

# A Complete Bibliography of Publications in *Cryptologia*

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

E-mail: [beebe@math.utah.edu](mailto:beebe@math.utah.edu), [beebe@acm.org](mailto:beebe@acm.org),  
[beebe@computer.org](mailto:beebe@computer.org) (Internet)  
WWW URL: <https://www.math.utah.edu/~beebe/>

01 April 2025  
Version 3.79

## Title word cross-reference

( <i>t, m</i> ) [?]. ( <i>t, n</i> ) [?, ?]. \$10.00 [?]. \$12.00 [?]. 128 [?]. \$139.99 [?]. \$15.00 [?]. \$16.95 [?, ?]. \$16.96 [?]. \$18.95 [?]. \$24.00 [?]. \$24.00/\$34 [?]. \$24.04 [?]. \$24.95 [?, ?]. \$26.95 [?]. \$29.95 [?]. \$30.00 [?]. \$30.95 [?]. \$38.00 [?]. \$39 [?]. \$39.95 [?]. \$43.39 [?]. \$45.00 [?]. \$5.95 [?]. \$54.00 [?]. \$54.95 [?]. \$54.99 [?]. \$6.50 [?]. \$6.95 [?]. \$69.00 [?]. \$69.95 [?]. \$75.00 [?]. \$89.95 [?]. <sup>th</sup> [?]. <i>A</i> [?]. $A^3$ [?, ?]. $\chi$ [?]. $H$ [?]. $k$ [?, ?, ?]. $M$ [?, ?, ?]. $M^3$ [?]. $n$ [?, ?, ?, ?]. $q$ [?]. -ary [?]. -Bit [?]. -error [?]. -out-of- [?, ?]. -sequences [?]. -tests [?]. 0 [?]. 000 [?]. 01Q [?, ?].	1 [?, ?, ?, ?, ?]. 1-4398-1763-4 [?]. 1/2in [?, ?]. 10 [?]. 100 [?, ?]. 10011-4211 [?]. 10016-8810 [?, ?]. 1221 [?]. 125 [?]. 15.00/\$23.60.0 [?]. 15th [?, ?]. 16th [?, ?]. 17-18 [?]. 18 [?]. 180-4 [?]. 1812 [?]. 18th [?, ?, ?, ?, ?, ?]. 18th-Century [?]. 1930s [?]. 1939 [?]. 1940 [?, ?]. 1940s [?]. 1941 [?]. 1942 [?]. 1943 [?]. 1945 [?, ?, ?, ?, ?, ?]. 1946 [?, ?, ?]. 1950s [?]. 1970s [?]. 1980s [?]. 1989 [?]. 19th [?, ?, ?, ?, ?, ?]. 19th-century [?].
	2 [?, ?, ?]. 200/220 [?]. 2000 [?]. 2004 [?, ?]. 2008 [?]. 2009 [?]. 2011 [?]. 2013 [?, ?]. 2014 [?]. 2017 [?]. 2019 [?]. 2024 [?]. 20755-6886 [?]. 209 [?, ?, ?, ?, ?, ?]. 20th [?]. 21 [?]. 22 [?]. 220 [?]. 24-Hour [?, ?, ?]. 25 [?, ?]. 25.00/\$39.30 [?]. 25.00/839.30 [?]. 25A1 [?]. 25B [?]. 26 [?, ?]. 28147 [?]. 28147-89 [?]. 285 [?]. 294 [?]. 2in [?, ?]. 2nd [?, ?, ?, ?].





















International [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Internet [?, ?]. Interpreters [?, ?]. Interpreting [?]. Interrogation [?]. Interrogators [?]. Interval [?]. Interview [?, ?]. Interviews [?]. Interwar [?]. intractability [?]. Intractable [?]. Intrigue [?]. Introducing [?]. **Introduction** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Intuitive [?]. invariant [?, ?, ?, ?, ?]. Invention [?]. Inventions [?]. Inventor [?, ?, ?]. Inverse [?, ?, ?, ?, ?]. Inverses [?]. Investigations [?]. invisible [?]. Involved [?]. IoT [?]. IRA [?, ?]. Iran [?]. Iraq [?]. Iron [?]. Ironies [?]. ISBN [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Islamic [?]. Island [?, ?, ?]. Isle [?]. Isomorphs [?]. Israel [?, ?, ?, ?, ?]. Israeli [?, ?]. Issues [?, ?]. Italian [?, ?, ?, ?]. Italy [?]. Ithaca [?]. iv [?, ?, ?, ?, ?].

