryptographer's toolbox. *Dr. Dobb's Journal of Software Tools*, 11 (5):58–??, May 1986. CODEN DDJOEB. ISSN 1044-789X.

Schwenter:1620:SSN

[Sch20] Daniel Schwenter. *Steganologia & steganographia nova: Geheime magische, naturliche Red vnd Schreibkunst, einem in der nahe vnd ferrne Alsbalden oder in gewiser Zeit, so woln in Schimpff als Ernst, etwas verborgens vnnd geheimes zu eroffnen durch Reden, Schreiben vnd mancherley Instrumenta: item wie verborgene Schrifften zu machen, auffzulosen, vnd mit sonderlichen Kunsten zu schreiben.* Resene Gibronte Runeclus Hanedi, Nürnberg, Germany, 1620. 16 + 299 + 5 pp. LCCN KK276 .E36 1575; Z103.5. Publication year uncertain. Publicirt vnd an Tag gegeben durch Resene Gibronte Runeclus Hanedi ... Nurnberg: Inn Verlegung Simon Halbmayers.

Schwenter:1633:SSA

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

Red vnnd Schreibkunst. Resene Gibronte Runeclusam Hunidem, Nürnberg, Germany, 1633. 24 + 370 pp. LCCN Z103 .S38 1633. Auffs neue revidirt, an etlichen Orten corrigirt, ... augirt, vnd dann zum drittenmal in Truck verfertiget durch Janum Herculem de Sunde, sonst Resene Gibronte Runeclusam Hunidem .... Nurnberg, In Verlegung Jeremiae Dumlers [between 1633 and 1636].

Schroeder:1969:IC

[Sch69] M. R. Schroeder. Images from computers. *IEEE Spectrum*, 6 (3):66–78, March 1969. CODEN IEESAM. ISSN 1939-9340.

Schroeder:1975:ESK

[Sch75] Michael D. Schroeder. Engineering a security kernel for Multics. *Operating Systems Review*, 9(5):25–32, November 1975. CODEN OSRED8. ISSN 0163-5980.

Schell:1983:SPA

[Sch83] K. J. Schell. Security printers application of lasers. *Proceedings of SPIE — The International Society for Optical Engineering*, 396:131–140, 1983. CODEN PSISDG. ISBN 0-89252-431-6. ISSN 0277-786X (print), 1996-756X (electronic).

Schroeder:1984:NTS

[Sch84] M. R. (Manfred Robert) Schroeder. *Number theory in science and communication: with applications in cryptography, physics, biology, digital information, and computing*, volume 7 of *Springer series in information sciences*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1984. ISBN 0-387-12164-1. xvi + 324 pp. LCCN QA241 .S318 1984.

Schroeder:1986:NTS

[Sch86] M. R. (Manfred Robert) Schroeder. *Number theory in science and communication: with applications in cryptography, physics, digital information, computing, and self-similarity*, volume 7 of *Springer series in information sciences*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second enlarged edition, 1986. ISBN 0-387-15800-6. xix + 374 pp. LCCN QA241 .S3181 1986.

Smith:1986:GCC

[SD86] G. W. Smith and J. B. H. Du Boulay. The generation of cryptic crossword clues. *The Computer Journal*, 29(3):282–284, June 1986. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Sicherman:1983:AQR

[SDV83] George L. Sicherman, Wiebren De Jonge, and Reind P. Van De Riet. Answering queries without revealing secrets. *ACM Transactions on Database Systems*, 8(1):41–59, March 1983. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://`

www.acm.org/pubs/articles/journals/tods/1983-8-1/p41-sicherman/p41-sicherman.pdf; http://www.acm.org/pubs/citations/journals/tods/1983-8-1/p41-sicherman/. Also published in/as: reprinted in deJonge thesis, Jun. 1985.

Smillie:1986:RWA

[SE86] K. W. Smillie and Ralph Erskine. Reviews: W. Aspray, Should the Term Fifth Generation Computers Be Banned?; C. A. Deavours and L. Kruh, Machine Cryptography and Modern Cryptanalysis; capsule reviews. *Annals of the History of Computing*, 8(2):199–200, 202, 204–205, April/June 1986. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1986/pdf/a2199.pdf; http://www.computer.org/annals/an1986/a2199abs.htm.

Seaton:1956:THS

[Sea56] E. Seaton. Thomas Hariot's secret script. *Ambix: Journal of the Society for the History of Alchemy and Chemistry*, 5(3–4):111–114, 1956. CODEN AMBXAO. ISSN 0002-6980 (print), 1745-8234 (electronic). URL http://www.tandfonline.com/doi/abs/10.1179/amb.1956.5.3-4.111.

Sears:1986:SWK

[Sea86] Peter Sears. *Secret writing: keys to the mysteries of reading and writing*. Teachers and Writers Collaborative, New York, NY, USA, 1986. ISBN 0-915924-86-2 (paperback). xv + 160 pp. LCCN Z 103.3 S4 1986 Resources for Teaching–2nd Floor. US$9.95. Discusses secret writing, ciphers, and the processes of creating and deciphering secret or difficult languages. Includes thinking and writing exercises.

Sedlak:1988:RCP

[Sed88] H. Sedlak. The RSA cryptographic processor: The first high speed one-chip solution. In Pomerance [Pom88], pages 95–105. CODEN LNCSD9. ISBN 0-387-18796-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1987; QA267.A1 L43 no.293. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0293.htm; http://www.springerlink.com/openurl.asp?genre=issue&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.

Seeley:1989:PCG

[See89] Donn Seeley. Password cracking: a game of wits. *Communications of the Association for Computing Machinery*, 32(6):700–703, June 1989. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/63529.html.

Serpell:1985:CES

[Ser85] S. C. Serpell. *Cryptographic equipment security: a code of practice*. Institution of Electronic and Radio Engineers, London, UK, 1985. ISBN 0-903748-62-2 (paperback). 25 pp. LCCN Z103.S47 1985.

Seshadri:1981:KPP

[Ses81] Raghavan Seshadri. Knapsack problems in public key encryption systems. Thesis (M.S.), University of Oklahoma, Norman, OK, USA, 1981. vii + 99 pp.

Shannon:1945:MTC

[Sha45] Claude Shannon. A mathematical theory of cryptography. Classified report, Bell Laboratories, Murray Hill, NJ, USA, September 1, 1945.

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

[Sha48b] Claude Shannon. A mathematical theory of communication (continued). *The Bell System Technical Journal*, 27(4): 623–656, October 1948. CODEN BSTJAN. ISSN 0005-8580.

Shannon:1949:CTS

[Sha49] Claude Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, ???? 1949. CODEN BSTJAN. ISSN 0005-8580. URL http://en.wikipedia.org/wiki/Communication_Theory_of_Secrecy_Systems; http://www.cs.ucla.edu/~jkong/research/security/shannon1949.pdf. A footnote on the initial page says: "The material in this paper appeared in a confidential report, 'A Mathematical Theory of Cryptography', dated Sept. 1, 1946, which has now been declassified.".

Shamir:1979:HSS

[Sha79] Adi Shamir. How to share a secret. *Communications of the Association for Computing Machinery*, 22(11):612–613, November 1979. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Shamir:1982:PTA

[Sha82] Adi Shamir. A polynomial time algorithm for breaking the basic Merkle–Hellman cryptosystem. In *23rd annual symposium*

on foundations of computer science (Chicago, Ill., 1982), pages 145–152. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1982.

Shamir:1983:ECT

[Sha83a] Adi Shamir. Embedding cryptographic trapdoors in arbitrary knapsack systems. *Information Processing Letters*, 17(2):77–79, August 24, 1983. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Shamir:1983:GCS

[Sha83b] Adi Shamir. On the generation of cryptographically strong pseudorandom sequences. *ACM Transactions on Computer Systems*, 1(1):38–44, February 1983. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

Shamir:1984:PTA

[Sha84] Adi Shamir. A polynomial-time algorithm for breaking the basic Merkle–Hellman cryptosystem. *IEEE Transactions on Information Theory*, 30(5):699–704, 1984. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Shamir:1985:IBC

[Sha85] Adi Shamir. Identity-based cryptosystems and signature schemes. In Blakley and Chaum [BC85], pages 47–53. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=47`. 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.

Shamir:1986:SPS

[Sha86] A. Shamir. The search for provably secure identification schemes. In Gleason [Gle87], pages 1488–1495. ISBN 0-8218-0110-4. LCCN QA1 .I8 1986 v. 1-2. Two volumes.

Shamir:1987:CSS

[Sha87] Adi Shamir. Cryptography: State of the science. In Ashenhurst [Ash87], page ?? ISBN 0-201-07794-9. LCCN QA76.24 .A33 1987. ACM Turing Award lecture.

Sharp:1988:DCO

[Sha88] R. L. Sharp. Design of a certifiable one-way data-flow device. *AT&T Technical Journal*, 67(3):44–52, May 1988. CODEN ATJOEM. ISSN 2376-676X (print), 8756-2324 (electronic).

Sherman:1986:CVT

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

tion). I, II, Detecting and exploiting algebraic weaknesses in cryptosystems. Algorithms for placing modules on a custom VLSI chip. Thesis (Ph.D.), Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA, October 1986. 221 pp. Supervised by Ronald Linn Rivest.

