

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

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

20 August 2025
Version 4.118

Title word cross-reference

(mod p) [?]. $1/2 + 1\text{Poly}(\log N)$ [?]. \$13.95 [?]. \$16.95 [?]. \$19.95 [?]. $25 \cdot 10^9$ [?]. $2^m \pm 1$ [?]. $2^n \pm 1$ [?]. $2n$ [?]. \$34.95 [?]. \$35.00 [?, ?]. \$49.95 [?, ?]. B [?]. D [?]. F_q [?]. $\frac{1}{2} + \frac{1}{\text{poly}(\log N)}$ [?]. $\text{GF}(2^n)$ [?]. $\text{GF}(p)$ [?, ?]. $\text{GF}(p^2)$ [?]. l [?]. M^3 [?]. $\text{GF}(2^m)$ [?]. $\text{GF}(p^n)$ [?]. N [?, ?, ?]. $n = 2$ [?]. NC^0 [?]. $O(\log n)$ [?]. $O(\log n)$ [?]. -Bit [?]. -ciphered [?]. -tree [?]. 0 [?, ?]. 0-471-90934-3 [?]. 0-7248-0274-6 [?]. 10 [?, ?]. 1004 [?]. 1040 [?]. 1113 [?]. 112 [?, ?]. 113 [?]. 12 [?]. 121 [?, ?]. 1413 [?].	1421 [?]. 1474 [?]. 1500-1815 [?]. 15th [?]. 18 [?]. 1917 [?]. 1938 [?, ?]. 1941 [?]. 1942 [?]. 1943 [?, ?]. 1944 [?]. 1945 [?]. 1975 [?]. 1976 [?]. 1977 [?]. 1981 [?]. 1982 [?]. 1983 [?, ?, ?]. 1984 [?, ?]. 1985 [?]. 1986 [?, ?]. 1987 [?, ?, ?]. 1988 [?]. 2 [?, ?]. 203-181 [?, ?]. 205 [?, ?]. 209 [?]. 20th [?]. 21 [?]. 232 [?]. 23rd [?]. 25 [?]. 25th [?, ?, ?]. 26th [?]. 27th [?]. 28th [?]. 293 [?]. 3 [?]. 30th [?]. '32 [?]. 32G [?, ?]. 36 [?, ?]. 38 [?]. 39 [?]. 4 [?, ?]. 536 [?].
---	---

6 [?, ?]. 644 [?]. 6th [?, ?].

8-bit [?]. 80b [?]. 80g [?]. '82 [?, ?]. 82d [?]. 84 [?]. '85 [?]. '86 [?]. '87 [?, ?, ?, ?, ?]. 87-872-0086-4 [?]. '88 [?]. '89 [?, ?, ?].

90c [?]. 912 [?]. 93 [?]. 931 [?]. 96 [?]. 989 [?].

A. [?]. AAECC [?]. AAECC-6 [?].
abbatis [?, ?, ?]. ABC [?]. Above [?].
Abraham [?]. Absence [?]. absentibus [?, ?]. absolute [?]. Abstract [?, ?, ?, ?, ?, ?, ?, ?, ?]. academic [?].
Academy [?]. accepts [?]. Access [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. accessed [?]. Account [?, ?, ?, ?]. accuracy [?, ?].
ACE [?]. Achieving [?, ?, ?]. ACM [?, ?, ?, ?, ?, ?, ?]. acontismologia [?].
Acquired [?, ?]. 'Action [?]. Activities [?]. ad [?, ?, ?]. Ada [?, ?]. Adaptive [?].
added [?]. adding [?]. Addition [?, ?].
additional [?, ?]. additive [?]. address [?].
addresses [?, ?]. ADFGVX [?, ?].
Adleman [?, ?, ?, ?]. administrator [?].
Adobe [?]. ADP [?]. Advanced [?, ?, ?, ?]. Advances [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
adventure [?]. Advisor [?]. Aerospace [?]. AFSC [?]. After [?]. Against [?, ?].
Age [?, ?, ?]. Agencies [?]. agency [?, ?, ?, ?, ?]. ages [?]. Agreement [?].
Ahituv [?]. al [?, ?, ?]. al-'Arab [?].
al-Maskhutah [?]. al-mu'amma [?].
al-ta'miyah [?]. Alan [?, ?]. Alberta [?].
algebra [?, ?]. Algebraic [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
algebraic-code [?]. algebraic-coded [?].
Algorithm [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
Algorithms [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
?, ?, ?, ?]. alios [?]. Alive [?]. Allied [?].
Allies [?, ?, ?, ?, ?]. Allocation [?, ?].