J

[?, ?].  
J. [?, ?]. J.-J [?]. Jacek [?]. Jack  
[?, ?, ?, ?]. Jackie [?]. Jackson [?, ?, ?, ?].  
Jacopo [?]. Jak [?]. James  
[?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Jan  
[?, ?, ?, ?, ?]. Janice [?]. January [?].  
Japan [?, ?, ?, ?]. Japanese  
[?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Jason [?].  
Javier [?]. Jean [?, ?]. Jefferson [?, ?, ?].  
Jefferson/Bazeries [?, ?]. Jeffrey [?].  
Jeffreys [?]. Jeffreys-Jones [?]. Jenkins  
[?]. Jennings [?]. Jeon [?]. Jerry [?].  
Jerzy [?]. Jevon [?]. Jill [?]. Jim [?].  
Jimmy [?]. JN [?, ?, ?, ?]. JN-25 [?, ?].  
JN-25A1 [?]. JN-25B [?]. JN25 [?]. Joan  
[?]. Joaquín [?]. Jochemsz [?]. Joe  
[?, ?, ?]. Joel [?, ?, ?]. Johann [?, ?].  
Johannes [?, ?]. John  
[?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].  
Johnson [?, ?, ?, ?, ?]. Johnston [?]. Joint  
[?, ?]. Jonathan [?, ?]. Jones [?]. José [?].  
Joseph [?]. Joshua [?]. Joss [?]. Josse [?].  
Journal [?, ?]. Journeys [?]. joy [?, ?]. Jr

Law [?, ?, ?, ?, ?, ?, ?, ?, ?]. Lawrence [?]. LC [?, ?]. LC-836MN [?]. LC-weak [?]. Leander [?]. Learned [?]. learning [?, ?]. Lectures [?]. Led [?]. Lee [?, ?]. Leeuw [?]. Leeuwen [?]. Legacy [?, ?, ?]. Legendary [?]. Leibniz [?]. Length [?, ?, ?, ?, ?, ?]. Leo [?, ?]. Leslie [?]. less [?]. Lessons [?, ?]. Lester [?, ?]. Letter [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Letters [?, ?, ?, ?, ?, ?, ?, ?]. level [?]. Levine [?]. levitation [?]. Lewin [?]. LFSRs [?]. Li [?]. Liberty [?, ?, ?, ?, ?, ?]. Library [?]. LICID [?]. lies [?]. Lieutenant [?]. Life [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Light [?]. lightweight [?, ?, ?]. like [?]. Liliput [?]. Limited [?]. Lindemann [?]. Line [?, ?, ?]. Linear [?, ?, ?, ?, ?, ?, ?, ?, ?]. linearity [?]. Linguistic [?, ?]. linguistics [?]. Linguists [?, ?]. Link [?, ?]. Lisbon [?]. listening [?, ?]. Lists [?]. Literacy [?]. Literature [?, ?]. Littlewood [?, ?, ?]. Liza [?]. Lobsters [?]. Location [?]. Loepp [?]. Logic [?]. London [?, ?, ?]. Long [?, ?, ?, ?, ?, ?]. long-term [?, ?]. Look [?]. Looking [?]. López [?]. López-Brea [?]. Lorenz [?, ?, ?]. Lost [?, ?, ?, ?, ?, ?]. Lotos [?, ?]. Louis [?, ?]. Love [?, ?, ?, ?, ?, ?, ?]. Lovell [?]. Lovers [?, ?]. Lovett [?]. Low [?, ?, ?]. Low-Complexity [?]. low-rank [?]. low-tech [?]. LSB [?]. LSFR [?, ?]. Ltd [?, ?]. Lu [?]. Luby [?]. LUCIDA [?]. LUCIFER [?, ?]. Ludlings [?]. Ludwig [?]. Luftwaffe [?, ?]. lugs [?]. Luigi [?]. Luke [?]. Luneburg [?]. lured [?]. Lurline [?]. Lustre [?]. Lyndon [?, ?].

M

[?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].  
M-125 [?]. M-134-C [?]. M-209  
[?, ?, ?, ?, ?, ?]. M-294 [?]. M-325 [?].  
M.I.T. [?, ?]. M4 [?]. MA [?]. MA4210  
[?]. Macbeth [?]. Machina [?, ?].  
Machine