Sherman:1987:CVT

[She87] Alan T. Sherman. *Cryptology and VLSI (a two-part dissertation). I, II, Detecting and exploiting algebraic weaknesses in cryptosystems. Algorithms for placing modules on a custom VLSI chip*. Thesis (Ph.D.), Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA, 1987. 221 pp. Supervised by Ronald Linn Rivest.

Sherman:1988:CVV

[She88] A. T. Sherman. Cryptology and VLSI (Very Large Scale Integration). I. Detecting and exploiting algebraic weaknesses in cryptosystems. II. Algorithms for placing modules on a custom VLSI chip. *Computers and Security*, 7(5):512, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888902234`.

Shulman:1976:ABC

[Shu76] David Shulman. *An annotated bibliography of cryptography*, volume 37 of *Garland reference library of the humanities*. Garland Pub., New York, NY, USA, 1976. ISBN 0-8240-9974-5. 388 pp. LCCN Z103.A1 S58.

Shulman:1980:BRB

[Shu80a] David Shulman. Book review: *United States diplomatic codes and ciphers 1775–1938*: By Ralph E. Weber. Chicago. xviii + 633 pp. Illus. $49.95. *Historia Mathematica*, 7(4):452–454, November 1980. CODEN HIMADS. ISSN 0315-0860 (print), 1090-249X (electronic). URL `http://www.sciencedirect.com/science/article/pii/0315086080900142`.

Shulman:1980:BRU

[Shu80b] David Shulman. Book review: *United States diplomatic codes and ciphers 1775–1938*: By Ralph E. Weber. Chicago. xviii + 633 pp. Illus. $49.95. *Historia Mathematica*, 7(4):452–454, November 1980. CODEN HIMADS. ISSN 0315-0860 (print), 1090-249X (electronic). URL `http://www.sciencedirect.com/science/article/pii/0315086080900142`.

Shumaker:1982:RCJ

[Shu82] 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*

and studies. Center for Medieval and Early Renaissance Studies, Binghamton, NY, USA, 1982. ISBN 0-86698-014-8. 207 pp. LCCN CB361 .S494 1982. Intended audience: Renaissance specialists, linguistics, students of occultism, and historians of science.

Sidhu:1981:APG

[Sid81] Deepinder P. Sidhu. Authentication protocols for general communication channels. In IEEE [IEE81], pages 30–40. CODEN CLCPDN. LCCN TK 5105.5 C66 1981. IEEE catalog no. 81CH1690-7.

Sieminski:1983:SBB

[Sie83] Gregory C. Sieminski. The search for a balance between scientific freedom and national security: a case study of cryptology. Thesis (M.S.), Defense Intelligence College, Washington, DC, USA, November 1983. v + 73 pp.

Siegenthaler:1984:CIN

[Sie84] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776–780, 1984. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Siegenthaler:1985:DCS

[Sie85] T. Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *IEEE Transactions on Computers*, C34:81–85, 1985. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). This paper breaks the cipher of [Gef73].

Silverman:1983:RVS

[Sil83] Jonathan M. Silverman. Reflections on the verification of the security of an operating system kernel. *Operating Systems Review*, 17(5):143–154, October 1983. CODEN OSRED8. ISSN 0163-5980.

Silverman:1987:MPQ

[Sil87] Robert D. Silverman. The multiple polynomial quadratic sieve. *Mathematics of Computation*, 48(177):329–339, January 1987. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Simonetta:1404:LTC

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

Simmons:1979:HID

[Sim79a] G. J. Simmons. How to insure that data acquired to verify treaty compliance are trustworthy. In IEEE, editor, *IEEE EASCON '79, Washington, DC, 1979*, pages 661–662. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1979. ISBN ???? LCCN ????

Simmons:1979:CCA

[Sim79b] Gustavus J. Simmons. Computational complexity and asym-

metric encryption. In *Proceedings of the Eighth Manitoba Conference on Numerical Mathematics and Computing (Univ. Manitoba, Winnipeg, Man., 1978)*, Congress. Numer., XXII, pages 65–93. Utilitas Mathematica Publishers, Winnipeg, Manitoba, Canada, 1979.

Simmons:1979:SAE

[Sim79c] Gustavus J. Simmons. Symmetric and asymmetric encryption. *ACM Computing Surveys*, 11(4):305–330, December 1979. CODEN CMSVAN. ISSN 0010-4892.

Simmons:1982:SCA

[Sim82a] Gustavus J. Simmons, editor. *Secure communications and asymmetric cryptosystems*, volume 69 of *AAAS Selected Symposia Series*. Westview Press, Boulder, CO, 1982. ISBN 0-86531-338-5. x + 338 pp.

Simmons:1982:SAE

[Sim82b] Gustavus J. Simmons. Symmetric and asymmetric encryption. In *Secure communications and asymmetric cryptosystems*, volume 69 of *AAAS Sel. Sympos. Ser.*, pages 241–298. Westview Press, Boulder, CO, USA, 1982.

Simmons:1983:PPS

[Sim83] G. J. Simmons. The prisoners' problem and the subliminal channel. In Chaum et al. [CRS83], pages 51–67. ISBN 1-4757-0604-9 (print), 1-4757-0602-2. LCCN QA76.9.A25 C79 1982. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1001.html`.

Simmons:1984:HID

[Sim84] G. J. Simmons. How to insure that data acquired to verify treaty compliance are trustworthy. *Proceedings of the IEEE*, 76(5):621–627, May 1984. CODEN IEEPAD. ISSN 0018-9219. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1003.html`.

Simmons:1985:ATC

[Sim85a] Gustavus J. Simmons. Authentication theory/coding theory. In Blakley and Chaum [BC85], pages 411–431. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=411`. 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.

Simmons:1985:SCD

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

[BCI85], pages 364–378. CODEN LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E951 1984. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1002.html`. Held at the University of Paris, Sorbonne.

Simmons:1988:SSC

[Sim88] G. J. Simmons. *Special section on cryptology*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. 533–627 pp.

Sinkov:1966:ECM

[Sin66] Abraham Sinkov. *Elementary cryptanalysis: a mathematical approach*, volume 22 of *New mathematical library*. Mathematical Association of America, Washington, DC, USA, 1966. ISBN 0-88385-622-0. ix + 222 pp. LCCN Z 104 S47 1980. With a supplement by Paul L. Irwin. Reissued in 1975 and 1980.

Sinkov:1968:ECMa

[Sin68a] Abraham Sinkov. *Elementary cryptanalysis: a mathematical approach*, volume 22 of *New mathematical library*. Random House, New York, NY, USA, 1968. ix + 189 pp. LCCN QA11 .N5 v.22.

Sinkov:1968:ECMb

[Sin68b] Abraham Sinkov. *Elementary cryptanalysis: a mathematical approach*, volume 22 of *New mathematical library*. Mathematical Association of America, Washington, DC, USA, 1968. ix + 222 pp.

Sinnott:1977:CTC

[Sin77] Robert Sinnott. *A catalogue of titles on chess, checkers, and cryptology in the library of the United States Military Academy, West Point, New York*. ????, Norwell, MA, USA, 1977. 35 pp.

Singh:1985:IPS

[Sin85] Kamaljit Singh. On improvements to password security. *Operating Systems Review*, 19(1): 53–60, January 1985. CODEN OSRED8. ISSN 0163-5980.

Sambur:1976:SEM

[SJ76] M. R. Sambur and N. S. Jayant. Speech encryption by manipulations of LPC parameters. *The Bell System Technical Journal*, 55(9):1373–1388, November 1976. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol55/bstj55-9-1373.pdf`.

Schneier:1997:RAS

[SK97] Bruce Schneier and John Kelsey. Remote auditing of software outputs using a trusted coprocessor. *Future Generation Computer Systems*, 13(1): 9–18, June 20, 1997. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.counterpane.com/remote_auditing.`

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

Schobi:1983:FAT

[SM83] P. Schöbi and J. L. Massey. Fast authentication in a trapdoor-knapsack public key cryptosystem. *Lecture Notes in Computer Science*, 149:289–306, 1983. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Smith:1943:CSS

[Smi43] Laurence Dwight Smith. *Cryptography, the science of secret writing*. W. W. Norton & Co., New York, NY, USA, 1943. 164 pp. LCCN Z104 .S5.

Smith:1944:CSS

[Smi44] Laurence Dwight Smith. *Cryptography: the science of secret writing*. G. Allen and Unwin, London, UK, 1944. 164 pp. LCCN Z104.S5.

Smith:1955:CSS

[Smi55] Laurence Dwight Smith. *Cryptography; the science of secret writing*. Dover Publications, Inc., New York, NY, USA, 1955. 164 pp. LCCN Z104 .S6. "An unabridged republication of the first edition with corrections.".

Smith:1971:DLC

[Smi71a] J. L. Smith. The design of Lucifer, a cryptographic device for data communications. Research Report RC-3326, IBM T. J. Watson Research Center, Yorktown Heights, NY, USA, 1971.

