

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
FAX: +1 801 581 4148

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

05 September 2023
Version 3.73

Title word cross-reference

(t, m) [?]. (t, n) [?, ?]. \$10.00 [?]. \$12.00 [?]. 128 [?]. \$139.99 [?]. \$15.00 [?]. \$16.95 [?, ?]. \$16.96 [?]. \$18.95 [?]. \$24.00 [?]. \$24.00/\$34 [?]. \$24.95 [?, ?]. \$26.95 [?]. \$29.95 [?]. \$30.95 [?]. \$38.00 [?]. \$39 [?]. \$43.39 [?]. \$45.00 [?]. \$5.95 [?]. \$54.00 [?]. \$54.95 [?]. \$54.99 [?]. \$6.50 [?]. \$6.95 [?]. \$69.00 [?]. \$69.95 [?]. \$75.00 [?]. \$89.95 [?]. th [?]. A [?]. A^3 [?, ?]. χ [?]. H [?]. k [?, ?, ?]. M [?, ?, ?]. M^3 [?]. n [?, ?, ?]. q [?]. -ary [?]. -Bit [?]. -error [?]. -out-of- [?, ?]. -sequences [?]. -tests [?]. 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 [?, ?, ?, ?].

3 [?, ?, ?, ?]. 3/4in [?, ?]. 30 [?]. 310 [?, ?, ?, ?, ?, ?, ?, ?]. 312 [?]. 325 [?]. 3336 [?]. 340 [?]. 35 [?]. 36 [?]. 3rd [?].

4 [?, ?, ?]. 40 [?]. 44 [?]. 45 [?]. 45th [?]. 47 [?]. 4in [?, ?].

5.0 [?]. 50 [?]. 52 [?, ?, ?]. 520 [?]. 57 [?, ?]. 5th [?].

6 [?, ?]. 67 [?]. 67/97 [?, ?, ?].

7 [?, ?]. 77-Year [?].

8 [?]. 80 [?, ?]. '82 [?]. 83 [?, ?]. 836MN [?]. 849th [?, ?]. 85 [?]. 89 [?].

9 [?, ?, ?, ?]. 9/11 [?, ?, ?, ?]. 97 [?, ?, ?]. 9761 [?]. 978 [?, ?, ?, ?, ?, ?, ?].

978-0-19-874783-3 [?].
978-0-7509-7885-9 [?].
978-0-8218-9883-3 [?].
978-0-9557164-1-6 [?].
978-1-3988-1244-4 [?].
978-1-4704-1048-3 [?].
978-1-78155-759-4 [?].
978-1-7988-8747-9 [?].
978-1-7988-8811-7 [?].
978-3-319-53278-3 [?].

Āryabhata [?].

A-22 [?]. A-5 [?]. A. [?, ?]. A.6 [?]. AAAS [?]. Abraham [?]. Abrutat [?]. Abuse [?]. Abwehr [?, ?, ?]. academic [?]. Accelerating [?]. Access [?]. Accessible [?]. Accident [?]. Accidental [?]. Account [?, ?]. Accounts [?, ?, ?]. Accumulated [?]. Achievements [?]. Acoustical [?]. Across [?, ?]. Act [?, ?, ?]. Action [?]. Actions [?]. Activist [?]. Activities [?]. Acts [?]. Adam [?]. adaptive [?].