[?]. Perera [?]. perfect [?]. Performance [?, ?, ?]. Perils [?]. Perimeter [?]. Period [?, ?, ?]. Periodic [?, ?, ?, ?, ?, ?, ?, ?]. Permutation [?, ?, ?, ?, ?, ?, ?, ?]. Permutations [?, ?, ?, ?]. Persian [?]. Person [?]. Personal [?, ?]. Perspective [?, ?]. Perspectives [?, ?]. Pessimistic [?]. Peter [?, ?, ?, ?, ?]. Petersen [?]. Petitcolas [?]. PFC [?]. PFC-CTR [?]. PFC-OCB [?]. PGP [?]. Phil [?]. Philby [?]. Philip [?]. Phillips [?]. Philosophical [?]. Phishing [?]. Photo [?]. Photographic [?]. Phrase [?]. Phrase-verified [?]. PICO [?]. Pictorial [?, ?]. Pictures [?]. Piece [?, ?]. Pietro [?]. Pin [?]. Pines [?]. Pinpointing [?]. pins [?]. Pioneer [?]. Pipher [?]. pixel [?]. Plaintext [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Plan [?]. Play [?, ?, ?, ?]. Playfair [?, ?, ?]. Playright [?]. Pleads [?]. Pletts [?]. Plugboard [?, ?]. Pluggable [?]. Pocket [?, ?, ?, ?]. Poe [?, ?]. poem [?]. Poetry [?]. Point [?, ?]. Point-Of [?]. Points [?, ?, ?]. Poles [?, ?]. Policy [?, ?, ?]. Polish [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Political [?]. Polyalphabetic [?, ?, ?, ?, ?, ?]. Polygraphic [?]. polynomial [?, ?]. Polynomials [?, ?, ?]. Pond [?]. Pont [?, ?]. Population [?]. Porzio [?]. Possible [?, ?, ?]. Post [?, ?, ?, ?, ?, ?, ?, ?, ?]. Post-Quantum [?, ?]. post-World [?]. Postage [?]. Postal [?]. postgraduate [?]. Postings [?, ?]. POTUS [?]. POTUS-Prime [?]. £15.00/\$23.60 [?]. POW [?]. Power [?, ?, ?, ?, ?]. POWs [?]. Poznań [?]. pp [?, ?, ?, ?, ?, ?, ?]. Practical [?, ?, ?, ?, ?]. Practice [?, ?, ?, ?, ?]. Practices [?]. practitioners [?]. pracy [?]. Praham [?]. Pre [?]. Pre-Pearl [?]. Preliminary [?, ?]. Prelude [?, ?]. Prentice [?, ?]. Prepared [?]. preserving [?]. Press [?, ?, ?, ?, ?, ?, ?]. Press/Random [?]. Pretext [?]. Price [?]. Primality [?, ?]. Primary [?]. Prime [?, ?]. Primer [?, ?]. primes [?, ?]. Primitive [?]. Principal [?]. Principle [?]. Principles [?, ?, ?, ?, ?]. prior [?]. Prisoners [?, ?]. Privacy [?, ?, ?, ?, ?, ?, ?, ?]. Private [?, ?]. Prize [?]. Pro [?]. Probabilistic [?]. Probability [?]. Probe [?]. Probed [?]. Problem [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Problems [?, ?, ?, ?, ?, ?]. Procedures [?]. Proceedings [?]. Processes [?]. Processing [?, ?, ?, ?, ?, ?, ?]. produced [?]. Product [?]. Production [?]. Prof [?, ?, ?]. Professional [?, ?]. Professor [?]. proficiency [?]. Program [?, ?]. Programming [?, ?]. Progress [?]. prohibition [?]. Project [?, ?, ?, ?, ?, ?, ?]. Project-based [?]. Prometheus [?]. Proof [?]. Propaganda [?]. Properties [?, ?]. Proposal [?]. proposals [?]. Proposed [?, ?, ?, ?, ?, ?]. propositions [?]. Protecting [?, ?]. Protection [?, ?, ?, ?, ?]. Proto [?]. Proto-Enigma [?]. Protocol [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Protocols [?, ?]. provable [?]. Provably [?]. Pseudo [?, ?, ?, ?]. Pseudo-Random [?, ?, ?]. Pseudorandom [?, ?]. Public [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Public-Key [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Publications [?, ?]. Published [?, ?, ?]. Publishing [?, ?, ?, ?, ?, ?]. Pueblo [?, ?]. Pulitzer [?]. Pulp [?]. Punitive [?]. Purple [?, ?, ?, ?, ?, ?, ?]. Pusan [?]. Putative [?]. Puzzle [?, ?, ?, ?, ?, ?]. Puzzles [?]. PVSS [?]. Pyry [?, ?]. Pythagorean [?]. Q. [?]. Qaeda [?]. QR [?]. Quadratic [?, ?, ?, ?]. Quantum [?, ?, ?, ?, ?, ?]. Quasigroups [?, ?, ?, ?, ?, ?]. quaternions [?]. Queen [?]. quest [?]. Question [?]. Questions [?]. Quick [?]. Quinn [?]. Quirantes [?]. Quisquater [?]. Quote [?, ?]. quotients [?].