Smith:1971:CSS

[Smi71b] Laurence Dwight Smith. *Cryptography, the science of secret writing*. Dover Publications, Inc., New York, NY, USA, 1971. ISBN 0-486-20247-X. 164 pp. LCCN Z 104 S65c 1971. "This Dover edition, first published in 1955, is an unabridged and corrected republication of the work originally published by W. W. Norton and Company in 1943." "Copyright renewed 1971." Bibliography: p. 156.

Smith:1974:RBC

[Smi74] J. L. Smith. Recirculating block cipher cryptographic system. U.S. Patent No. 3,796,830, March 12, 1974.

Smith:1983:PKC

[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.

Smith:1987:AUW

[Smi87] Sidney L. Smith. Authenticating users by word association. *Computers and Security*, 6(6): 464–470, December 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.

sciencedirect.com/science/article/pii/0167404887900277.

Smith:1972:EAC

[SNO72] J. L. Smith, W. A. Notz, and P. R. Osseck. An experimental application of cryptography to a remotely accessed data system. *Proceedings of the ACM 1972 Annual Conference*, ??(??):282–297, ???? 1972.

Steiner:1988:KAS

[SNS88] Jennifer G. Steiner, Clifford Neuman, and Jeffrey I. Schiller. Kerberos: An authentication service for open network systems. In USENIX Association [USE88c], pages 191–202. ISBN ???? LCCN ????

Snyder:1979:IUC

[Sny79] Samuel S. Snyder. Influence of U.S. Cryptologic Organizations on the digital computer industry. *The Journal of Systems and Software*, 1(1):87–102, ???? 1979. CODEN JSSODM. ISSN 0164-1212.

Snyder:1980:CAP

[Sny80] Samuel S. Snyder. Computer advances pioneered by cryptologic organizations. *Annals of the History of Computing*, 2(1):60–70, January/March 1980. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1980/pdf/a1060.pdf; http://www.computer.org/annals/an1980/a1060abs.htm.

Sorkis:1980:USM

[Sor80] Michael Sorkis. Use of statistically matched codes in a data encryption system. Thesis (M.S.), Southern Illinois University at Carbondale, Carbondale, IL, USA, 1980. v + 91 pp.

Smith:1979:UFM

[SP79] Donald R. Smith and James T. Palmer. Universal fixed messages and the Rivest–Shamir–Adleman cryptosystem. *Mathematika*, 26(1):44–52, 1979. CODEN MTKAAB. ISSN 0025-5793.

Seberry:1989:CIC

[SP89] Jennifer Seberry and Josef Pieprzyk. *Cryptography: an introduction to computer security*. Prentice Hall advances in computer science series. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 1989. ISBN 0-13-194986-1. viii + 375 pp. LCCN QA76.9.A25 S371 1989.

Spender:1987:ICU

[Spe87] J-C. Spender. Identifying computer users with authentication devices (tokens). *Computers and Security*, 6(5):385–395, October 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404887900113.

Saltzer:1984:EEA

[SRC84] J. H. Saltzer, D. P. Reed, and D. D. Clark. End-to-end argu-

ments in system design. *ACM Transactions on Computer Systems*, 2(4):277–288, November 1984. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

Shamir:1984:CCV

[SS84] A. Shamir and C. P. Schnorr. Cryptanalysis of certain variants of Rabin's signature scheme. *Information Processing Letters*, 19(3):113–115, October 19, 1984. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Siromoney:1986:PKC

[SS86] Rani Siromoney and Gift Siromoney. A public key cryptosystem that defies cryptanalysis. In *Workshop on Mathematics of Computer Algorithms (Madras, 1986)*, volume 111 of *IMS Rep.*, pages D.3.17, 4. Inst. Math. Sci., Madras, 1986.

Shepherd:1989:CSS

[SS89] S. J. Shepherd and P. W. Sanders. A comprehensive security service - functional specification. Ibm internal document, IBM (United Kingdom Laboratories), Hursley Park, Winchester, UK, May 1989.

Subramanian:1987:DTP

[SSA87] K. G. Subramanian, Rani Siromoney, and P. Jeyanthi Abisha. A D0L-T0L public key cryptosystem. *Information Processing Letters*, 26(2):95–97, October 19, 1987. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Siromoney:1988:CPL

[SSA88] R. Siromoney, K. G. Subramanian, and Jeyanthi Abisha. Cryptosystems for picture languages. In *Syntactic and structural pattern recognition (Barcelona and Sitges, 1986)*, volume 45 of *NATO Adv. Sci. Inst. Ser. F Comput. Systems Sci.*, pages 315–332. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988.

Smith:1981:VEP

[SSDG81] Michael K. Smith, Ann E. Siebert, Benedetto L. DiVito, and Donald I. Good. A verified encrypted packet interface. *ACM SIGSOFT Software Engineering Notes*, 6(3):13–16, July 1981. CODEN SFENDP. ISSN 0163-5948 (print), 1943-5843 (electronic).

StJohns:1984:RAS

[St.84] M. St. Johns. RFC 912: Authentication service, September 1, 1984. URL `ftp://ftp.internic.net/rfc/rfc912.txt`; `ftp://ftp.internic.net/rfc/rfc931.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc912.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc931.txt`; `https://www.math.utah.edu/pub/tex/bib/cryptography.bib`. Obsoleted by RFC0931 [St.85]. Status: UNKNOWN.

StJohns:1985:RAS

[St.85] M. St. Johns. RFC 931: Authentication server, January 1, 1985. URL ftp://ftp.internic.net/rfc/rfc912.txt; ftp://ftp.internic.net/rfc/rfc931.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc912.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc931.txt. Obsoleted RFC1413 [St.93]. Obsoletes RFC0912 [St.84]. Status: UNKNOWN.

Shawe-Taylor:1989:BRB

[ST89] John Shawe-Taylor. Book review: *Cryptography: an introduction to computer security*, by Jennifer Seberry and Josef Pieprzyk. Prentice-Hall International, Hemel Hempstead, United Kingdom, 1988, Price £17.95 (paperback), ISBN 0-7248-0274-6. *Science of Computer Programming*, 12(3):259–260, September 1989. CODEN SCPGD4. ISSN 0167-6423 (print), 1872-7964 (electronic). URL http://www.sciencedirect.com/science/article/pii/0167642389900063.

StJohns:1993:RIP

[St.93] M. St. Johns. RFC 1413: Identification protocol, January 1993. URL ftp://ftp.internic.net/rfc/rfc1413.txt; ftp://ftp.internic.net/rfc/rfc931.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc1413.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc931.txt; https://www.math.utah.edu/pub/tex/bib/cryptography.bib. Obsoletes RFC0931 [St.85]. Status: PROPOSED STANDARD.

Stark:1970:INT

[Sta70] Harold M. Stark. *An introduction to number theory*. Markham mathematics series. Markham Publishing Company, Chicago, IL, USA, 1970. ISBN 0-8410-1014-5. x + 347 pp. LCCN QA241 .S72.

Stark:1978:INT

[Sta78] Harold M. Stark. *An introduction to number theory*. MIT Press, Cambridge, MA, USA, 1978. ISBN 0-262-69060-8. x + 347 pp. LCCN QA241 .S72 1978.

Stevenson:1976:MCI

[Ste76] William Stevenson. *A man called Intrepid: the secret war*. Harcourt, Brace, Jovanovich, San Diego, CA, USA, 1976. ISBN 0-15-156795-6. xxv + 486 + 16 pp. LCCN D810.S8 S85.

Stern:1987:SLC

[Ste87] J. Stern. Secret linear congruential generators are not cryptographically secure. In IEEE [IEE87a], pages 421–426. ISBN 0-8186-0807-2, 0-8186-4807-4 (fiche), 0-8186-8807-6 (case). LCCN QA 76 S979 1987.

Stevens:1988:CPR

[Ste88] A. Stevens. C programming: off and running .... *Dr. Dobb's Journal of Software Tools*, 13

(8):98, 101–102, 104, 106–107, 109–110, 113, August 1988. CODEN DDJOEB. ISSN 0888-3076.

Stephenson:1989:PPM

[Ste89] Peter Stephenson. Personal and private (microcomputer security). *BYTE Magazine*, 14(6): 285–288, June 1989. CODEN BYTEDJ. ISSN 0360-5280.

Stout:1965:DRN

[Sto65] Rex Stout. *The Doorbell Rang: a Nero Wolfe Novel*. ????, ????, 1965. ?? pp.

Stoll:1989:CET

[Sto89] Clifford Stoll. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Doubleday, New York, NY, USA, 1989. ISBN 0-385-24946-2, 0-307-81942-6 (e-book), 0-7434-1145-5, 0-7434-1146-3, 1-299-04734-3. vi + 326 pp. LCCN UB271.R92 H477 1989; UB271.R92 H4771 1989; UB271.R92 S47 1989. US$18.95. URL `http://vxer.org/lib/pdf/The%20Cuckoo%27s%20Egg.pdf`.

Stripp:1987:BJC

[Str87] Alan J. Stripp. Breaking Japanese codes. *Intelligence and National Security*, 2(4):135–??, 1987. ISSN 0268-4527 (print), 1743-9019 (electronic).