[?, ?, ?]. Dictionary [?, ?]. Did
[?, ?, ?, ?, ?]. Dienst} [?]. Dies [?, ?].
differencing [?, ?]. Different [?].
Differential [?, ?, ?, ?, ?, ?, ?].
Differential-Style [?]. differentials [?].
Diffie [?]. diffusion [?]. Digital
[?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
Digraphic [?]. Dilly [?, ?, ?]. Dingman
[?]. Dingyi [?]. Diplomacy [?, ?].
Diplomat [?]. Diplomatic
[?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Direction [?].
Directional [?]. Disclose [?]. Disclosed
[?]. disclosure [?]. Discovered [?].
Discovery [?, ?, ?]. discrete [?].
discussion [?]. Disk [?, ?]. Disks [?, ?].
Dispatch [?]. Display [?]. Dispute [?].
Dissenting [?]. distance [?].
Distinguished [?]. Distinguishers [?].
Distributed [?, ?, ?]. Distribution
[?, ?, ?, ?, ?]. distributions [?]. Divide
[?, ?]. Divide-and-Conquer [?]. Divisions
[?]. DNA [?]. DNA-Based [?]. Do [?].
'Doc [?]. Document [?, ?]. Documentary
[?, ?]. Documents [?, ?, ?]. Dodgson
[?, ?]. Dodo [?]. does [?, ?]. Doing [?].
Dominic [?]. Donald [?, ?]. Dönitz [?, ?].
Donovan [?]. Don't [?, ?]. Dooley
[?, ?, ?]. Dot [?, ?]. 'Double
[?, ?, ?, ?, ?, ?, ?]. Double-Base [?].
Doubleday [?]. Down [?, ?, ?]. DPEPE
[?, ?]. DPJO [?, ?]. Dr. [?, ?, ?]. Draft [?].
Dragon [?]. Drawbacks [?]. Drazin
[?, ?, ?, ?]. Driscoll [?, ?, ?]. Dropping [?].
DSA [?]. Duits [?, ?]. Duke [?]. Dunedin
[?]. Dunin [?]. duplication [?]. During
[?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
Dustin [?]. Dutch [?, ?, ?, ?, ?]. Duties
[?]. Dynamic [?, ?, ?, ?].

E. [?]. Earliest [?, ?, ?]. Early
[?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
Easier [?]. East [?, ?, ?]. Eastcote [?].
Easter [?, ?]. Eastern [?]. Eavesdroppers
[?]. Eavesdropping [?, ?, ?, ?, ?, ?, ?, ?].

One-Way [?, ?]. Online [?, ?]. Only [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. OP [?, ?]. OP-20-G [?, ?]. Open [?]. Openness [?]. Opens [?]. Operating [?]. Operation [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Operational [?]. Operations [?, ?, ?, ?, ?, ?]. Operator [?, ?, ?, ?]. Opinion [?, ?]. Opportunities [?]. Optimal [?]. Optimization [?]. Optimized [?]. oracle [?]. Oral [?]. Order [?, ?, ?, ?, ?]. Organisational [?]. Organization [?, ?, ?, ?, ?, ?, ?]. Organizations [?]. organized [?]. Orient [?]. Oriental [?]. Origin [?, ?]. Original [?, ?]. Origins [?, ?, ?, ?, ?, ?, ?, ?]. OSS [?]. Other [?, ?, ?, ?, ?, ?, ?, ?, ?]. OTP [?, ?]. Ottoman [?]. Out-of-Band [?]. Outdated [?]. Outline [?]. Outreach [?]. Outstanding [?]. Outstations [?]. outwitted [?]. Overlapping [?]. Overlaps [?]. Overview [?, ?, ?, ?, ?, ?]. Own [?, ?]. Oxford [?].

Peace [?]. Peacet ime [?]. Pearl [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Pearson [?, ?, ?]. Pedagogical [?]. Pei [?]. Pelling [?]. Pend ergass [?]. Pennsylvania [?]. Pensionary [?]. Pentagon [?, ?]. Penumbra [?, ?, ?]. People [?, ?]. perceptions [?]. Percy [?]. Perera [?]. 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 [?].
 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
 [?]. Pyry [?, ?]. Pythagorean [?].
 Qaeda [?]. QR [?]. Quadratic [?, ?, ?, ?].
 Quantum [?, ?, ?, ?, ?]. Quasigroups
 [?, ?, ?, ?, ?]. quaternions [?]. 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 [?]. 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 [?].
 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 [?, ?, ?, ?].

[?]. **yesterday** [?]. **Yoo** [?]. **York** [?, ?, ?, ?, ?]. **Young** [?, ?, ?, ?, ?]. **Younger** [?]. **Yudhijit** [?]. **Yung** [?].

Z [?, ?, ?, ?, ?]. **Z30** [?]. **Zachod** [?]. **Zdzislaw** [?, ?, ?, ?]. **Zeilinger** [?]. **Zendia** [?]. **Zero** [?, ?]. **Zero-Knowledge** [?]. **Zhou** [?]. **Zimmermann** [?, ?, ?, ?]. **Zodiac** [?]. **Zodiac-340** [?]. **Zullo** [?, ?]. **Zuse** [?]. **Zygaliski** [?, ?, ?, ?, ?].