R [?, ?, ?, ?]. Rabid [?]. Rabin [?]. Race [?, ?]. Rackoff [?]. Radio [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Rail [?]. Ralph [?, ?]. RAM [?]. Ramón [?]. Ramsden [?]. Random [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Random-Key [?]. Randomness [?]. Randy [?]. rank [?]. Rapa [?]. Rapid [?, ?]. Rasterschlüssel [?, ?]. Ratcliff [?]. Raton [?]. Raymond [?]. RC4 [?]. Re [?, ?, ?]. Re-Run [?]. Read [?, ?]. Reader [?]. Reading [?, ?, ?, ?]. Ready [?]. Ready-Made [?]. Real [?, ?, ?, ?, ?, ?, ?, ?, ?]. Real-Time [?]. Realizing [?, ?]. Rear [?]. Rebecca [?]. Rebus [?]. Receive [?]. Reciprocal [?, ?]. Reciprocity [?]. Recoding [?]. Recognition [?, ?, ?, ?, ?]. Recognized [?]. Recognizing [?]. Recollections [?]. Recommendation [?]. recommendations [?]. Reconciliation [?]. reconstructed [?]. Reconstruction [?, ?, ?, ?]. Record [?, ?, ?, ?, ?]. Records [?, ?, ?, ?, ?, ?]. Recovered [?, ?, ?]. Recovering [?, ?]. Recovery [?, ?, ?]. Recursive [?, ?, ?, ?, ?]. Red [?]. Redditch [?]. Reducing [?]. Redundancy [?, ?, ?, ?]. Reed [?]. Reeds [?]. Reference [?, ?]. Reflections [?, ?, ?, ?]. Reflective [?]. Reflector [?, ?, ?, ?]. Reform [?]. Regarding [?, ?]. Register [?, ?, ?, ?, ?]. registers [?]. Reich [?, ?]. Reihenschieber [?]. Reintroduction [?]. Rejewski [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Related [?, ?, ?, ?]. Related-key [?]. Relation [?]. Relationship [?, ?]. Relative [?, ?]. Relatives [?]. Relaxation [?]. Release [?]. releases [?]. Remark [?]. Remarkable [?, ?]. Remarks [?, ?, ?, ?, ?, ?]. REME [?]. Remember [?]. remembered [?]. Reminiscence [?]. Reminiscences [?]. Remote [?, ?, ?, ?]. Rempe [?]. Rempe-Gillen [?]. Renaissance [?, ?]. Rent [?]. Reorganization [?]. repeats [?].

Rites [?]. Ritz [?]. River [?, ?].  
Riverbank [?, ?, ?, ?, ?, ?, ?, ?]. Riyadh [?].  
Rózycki [?, ?]. Road [?, ?, ?, ?]. roaming [?].  
Rob [?]. Robert [?, ?, ?]. Roberts [?].  
Robin [?, ?, ?]. Robust [?]. Rochefort [?, ?, ?].  
Rochford [?]. Rockex [?]. Roger [?].  
Rohaly [?, ?]. Rohonc [?, ?, ?]. Role [?, ?].  
Romanian [?]. Ron [?]. Ronald [?].  
rongorongo} [?, ?, ?, ?, ?, ?]. Roof [?, ?].  
Room [?, ?, ?, ?, ?]. Roosevelt [?, ?, ?].  
Roper [?]. Rosario [?]. Rose [?, ?]. Ross [?, ?]. rotation [?, ?]. ROTERM [?].  
Roth [?]. Rotor [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Rotors [?, ?, ?]. Round [?, ?]. Row [?]. Roy [?].  
Royal [?, ?]. RSA [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].  
RSA-cryptosystem [?]. RT [?, ?].  
RT-OCFB [?]. Rubik [?]. Rudyard [?].  
Rule [?, ?]. Ruled [?]. Rules [?, ?]. Run [?, ?]. Runic [?, ?]. Running [?, ?, ?, ?, ?, ?].  
Russell [?]. Russia [?, ?]. Russian [?, ?, ?, ?, ?, ?, ?]. Russo [?]. Ryan [?].  
  
S [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. S-Box [?, ?]. S-boxes [?]. S. [?]. S./CB [?]. SA [?].  
Sacco [?]. Saddle [?, ?]. Safford [?, ?].  
Saga [?, ?]. Sale [?]. Salvo [?]. same [?, ?].  
same-letter [?]. Samples [?]. Samuel [?, ?, ?]. San [?]. Sanborn [?]. ‘Santiago’ [?]. Sarah [?]. Sarasvatī [?]. SAS [?].  
SAS-SIP [?]. Satire [?, ?]. Sator [?].  
SAUDI [?]. Savage [?]. say [?]. Sayers [?].  
SCAG [?]. Scalar [?]. SCAMP [?]. scan [?]. Scatter [?]. Scavenger [?]. scenario [?, ?]. scenarios [?]. Schedules [?].  
Scheme [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].  
Schemes [?, ?, ?, ?]. Scheuble [?].  
Schieber [?]. Schmeh [?, ?, ?].  
Scholarship [?]. Scholastic [?]. School [?, ?, ?].  
Schriften [?, ?]. Schuster [?, ?].  
Schwartz [?]. Science [?]. Scientific [?].  
Score [?]. Scotch [?]. Scott [?, ?]. Script