Stripp:1989:CFE

[Str89] Alan Stripp. *Codebreaker in the Far East*. Cass series–studies in intelligence. F. Cass, London, England, 1989. ISBN 0-7146-3363-1. xiv + 204 pp. LCCN D810.C88 S76 1989.

Summers:1984:OCS

[Sum84] R. C. Summers. An overview of computer security. *IBM Systems Journal*, 23(4):309–325, 1984. CODEN IBMSA7. ISSN 0018-8670.

SuperMacSoftware:1988:SDE

[Sup88] SuperMac Software. Sentinel Data encryption utility, 1988.

Shulman:1961:GC

[SW61] David Shulman and Joseph Weintraub. *A glossary of cryptography*. Handbook of cryptography; section 1. Crypto Press, New York, NY, USA, 1961. various pp. LCCN Z103 .S48.

Smith:1983:HCR

[SW83] J. W. Smith and S. S. Wagstaff, Jr. How to crack an RSA cryptosystem. *Congressus Numerantium*, 40:367–373, 1983. ISSN 0384-9864.

Salzer:1981:RHH

[SWT+81] Herbert E. Salzer, Eric A. Weiss, Henry S. Tropp, Jane Smith, and Robert W. Rector. Reviews: H. H. Goldstine: A History of Numerical Analysis; Electronics: An Age of Innovation; J. A. N. Lee: Banquet Anecdotes and Conference Excerpts; R. L. Wexelblat: History of Programming Languages: Capsule reviews. *Annals of the History of*

Computing, 3(3):289–302, July/September 1981. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1981/pdf/a3289.pdf`; `http://www.computer.org/annals/an1981/a3289abs.htm`. See minor correction [Ano81a].

Sun:1989:TKE

[SX89] Qi Sun and Rong Xiao. Two kinds of elliptic curves over F_q used to set up cryptosystems. *Sichuan Daxue Xuebao*, 26(1): 39–43, 1989. CODEN SCTHAO. ISSN 0490-6756.

Salomaa:1986:PCB

[SY86a] A. Salomaa and S. Yu. On a public-key cryptosystem based on iterated morphisms and substitutions. *Theoretical Computer Science*, 48(2-3):283–296, ???? 1986. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Salomaa:1986:PKC

[SY86b] Arto Salomaa and Sheng Yu. On a public-key cryptosystem based on iterated morphisms and substitutions. *Theoretical Computer Science*, 48(2-3):283–296 (1987), 1986. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Tao:1985:FAP

[TC85] Ren Ji Tao and Shi Hua Chen. A finite automaton public key cryptosystem and digital signatures. *Chinese Journal of Computers = Chi suan chi hsueh pao*, 8(6):401–409, 1985. CODEN JIXUDT. ISSN 0254-4164.

Tao:1986:TVF

[TC86] Ren Ji Tao and Shi Hua Chen. Two varieties of finite automaton public key cryptosystem and digital signatures. *Journal of computer science and technology*, 1(1):9–18, 1986. CODEN JCTEEM. ISSN 1000-9000.

Tedrick:1985:FES

[Ted85] Tom Tedrick. Fair exchange of secrets (extended abstract). In Blakley and Chaum [BC85], pages 434–438. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=434`. 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.

TI:1984:TTU

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

Thomas:1974:RPS

[Tho74] R. Thomas. RFC 644: On the problem of signature authentication for network mail, July 22, 1974. URL `ftp://ftp.internic.net/rfc/rfc644.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc644.txt`. Status: UNKNOWN. Not online.

Thompson:1984:RTT

[Tho84] Ken Thompson. Reflections on trusting trust. *Communications of the Association for Computing Machinery*, 27(8):761–763, August 1984. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1028.html`.

Thomas:1986:SDE

[Tho86] John A. Thomas. Survey of data encryption in DOL. *Dr. Dobb's Journal of Software Tools*, 11 (6):16–??, June 1986. CODEN DDJOEB. ISSN 1044-789X.

Thompson:1987:RTT

[Tho87] Ken Thompson. Reflections on trusting trust. In Ashenhurst [Ash87], page ?? ISBN 0-201-07794-9. LCCN QA76.24 .A33 1987. ACM Turing Award lecture.

Tsujii:1988:PKC

[TIF+88] Shigeo Tsujii, Toshiya Itoh, Atsushi Fujioka, Kaoru Kurosawa, and Tsutomu Matsumoto. A public-key cryptosystem based on the difficulty of solving a system of nonlinear equations. *Systems and computers in Japan*, 19(2):10–18, 1988. CODEN SCJAEP. ISSN 0882-1666.

Tippett:1927:RSN

[Tip27] L. H. C. (Leonard Henry Caleb) Tippett. *Random sampling numbers*, volume 15 of *Tracts for computers*. Cambridge University Press, Cambridge, UK, 1927. viii + xxvi pp. Reprinted in 1952. Reprinted in 1959 with a foreword by Karl Pearson.

Thompson:1963:SDE

[TP63] James Westfall Thompson and Saul Kussiel Padover. *Secret diplomacy; espionage and cryptography, 1500-1815*. F. Ungar Pub. Co, New York, NY, USA, 1963. 290 pp. LCCN JX1648 .T5 1963. "Appendix: Cryptography": p. 253–263. Bibliography: p. 265–282.

Trithemius:1518:PLS

[Tri18] Johannes Trithemius. *Polygraphiae Libri Sex*. ????, ????, 1518. ???? pp.

Trithemius:1606:CGT

[Tri06a] Johannes Trithemius. *Clauis generalis triplex in libros steganographicos Iohannis Trithemij ....* Iohannis Berneri, Frankfurt, Germany, 1606. 7 + 1 pp. LCCN Z103.T84 S 1606. Ab ipso authore conscripta ... Darmbstadij: Excudebat Balthasar Hofmann,

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

Trithemius:1606:CSI

[Tri06b] Johannes Trithemius. *Clauis Steganographiae Ioannis Trithemij, abbatis Spanheimensis, ad Serenissimum Principem Dn. Philippum ....* Ioannem Bernerum, Frankfurt, Germany, 1606. 70 pp. LCCN Z103.T84 S 1606. Venundatur apud Ioannem Bernerum, bibliopolam Francofurtensem, anno 1606.

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 studiosorum publici iuris facta. Francofurti. Ex officina typographica Matthiae Beckeri, sumptibus Ioannis Berneri, anno 1606.

Trithemius:1621:CGT

[Tri21a] Johannes Trithemius. *Clauis generalis triplex in libros steganographicos Iohannis Trithemij ....* Balthasar Hofmann, Darmstadt, Germany, 1621. 7 + 1 pp. LCCN Z103 .T84 1621. Ab ipso authore conscripta ... Darmbstadij. Excudebat Balthasar Hofmann, impensis Iohannis Berneri, bibliop. Francof., anno 1621.

Trithemius:1621:CSI

[Tri21b] Johannes Trithemius. *Clauis Steganographiae Ioannis Trithemij, abbatis Spanheimensis, ad Serenissimum Principem Dn. Philippum ....* Iohannem Bernerum, Frankfurt, Germany, 1621. 64 pp. LCCN Z103 .T84 1621. Venundatur apud Iohannem Bernerum, bibliopolam Francofurtensem, anno 1621.

Trithemius:1621:SHE

[Tri21c] Johannes Trithemius. *Steganographia: hoc est, ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa.* Balthasaris Aulaeandri, Darmstadt, Germany, 1621. 8 + 152 + 2 pp. LCCN Z103 .T84 1621. Authore ... Ioanne Trithemio ...; praefixa est huic operi sua clauis, seu vera introductio ab ipso authore concinnata ... nunc vero in gratiam secretioris philosophiae studiosorum publici iuris facta. Darmbstadij. Ex officina typographica Balthasaris Aulaeandri, sumptibus vero Ioannis Berneri, bibliop. Francof., anno 1621.

Terry:1988:MSV

[TS88] Douglas B. Terry and Daniel C. Swinehart. Managing stored voice in the Etherphone system. *ACM Transactions on Computer Systems*, 6(1):3–27, February 1988. CO-

DEN ACSYEC. ISSN 0734-2071. URL http://www.acm.org:80/pubs/citations/journals/tocs/1988-6-1/p3-terry/.

Tsudik:1989:DAI

[Tsu89] G. Tsudik. Datagram authentication in Internet gateways: Implications of fragmentation and dynamic routing. *IEEE Journal on Selected Areas in Communications*, 7(4):499–??, May 1, 1989. CODEN ISACEM. ISSN 0733-8716.

Thersites:1984:IKE

[TT84a] Joan Thersites and John A. Thomas. An infinite key encryption system. *Dr. Dobb's Journal of Software Tools*, 9(8): 44–??, August 1984. CODEN DDJOEB. ISSN 1044-789X.

Thomas:1984:IKE

[TT84b] John A. Thomas and Joan Thersites. Infinite key encryption system. *Dr. Dobb's Journal of Software Tools*, 9(8):44–??, August 1984. CODEN DDJOEB. ISSN 1044-789X.

Tuchman:1966:ZT

[Tuc66] Barbara W. Tuchman. *The Zimmermann telegram*. MacMillan Publishing Company, New York, NY, USA, 1966. xii + 244 pp. LCCN D511 .T77 1966. Reprint of original 1958 edition. Kahn [Kah96] describes this book as "recount[ing] the political effects of the most important cryptogram solution in history".

Tuckerman:1970:SVV

[Tuc70] Bryant Tuckerman. A study of the Vigenére–Vernam single and multiple loop enciphering systems. Research Report RC-2879, IBM T. J. Watson Research Center, Yorktown Heights, NY, USA, May 14, 1970.

Tuchman:1979:HPN

[Tuc79a] W. Tuchman. Hellman presents no shortcut solutions to DES. *IEEE Spectrum*, 16(7):40–41, July 1979. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Tuchman:1979:IHP

[Tuc79b] W. Tuchman. IV. 'Hellman presents no shortcut solutions to the DES'. *IEEE Spectrum*, 16(7):40–41, July 1979. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Turing:1941:APC

[Tur41a] Alan M. Turing. The applications of probability to cryptography. Report, GCHQ, Cheltenham, UK, 1941. URL http://www.gchq.gov.uk/Press/Pages/turing-papers-released.aspx; http://www.theregister.co.uk/2012/04/23/turing_papers_released/. Unclassified and released 23 April 2012. Date uncertain, but believed to be between April 1941 and April 1942.

Turing:1941:SR

[Tur41b] Alan M. Turing. On statistics of repetitions. Report, GCHQ, Cheltenham, UK, 1941. URL `http://www.gchq.gov.uk/Press/Pages/turing-papers-released.aspx; http://www.theregister.co.uk/2012/04/23/turing_papers_released/`. Unclassified and released 23 April 2012. Date uncertain, but believed to be between April 1941 and April 1942.

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

[UG23] United States.Army.Signal Corps and George Fabyan Collection (Library of Congress). *Elements of cryptanalysis*. Number 3 in Training pamphlet. United States Government Printing Office, Washington, DC, USA, 1923. vii + 157 pp.

USWarDept:1924:EC

[Uni24a] United States.War Dept. *Elements of cryptanalysis*, volume 3 of *Its training pamphlet*. Government Printing Office, Washington, DC, USA, 1924. vii + 157 pp. LCCN Z104 .U6.

USWD:1924:EC

[Uni24b] United States.War Dept. *Elements of cryptanalysis*. Number 3 in Its Training pamphlet. United States Government Printing Office, Washington, DC, USA, 1924. vii + 157 pp.

USASC:1940:CML

[Uni40] United States Army Signal Corps. *Cryptanalyst's manual*. United States Government Printing Office, Washington, DC, USA, 1940. ???? pp. LCCN Z104 .U33c.

USASC:1942:ACC

[Uni42] United States.Army.Signal Corps. *Articles on cryptography and cryptanalysis*. United States Government Printing Office, Washington, DC, USA, 1942. v + 316 pp.

USDOS:1970:BC

[Uni70] United States.Dept.of the Army. *Basic cryptanalysis*. United States Government Printing Office, Washington, DC, USA, September 13, 1970. various pp.

USNBS:1977:DES

[Uni77] United States.National Bureau of Standards. *Data Encryption Standard*, volume 46 of *Federal Information Processing Standards publication*. U.S. National Bureau of Standards,

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

USCSC:1978:CSD

[Uni78a] United States.Civil Service Commission. *Computer security and the Data Encryption Standard: proceedings of the Conference on Computer Security and the Data Encryption Standard held at the National Bureau of Standards in Gaithersburg, Maryland, on February 15, 1977*. Washington, DC, USA, 1978. viii + 125 pp.

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

USNA:1979:CS

[Uni79a] United States.National Archives and Records Service. Cryptology studies. Records of the National Security Agency RG457, National Archives of the United States, Washington, DC, USA, 1979. ?? pp.

USNSG:1979:IRW

[Uni79b] United States.Naval Security Group. *Intelligence reports on the war in the Atlantic, 1942–1945: the account of the war in the Atlantic from Dec. 1942 to May 1945 as seen through and influenced by decryption of German naval radio traffic: [guide]*. Michael Glazier, Wilmington, DE, USA, 1979. 6 pp.

USNBS:1981:GIU

[Uni81] United States.National Bureau of Standards. *Guidelines for implementing and using the NBS Data Encryption Standard: category: ADP operations, subcategory: computer security*. FIPS Pub; 74. U.S. National Bureau of Standards, Gaithersburg, MD, USA, April 1, 1981. CODEN FIPPAT. 39 pp.

USDA:1982:SMM

[Uni82a] United States.Dept.of the Army. *Soldier's manual: MOS 32G: fixed cryptographic equipment repairer, skill levels 1 and 2*. Dept. of the Army, Headquarters, Washington, DC, USA (??), May 1982. various pp.

USDA:1982:TGM

[Uni82b] United States.Dept.of the Army. *Trainer's guide: MOS 32G: fixed cryptographic equipment repairer*. Dept. of the Army, Headquarters, Washington, DC, USA (??), May 14, 1982. 35 pp.

USGSA:1982:TGS

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

ing the Data Encryption Standard. General Services Administration, Washington, DC, USA, April 14, 1982. 12 pp. Federal Standard 1027.

USNBS:1983:FPD

[Uni83] *FIPS Pub 46: Data Encryption Standard. FIPS publication change notice*, page various, 1983. U.S. Department of Commerce, National Bureau of Standards, Washinton, DC, USA.

USGSAOIRM:1984:ISR

[Uni84] United States.General Services Administration.Office of Information Resources Management. *Interoperability and security requirements for use of the Data Encryption Standard in the physical layer of data communications*. Office of Information Resources Management, 1984. various pp. Cover title. "August 3, 1983." "FSC TELE.".

USGAOPEMD:1987:PDD

[Uni87] United States.General Accounting Office.Program Evaluation and Methodology Division. *Privacy data: the Data Encryption Standard provides valuable protection*. Transfer paper - Program Evaluation and Methodology Division; 8 Transfer paper (United States. General Accounting Office. Program Evaluation and Methodology Division); 8. The Division, Washington, DC, USA, 1987. 80 pp.

USDA:1988:CED

[Uni88a] United States.Dept.of the Army. Cryptographic equipment destroyer, incendiary, TH1/TH4, M1A1, M1A2, and M2A1: ammunition surveillance procedures. Department of the Army supply bulletin SB 742-1375-94-801, Dept. of the Army, Headquarters, Washington, DC, USA (??), April 6, 1988. various pp. Supersedes SB 742-1375-94-3, 21 March 1974.

USNBS:1988:DES

[Uni88b] United States.National Bureau of Standards. *Data Encryption Standard*. Number 46-1 in Federal Information Processing Standards publication. National Technical Information Service, Washington, DC, USA, 1988. 16 pp. LCCN JK468.A8 A31 no.46 1988. Category: ADP operations; subcategory: computer security. Supersedes FIPS PUB 46, 1977 January 15. Shipping list no.: 88-367-P. Reaffirmed 1988 January 22.

USGSA:1983:ISR

[UNN83] United States.General Services Administration, National Communications System (U.S.). Office of Technology and Standards, and National Institute of Standards and Technology (U. S.). Interoperability and security requirements for use of the Data Encryption Standard in the physical layer of data communications. Technical report, General Services Admin-

istration, Office of Information Resources Management, Washington, DC, USA, August 3, 1983. 4 pp. Federal standard 1026. Federal information processing standards publication, FIPS PUB 139.

USGSA:1985:ISR

[UNN85] United States.General Services Administration, National Communications System (U.S.). Office of Technology and Standards, and National Institute of Standards and Technology (U. S.). Interoperability and security requirements for use of the Data Encryption Standard with CCITT group 3 facsimile equipment. Technical report, General Services Administration, Office of Information Resources Management, Washington, DC, USA, April 4, 1985. 2 pp. Federal standard 1028. Federal information processing standards publication, FIPS PUB 141.

USENIX:1988:USWa

[USE88a] USENIX, editor. *UNIX Security Workshop Proceedings, August 29–30, 1988. Portland, OR*. USENIX Association, Berkeley, CA, USA, 1988. LCCN QA76.8.U65 U55 1988(1)-1990(2)//.

USENIX:1988:PFU

[USE88b] USENIX Association, editor. *Proceedings of the (First) USENIX Security Workshop, August 29–30, 1988, Portland, OR, USA*. USENIX Association, Berkeley, CA, USA, 1988. LCCN QA76.8.U65 U55 1988(1)-1990(2)//.

USENIX:1988:UCPb

[USE88c] USENIX Association, editor. *USENIX Conference Proceedings (Dallas, TX, USA)*. USENIX Association, Berkeley, CA, USA, Winter 1988. ISBN ???? LCCN ????

USENIX:1989:UCPb

[USE89a] USENIX, editor. *USENIX Conference Proceedings, Summer, 1989. Baltimore, MD*. USENIX Association, Berkeley, CA, USA, Summer 1989.

USENIX:1989:PSU

[USE89b] USENIX Association, editor. *Proceedings of the Summer 1989 USENIX Conference: June 12 — June 16, 1989, Baltimore, Maryland USA*. USENIX Association, Berkeley, CA, USA, 1989. LCCN QA 76.76 O63 U83 1989.

USENIX:1999:UAT

[USE99] USENIX, editor. *Usenix Annual Technical Conference. June 6–11, 1999. Monterey, California, USA*. USENIX Association, Berkeley, CA, USA, 1999. ISBN 1-880446-33-2. LCCN A76.8.U65 U843 1999. URL `http://db.usenix.org/publications/library/proceedings/usenix99`.

USWD:1980:EC

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

Office. *Elements of cryptanalysis*. Training pamphlet; no. 3 War Dept document; no. 117 Training pamphlet (United States. War Dept.); no. 3. Document (United States. War Dept.); no. 117. United States Government Printing Office, Washington, DC, USA, 1980. 165 pp.

USWD:1983:EC

[UU83] United States.War Dept and United States.Adjutant-General's Office. *Elements of cryptanalysis*. United States. War Dept. Training pamphlet no. 3. War Dept document no. 117. United States Government Printing Office, Washington, DC, USA, 1983. 165 pp.

USDOA:1989:BC

[UU89] United States.Dept.of the Army and United States Army Intelligence School. *Basic cryptanalysis*. United States Army Intelligence School, Fort Devens, Ma., coordinating draft. edition, 1989. various pp.

VanderBank:1988:CFM

[VA88] Dirk Van der Bank and Edwin Anderssen. Cryptographic figures of merit. *Computers and Security*, 7(3): 299–303, June 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888900363`.

Valerio:1892:C

[Val92] Paul Louis Eugene Valerio. De la cryptographie. *Journal des Sciences militares, 9th series, Paris*, ??(??):??, December 1892.

Vamos:1985:BRB

[Vam85] T. Vamos. Book review: *Mr. Babbage's secret. The tale of a cypher — and APL*: Ole Immanuel Franksen. *Automatica*, 21(5):616, September 1985. CODEN ???? ISSN ???? URL `http://www.sciencedirect.com/science/article/pii/0005109885900135`.

VanTassel:1969:ACT

[Van69] Dennie Van Tassel. Advanced cryptographic techniques for computers. *Communications of the Association for Computing Machinery*, 12(12):664–665, December 1969. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Vandeberg:1986:ICS

[Van86] Ronald D. Vandeberg. Implementation of a coprocessing system to support data encryption. Thesis (M.S. in Computer Science), University of Wisconsin-Milwaukee, Milwaukee, WI, USA, 1986. 112 pp.

VanHeurck:1987:TNS

[Van87] Philippe Van Heurck. TRASEX: national security system for EFTs in Belgium. *Computer Networks and ISDN Systems*, 14

(2–5):389–395, 1987. CODEN CNISE9. ISSN 0169-7552.

vanTilborg:1988:IC

[van88] Henk C. A. van Tilborg. *An introduction to cryptology*, volume SECS 52 of *The Kluwer international series in engineering and computer science; Communications and information theory*. Kluwer Academic Publishers, Dordrecht, The Netherlands, 1988. ISBN 0-89838-271-8. x + 170 pp. LCCN Z103 .T541 1988. US$45.00.

vandenAssem:1986:CPA

[vdAvE86] R. van den Assem and W. J. van Elk. A chosen-plaintext attack on the Microsoft BASIC protection. *Computers and Security*, 5(1):36–45, March 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404886901161`.

Vernam:1926:CPT

[Ver26] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal American Institute of Electrical Engineers*, XLV(??):109–115, 1926.

Vallee:1988:HBO

[VGT88] Brigitte Vallée, Marc Girault, and Philippe Toffin. How to break Okamoto's cryptosystem by reducing lattice bases. *Lecture Notes in Computer Science*, 330:281–291, 1988. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vallee:1989:HGR

[VGT89] Brigitte Vallée, Marc Girault, and Philippe Toffin. How to guess l th roots modulo n by reducing lattice bases. In Mora [Mor89], pages 427–442. CODEN LNCSD9. ISBN 0-387-51083-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA268 .A35 1988. US$36.00 (USA).

Vincent:1971:PAG

[Vin71] C. H. Vincent. Precautions for accuracy in the generation of truly random binary numbers. *Journal of Physics. E: Scientific Instruments*, 4(11):825–828, 1971. CODEN JPSIAE. ISSN 0022-3735. URL `http://stacks.iop.org/0022-3735/4/i=11/a=007`. See corrigendum [Vin72].

Vincent:1972:CPA

[Vin72] C. H. Vincent. Corrigendum: Precautions for accuracy in the generation of truly random binary numbers. *Journal of Physics. E: Scientific Instruments*, 5(6):546, 1972. CODEN JPSIAE. ISSN 0022-3735. URL `http://stacks.iop.org/0022-3735/5/i=6/a=521`. See [Vin71].

Voydock:1983:SMH

[VK83] Victor L. Voydock and Stephen T. Kent. Security mechanisms in high-level network pro-

tocols. *ACM Computing Surveys*, 15(2):135–171, June 1983. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Voydock:1984:SMT

[VK84] Victor L. Voydock and Stephen T. Kent. Security mechanisms in a transport layer protocol. *Computer Networks: The International Journal of Distributed Informatique*, 8(5–6):433–449, October/December 1984. CODEN CNETDP. ISSN 0376-5075.

Kerckhoffs:1883:CMF

[vN83] Auguste Kerckhoffs (von Nieuwenhof). La cryptographie militaire. (French) [Military cryptography]. *Journal des Sciences Militaires*, IX(??):5–38, 161–191, January/February 1883. URL `http://www.cl.cam.ac.uk/~fapp2/kerckhoffs/la_cryptographie_militaire_i.htm` `https://www.petitcolas.net/kerckhoffs/`; `https://www.petitcolas.net/kerckhoffs/crypto_militaire_1_b.pdf`; `https://www.petitcolas.net/kerckhoffs/crypto_militaire_2.pdf`.

Vogel:1985:LCC

[Vog85] Rainer Vogel. On the linear complexity of cascaded sequences. In Beth et al. [BCI85], pages 99–109. CODEN LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). 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.

Volts:1941:BCP

[Vol41] James D. Volts. *Bibliography of cryptography: Part I: Cryptography*. U. S. Army, Cincinnati, OH, USA, 1941. various pp. LCCN ???? Chronologically arranged, covering period 1518–1940, and indexed by authors.

Voukalis:1980:DFC

[Vou80a] D. C. Voukalis. The distance factor in cryptosystems. *International Journal of Electronics Theoretical & Experimental*, 49(1):73–75, 1980. CODEN IJELA2. ISSN 0020-7217.

Voukalis:1980:GSE

[Vou80b] D. C. Voukalis. A good solution of the encryption problem using matrix code, distance factor and PN sequences. *Internat. J. Electron.*, 48(3):271–274, 1980. CODEN IJELA2. ISSN 0020-7217.

Vassiliadis:1988:PEA

[VPS88] Stamatis Vassiliadis, Michael Putrino, and Eric M. Schwarz. Parallel encrypted array multipliers. *IBM Journal of Research and Development*, 32(4):536–551, July 1988. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Volts:1941:BC

[VS41] James D. Volts and David Shulman. *Bibliography of cryptography*. U. S. Army, Cincinnati, OH. USA, 1941. 93 pp. LCCN Z103.A1 V6 1941. Typewritten (carbon copy) Three heavy leaves precede sections II-IV (not included in pagination). This copy was made especially for the United States Army from the original manuscript. Third copy: pencilled note on cover. Contents: pt.1. Cryptography; pt.2. Titles relating indirectly to cryptography; pt.3. Rejected titles; pt.4. Author index.

vanTilburg:1986:DBK

[vTB86] Johan van Tilburg and Dick E. Boekee. Divergence bounds on key equivocation and error probability in cryptanalysis. *Lecture Notes in Computer Science*, 218:489–513, 1986. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vazirani:1985:ESP

[VV85] Umesh V. Vazirani and Vijay V. Vazirani. Efficient and secure pseudo-random number generation (extended abstract). In Blakley and Chaum [BC85], pages 193–202. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=??&volume=0&issue=0&spage=193`. 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.

Valiant:1986:NED

[VV86] L. G. Valiant and V. V. Vazirani. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47(1):85–93, ???? 1986. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Waber:1987:VEC

[Wab87] John James Waber. Voice encryption for cellular telephones. Thesis (M.S.), University of Colorado, Boulder, CO, USA, 1987. x + 124 pp.

Wagner:1983:F

[Wag83] Neal R. Wagner. Fingerprinting. In IEEE [IEE83], pages 18–22. ISBN 0-8186-0467-0 (paperback), 0-8186-4467-2 (microfiche), 0-8186-8467-4 (hardcover). LCCN QA76.9.A25 S95 1983. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1030.html`.

Walden:1900:ADB

[Wal00] John William Henry Walden. *August, Duke of Braunschweig-Luneburg: The cryptomenytics and cryptography of Gustavus Selenus: in nine books:*

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

[Wan86] Yuedong Wang. *Using encryption for authentication in local area networks*. ????, ????, 1986. ?? pp.

Warren:1982:BTC

[War82] Alexander Z. Warren. *Basicplus through cryptanalysis; an introduction to structured programming*. ????, ????, 1982. 100 pp. Privately printed.

Watler:1989:VAC

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

Wegman:1981:NHF

[WC81] Mark N. Wegman and J. Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, June 1981. CODEN JCSSBM. ISSN 0022-0000.

Worthington:1986:IDS

[WCWG86] T. K. Worthington, J. J. Chainer, J. D. Willford, and S. C. Gunderson. IBM dynamic signature verification. *Computers and Security*, 5(2): 167–168, June 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/016740488690146X`.

Weber:1979:USD

[Web79] Ralph Edward Weber. *United States Diplomatic Codes and Ciphers, 1775–1938*. Precedent Publishing, Chicago, IL, USA, 1979. ISBN 0-913750-20-4. xviii + 633 pp. LCCN Z103 .W4. US$49.95.

Webb:1988:NPK

[Web88] W. A. Webb. A nonlinear public key cryptosystem. *Computers and Mathematics with Applications*, 15(2):81–84, 1988. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic).

Weingarten:1983:CCP

[Wei83] F. Weingarten. Controlling cryptographic publication. *Computers and Security*, 2(1): 41–48, January 1983. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404883900330`.

Weiss:1988:BOP

[Wei88] Eric A. Weiss. Biographies: Oh, pioneers! *Annals of the History of Computing*, 10(4):348–361, October/

December 1988. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1988/pdf/a4348.pdf`; `http://www.computer.org/annals/an1988/a4348abs.htm`.

Wells:1980:ADB

[Wel80] David L. Wells. Achieving data base protection through the use of subkey encryption. Thesis (Doctor of Engineering), University of Wisconsin-Milwaukee, Milwaukee, WI, USA, 1980. 131 pp.

Welchman:1982:HSS

[Wel82a] Gordon Welchman. *The Hut Six story: breaking the Enigma codes*. McGraw-Hill, New York, NY, USA, 1982. ISBN 0-07-069180-0. ix + 326 pp. LCCN D810.C88 W44.

Wells:1982:USE

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

Welchman:1986:PBB

[Wel86] G. Welchman. From Polish Bomba to British Bombe. The birth of Ultra. *Intelligence and National Security*, 1(1):71–110, ???? 1986. ISSN 0268-4527 (print), 1743-9019 (electronic).

Wells:1988:NAI

[Wel88a] Codie Wells. A note on "Protection Imperfect". *Operating Systems Review*, 22(4):35, October 1988. CODEN OSRED8. ISSN 0163-5980. See [Hog88].

Welsh:1988:CC

[Wel88b] Dominic Welsh. *Codes and cryptography*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1988. ISBN 0-19-853288-1 (hardcover), 0-19-853287-3 (paperback). ix + 257 pp. LCCN Z103 .W461 1988. UK£30.00, US$60.00 (hardcover), UK£15.00 (paperback).

Welsh:1989:CC

[Wel89] Dominic Welsh. *Codes and cryptography*. Oxford science publications. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1989. ISBN 0-19-853287-3 (paperback). ix + 257 pp. LCCN Z 103 W46 1989. Reprinted with corrections.

Wilkes:1982:MRJ

[WG82] Maurice V. Wilkes and I. J. Good. Meetings in retrospect: J. G. Brainerd on the ENIAC; A Report on T. H. Flowers's Lecture on Colossus. *Annals of the History of Computing*, 4(1):53–59, January/March 1982. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1982/pdf/a1053.pdf`; `http://www.computer.`

org/annals/an1982/a1053abs.htm.

Wheeler:1987:BE

[Whe87] David Wheeler. Block encryption. Technical report 120, Computer Laboratory, University of Cambridge, Cambridge, Cambridgeshire, UK, 1987. 4 pp.

Wichmann:1987:NAR

[Wic87] B. A. Wichmann. Note on Algorithm 121: RSA key calculation in Ada. *The Computer Journal*, 30(3):276, June 1987. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_30/Issue_03/tiff/276.tif. See [Hun85].

Wiedemann:1986:QC

[Wie87] D. Wiedemann. Quantum cryptography. *ACM SIGACT News*, 18(2):48–51, September/March 1986–1987. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Wilkins:1641:MSS

[Wil41] John Wilkins. *Mercury, or the Secret and Swift Messenger*. ????, ????, 1641. ???? pp.

Wilkes:1968:TSCa

[Wil68a] M. V. (Maurice Vincent) Wilkes. *Time-sharing computer systems*, volume 5 of *Macdonald computer monographs*. Macdonald and Co., London, UK, 1968. ISBN 0-356-02426-1. vii + 102 pp. LCCN QA76.5 .W523 1968b.

Wilkes:1968:TSCb

[Wil68b] M. V. (Maurice Vincent) Wilkes. *Time-sharing computer systems*, volume 5 of *Computer monograph series*. American Elsevier Pub. Co., New York, NY, USA, 1968. 102 pp. LCCN QA76.5 .W523.

Wilkes:1972:TSC

[Wil72] M. V. (Maurice Vincent) Wilkes. *Time-sharing computer systems*, volume 5 of *Computer monographs*. Macdonald and Co., London, UK, second edition, 1972. ISBN 0-444-19583-1 (Elsevier). ix + 149 pp. LCCN QA76.5 .W523 1972.

Wilkes:1975:TSC

[Wil75] M. V. (Maurice Vincent) Wilkes. *Time-sharing computer systems*. Computer monographs. Macdonald and Jane's, London, UK, third edition, 1975. ISBN 0-444-19525-4 (American Elsevier). ii + 166 pp. LCCN QA76.53 .W54 1975.

Williams:1980:MRP

[Wil80] H. C. Williams. A modification of the RSA public-key encryption procedure. *IEEE Transactions on Information Theory*, 26(6):726–729, 1980. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Willett:1982:CON

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

curity, 1(2):177–186, June 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404882900104`.

Willett:1982:TPK

[Wil82b] Michael Willett. A tutorial on public key cryptography. *Computers and Security*, 1(1): 72–79, January 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404882900281`.

Williams:1982:CHP

[Wil82c] Hugh C. Williams. Computationally "hard" problems as a source for cryptosystems. In *Secure communications and asymmetric cryptosystems*, volume 69 of *AAAS Sel. Sympos. Ser.*, pages 11–39. Westview, Boulder, CO, 1982.

Willett:1983:TKS

[Wil83a] Michael Willett. Trapdoor knapsacks without superincreasing structure. *Information Processing Letters*, 17(1):7–11, July 19, 1983. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Williams:1983:PAP

[Wil83b] M. H. Williams. The problem of absolute privacy. *Information Processing Letters*, 17(3): 169–171, October 5, 1983. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Williams:1985:SPK

[Wil85] H. C. Williams. Some public-key crypto-functions as intractable as factorization. In Blakley and Chaum [BC85], pages 66–70. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=66`. 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.

Williams:1986:PKE

[Wil86a] H. C. Williams. An M^3 public-key encryption scheme. In *Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985)*, volume 218 of *Lecture Notes in Comput. Sci.*, pages 358–368. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1986.

Williams:1986:ACC

[Wil86b] Hugh C. Williams, editor. *Advances in cryptology — CRYPTO '85: proceedings: August 18–22, 1985*, volume

218 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1986. CODEN LNCSD9. ISBN 0-387-16463-4 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1985; QA267.A1 L43 no.218. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0218.htm; http://www.springerlink.com/content/978-0-387-16463-2; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=218.

Williams:1986:CTU

[Wil86c] John J. Williams. *Cryptanalysis techniques: the ultimate decryption manual*. Consumertronics Co., Alamogordo, NM, USA, 1986. 11 + 3 + 1 pp.

Winterbotham:1969:SP

[Win69] F. W. (Frederick William) Winterbotham. *Secret and personal*. Kimber, London, UK, 1969. ISBN 0-7183-0321-0. 192 pp. LCCN D810.S7 W48; D810.S7 W73.

Winterbotham:1974:US

[Win74a] F. W. (Frederick William) Winterbotham. *The Ultra secret*. Weidenfeld and Nicolson, London, UK, 1974. ISBN 0-297-76832-8. xiii + 199 pp. LCCN D810.C88 W56.

Winterbotham:1974:USF

[Win74b] F. W. (Frederick William) Winterbotham. *The Ultra secret: the first account of the most astounding cryptanalysis coup of World War II — how the British broke the German code and read most of the signals between Hitler and his generals throughout the war*. Harper & Row, New York, NY, USA, 1974. ISBN 0-06-014678-8. xiii + 199 pp. LCCN D810.C95 W73 1974.

Winterbotham:1975:US

[Win75] F. W. (Frederick William) Winterbotham. *The Ultra secret*. Dell, New York, NY, USA, 1975. ISBN ???? 286 pp. LCCN D810.C88 W56 1976.

Winterbotham:1978:NC

[Win78] F. W. (Frederick William) Winterbotham. *The Nazi connection*. Harper & Row, New York, NY, USA, 1978. ISBN 0-06-014686-9. 222 pp. LCCN D810.S8 .W538 1978.

Winternitz:1983:POW

[Win83] Robert S. Winternitz. Producing a one-way hash function from DES. In Chaum et al. [CRS83], pages 203–207. ISBN 1-4757-0604-9 (print), 1-4757-0602-2. LCCN QA76.9.A25 C79 1982.

Winternitz:1984:SOH

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

Symposium on Security and Privacy, pages 88–90, 1984. CODEN PSSPEO. ISBN 0-8186-0532-4. IEEE Service Cent. Piscataway, NJ, USA.

Winterbotham:1989:US

[Win89] F. W. (Frederick William) Winterbotham. *The Ultra spy*. Macmillan, London, UK, 1989. ISBN 0-333-51425-4. 258 + 8 pp. LCCN UB271.G72 W564 1989. US$12.95.

Wagner:1985:PKC

[WM85] Neal R. Wagner and Marianne R. Magyarik. A public-key cryptosystem based on the word problem. In Blakley and Chaum [BC85], pages 19–36. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=19`. 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.

Wolfe:1943:FCCa

[Wol43a] Jack Martin Wolfe. *A first course in cryptanalysis*. Brooklyn college press, Brooklyn, NY, USA, 1943. ?? pp. LCCN Z104 .W6 1943 v. 1-3 (1943). Reproduced from type-written copy. Lesson 11 (44 numb) inserted after v. 2.

Wolfe:1943:FCCb

[Wol43b] Jack Martin Wolfe. *A first course in cryptanalysis*. University Press, Ann Arbor, MI, USA, 1943. various pp. Three volumes.

Wolfe:1943:FCCc

[Wol43c] Jack Martin Wolfe. *A first course in cryptanalysis*. Brooklyn College Press, Brooklyn, NY, USA, 1943. various pp. Three volumes.

Wolfe:1970:SWC

[Wol70] James Raymond Wolfe. *Secret writing: the craft of the cryptographer*. McGraw-Hill, New York, NY, USA, 1970. 192 pp. LCCN 652.8 W. Explains the distinction between ciphers and codes and describes their past and present use in secret communications.

Wolfe:1983:FCC

[Wol83] Jack Martin Wolfe. *A first course in cryptanalysis [!]*. Brooklyn College Press, Brooklyn, 1983. various pp. Three volumes.

Wood:1982:FAC

[Woo82] Charles Cresson Wood. Future applications of cryptography. *Computers and Security*, 1 (1):65–71, January 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (elec-

tronic). URL https://www.sciencedirect.com/science/article/pii/016740488290027X.

Worth:1975:CMA

[Wor75] Vivian I. Worth. Cryptology: mathematical applications. Thesis (M.S.), Central Missouri State University, Warrensburg, MO, USA, 1975. iv + 63 pp.

Wortmann:1987:BRB

[Wor87] J. C. Wortmann. Book review: *Mr. Babbage's secret: The tale of a Cypher — and APL*: Strandberg, Birkerød, (Denmark) 1984, 319 pages. *European Journal of Operational Research*, 29(2):216, May 1987. CODEN EJORDT. ISSN 0377-2217 (print), 1872-6860 (electronic). URL http://www.sciencedirect.com/science/article/pii/0221787901184.

Wrixon:1989:CCS

[Wri89] Fred B. Wrixon. *Codes, ciphers, and secret language*. Harrap, London, UK, 1989. ISBN 0-245-54880-7. 266 pp. LCCN Z103 .W77 1989b.

Williams:1979:SRC

[WS79] H. C. Williams and B. Schmid. Some remarks concerning the M.I.T. public-key cryptosystem. *BIT*, 19(4):525–538, December 1979. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=19&issue=4&spage=525.

Webster:1986:DB

[WT86] A. F. Webster and Stafford E. Tavares. On the design of S-boxes. In Williams [Wil86b], pages 523–534. CODEN LNCSD9. ISBN 0-387-16463-4 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1985; QA267.A1 L43 no.218. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0218.htm; http://www.springerlink.com/content/978-0-387-16463-2; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=218.

Weiss:1985:RCM

[WTE+85] Eric A. Weiss, Henry S. Tropp, Ralph Erskine, John A. N. Lee, Gwen Bell, and M. R. Williams. Reviews: The Computer Museum and J. Bernstein, Three Degrees Above Zero: Bell Labs in the Information Age and D. R. Hartree, Calculating Machines: Recent and Prospective Developments and Their Impact on Mathematical Physics, and, Calculating Instruments and Machines and W. Kozaczuk, Enigma: How the German Machine Cipher Was Broken and How It Was Read by the Allies in World War Two and S. Levy, Hackers and A. Osborne and J. Dvorak, Hypergrowth: The Rise and Fall of Osborne Computer Corporation and E. W.

Pugh, Memories that Shaped an Industry and capsule reviews. *Annals of the History of Computing*, 7(3):258–277, July/September 1985. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1985/pdf/a3258.pdf; http://www.computer.org/annals/an1985/a3258abs.htm`.

Williams:1979:CAA

[WW79] P. W. Williams and D. Woodhead. Computer assisted analysis of cryptic crosswords. *The Computer Journal*, 22(1):67–70, February 1979. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Wah:1984:RAM

[WW84] P. K. S. Wah and M. Z. Wang. Realization and application of the Massey–Omura lock. In IEEE, editor, *1984 International Zurich Seminar on Digital Communications: applications of source coding, channel coding and secrecy coding: March 6–8, 1984, Zürich, Switzerland, Swiss Federal Institute of Technology: proceedings*, pages 175–182. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1984. LCCN TK7881.5 I65 1984. IEEE catalog number 84CH1998-4.

Yao:1982:PSC

[Yao82a] A. Yao. Protocols for secure computation. In IEEE [IEE82a], pages 160–164. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA76.6 .S95 1982. IEEE catalog no. 82CH1806-9. IEEE Computer Society order no. 440.

Yao:1982:TAT

[Yao82b] A. C. Yao. Theory and application of trapdoor functions. In IEEE [IEE82a], pages 80–91. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA76.6 .S95 1982. IEEE catalog no. 82CH1806-9. IEEE Computer Society order no. 440.

Yao:1986:HGE

[Yao86] A. C. Yao. How to generate and exchange secrets. In IEEE [IEE86b], pages 162–167. ISBN 0-8186-0740-8 (paperback), 0-8186-4740-X (microfiche), 0-8186-8740-1 (casebound). LCCN QA 76 S979 1986; TK7885.A1 S92 1986.

Yardley:1931:ABC

[Yar31] Herbert O. Yardley. *The American Black Chamber*. Faber & Faber Limited, London, UK, 1931. x + 264 + 1 pp. LCCN D639.S7 Y3 1931b. The history and work of the Cryptographic bureau, officially known as section 8 of the Military intelligence division (MI-8).

Yardley:1940:SSA

[Yar40] Herbert O. Yardley. *Secret service in America: The American Black Chamber*. Faber & Faber Limited, London, UK, 1940. x

+ 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

[Yar83] Herbert O. Yardley. *The Chinese Black Chamber: an adventure in espionage*. Houghton-Mifflin, Boston, MA, USA, 1983. ISBN 0-395-34648-7. xxiv + 225 pp. LCCN DS777.533.S65 Y37 1983. US$13.95. Chinese title: Chung-kuo hei shih.

Yasaki:1976:EAK

[Yas76] E. K. Yasaki. Encryption algorithm: key size is the thing. *Datamation*, 22(3):164–166, March 1976. CODEN DTMNAT. ISSN 0011-6963.

Yung:1985:CSP

[Yun85a] Mordechai Yung. Cryptoprotocols: Subscription to a public key, the secret blocking and the multi-player mental poker game (extended abstract). In Blakley and Chaum [BC85], pages 439–453. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=439`. 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.

Yung:1985:SUK

[Yun85b] Mordechai M. Yung. A secure and useful "keyless cryptosystem". *Information Processing Letters*, 21(1):35–38, July 10, 1985. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Yu:1989:DEB

[YY89] K. W. Yu and T. L. Yu. Data encryption based upon time reversal transformations. *The Computer Journal*, 32(3):241–245, June 1989. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Zafiropulo:1963:RAD

[Zaf63] Jean Zafiropulo. Le rôle de l'analogie dans le déchiffrement de l'écriture mycénienne linéaire B. (French) [The role of analogy in deciphering Mycenaean linear script B]. *Dialectica: International Review of Philosophy of Knowledge*, 17(4):307–327, December 1963. CODEN ???? ISSN 0012-2017 (print), 1746-8361 (electronic).

Zeidler:1979:DDE

[Zei79] Howard M. Zeidler. *Digital data encryption*. SRI International, 333 Ravenswood Avenue, Menlo Park, CA 94025-3493, USA, Tel:

+1 415 859 6387, FAX: +1 415 859-6028, 1979. 20 pp.

Zim:1948:CSW

[Zim48] Herbert S. Zim. *Codes and secret writing*. William Morrow, New York, NY, USA, 1948. vi + 154 pp. LCCN Z104 .Z5.

Zorpette:1987:BEC

[Zor87] Glenn Zorpette. Breaking the enemy's code: British intelligence deciphered Germany's top-secret military communications with Colossus, an early vacuum-tube computer. *IEEE Spectrum*, 24(9):47–51, September 1987. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).