Alone [?]. Alphabet [?]. alphabétiques [?]. alphabets [?, ?]. Alsbalden [?]. also [?]. Alternating [?, ?]. alternatives [?].
always [?]. Amer [?]. America [?, ?, ?].
American [?, ?, ?, ?, ?]. ammunition [?].
among [?]. amplification [?]. Amsterdam [?, ?, ?]. Analog [?, ?, ?, ?, ?]. analogie [?].
analogy [?]. Analyse [?]. analyses [?].
Analysis [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Analytical [?, ?, ?, ?, ?].
Analyzing [?, ?]. ancient [?].
Anecdotes [?]. Angeles [?]. angels [?].
Anglica [?]. animi [?, ?]. Annex [?].
Anniversary [?]. Annotated [?, ?, ?, ?].
Annual [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
Answering [?]. Antipalindromic [?]. any [?, ?, ?, ?].
aperiendi [?, ?]. APL [?, ?, ?, ?, ?].
Apparatus [?, ?].
apparently [?]. appendix [?].
Application [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Applications [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
?, ?, ?, ?, ?, ?, ?, ?, ?]. Applied [?, ?, ?, ?, ?].
approach [?, ?, ?, ?, ?].
Approaching [?]. approximation [?].
April [?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
'Arab [?]. Arabicis [?]. Arbitrary [?, ?].
Archaeological [?]. architectural [?].
Architecture [?, ?]. architectures [?].
area [?, ?]. Arguments [?]. arise [?].
Arithmetic [?, ?]. Army [?].
Arnoldum [?]. Array [?]. Ars [?, ?, ?].
arsque [?]. art [?, ?, ?]. Arte [?]. Articles [?, ?, ?, ?].
artificia [?]. Artificial [?].
ASCII [?]. Asimov [?]. Aspray [?].
Assessment [?, ?]. Assigning [?]. assisted [?].
Association [?, ?]. Associative [?, ?].
Assumption [?]. astounding [?].
Asymmetric [?, ?, ?, ?, ?].
asymptotically [?]. AT&T [?]. Atkin [?].
Atlantic [?, ?]. Atlantik [?]. atque [?].
attack [?, ?, ?, ?, ?, ?, ?, ?]. Attacks [?, ?, ?, ?].
attributed [?, ?]. aucta [?].

change [?]. Channel [?, ?, ?, ?, ?].
 Channels [?, ?, ?]. Character [?].
 characteristic [?]. characteristics [?].
 characters [?]. checkers [?]. checking [?].
 Checks [?]. checksum [?, ?]. chemical [?].
 chess [?]. Chicago [?, ?, ?, ?].
 Chifferbyråernas [?]. chiffrée [?]. chiffres
 [?]. Chiffriersysteme [?].
 Chiffrierverfahren [?]. Chinese [?, ?, ?].
 Chinesische [?]. Chip [?, ?, ?, ?, ?]. chips
 [?]. Chosen [?, ?, ?]. Chosen-Message [?].
 chosen-plaintext [?]. chrestomathy [?].
 Christ [?]. cialach [?]. Cicco [?]. Cifra [?].
 Cipher [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?]. cipher-writing
 [?]. ciphered [?]. Ciphers [?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?]. Ciphertext [?, ?]. Circle [?]. circuits [?].
 citations [?, ?, ?]. City [?]. civil [?].
 Clandestina [?]. clarissime [?]. Clark [?].
 Class [?, ?]. classes [?]. classic [?].
 classical [?]. Clauis [?, ?, ?, ?]. clear [?].
 Clemson [?]. climax [?]. clues [?]. CMOS
 [?]. Co [?, ?]. Code
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Code-Breaking [?]. Codebreaker [?].
 Codebreakers [?, ?, ?, ?, ?].
 Codebreaking [?]. coded [?]. Codes
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?]. Codewords [?]. Coding
 [?, ?, ?, ?, ?, ?, ?, ?, ?]. Cogitata [?].
 Cognitive [?]. Coin [?, ?, ?, ?].
 Coincidence [?, ?, ?]. Collected [?].
 collection [?]. collections [?]. collective
 [?]. College [?]. Collision [?].
 Collision-free [?]. Colloquium [?, ?].
 Colonel [?, ?]. Colossus [?, ?, ?, ?, ?, ?, ?].
 column [?, ?]. columnar [?, ?].
 combinations [?]. Combinatorial [?].
 combined [?]. Combining [?]. Command
 [?]. Comment [?]. Commentaries [?].
 Comments [?, ?, ?, ?]. Committee [?].
 commonly [?]. communicating [?].
 Communication [?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Communications [?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Communities
 [?, ?]. compact [?]. Companies [?].
 Company [?, ?, ?]. Compcon [?, ?].
 Competition [?]. complete [?].
 Completeness [?, ?, ?]. Complexity
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Compliance [?, ?]. composed [?].
 composite [?]. composition [?].
 Comprehensive [?]. Compression
 [?, ?, ?]. Compromise [?]. Computation
 [?, ?, ?, ?, ?, ?]. Computational [?, ?].
 Computationally [?, ?]. Computations
 [?, ?]. compute [?]. Computer
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?]. Computerized
 [?]. Computers
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Computing [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?]. conceal [?].
 concealability [?]. concealed [?]. concept
 [?]. Concepts [?, ?]. Concerning [?, ?, ?].
 concinnatae [?]. concise [?]. conclusion
 [?]. concrete [?]. Conditionals [?].
 Conference [?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 conferring [?, ?]. confidentiality [?].
 confidentially [?]. Confinement [?].
 conglobatae [?]. Congress [?].
 congruence [?]. congruences [?].
 congruential [?, ?, ?, ?]. conjecture
 [?, ?]. conjurationes [?]. Connection
 [?, ?]. Consensus [?]. Consequences [?].
 Considerations [?, ?]. Constant [?, ?].
 Constant-Time [?]. Construct [?, ?, ?].
 constructing [?, ?]. contain [?].
 contained [?]. containing [?, ?].

contenant [?]. Continued [?, ?].
 Continuously [?]. contracts [?].
 Contribution [?]. Contributions [?].
 Control [?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Controlled [?, ?, ?]. Controlling [?, ?].
 Conventional [?, ?]. conversations [?].
 convoy [?, ?]. coprocessing [?].
 Coprocessor [?]. core [?]. Corporation
 [?]. Correcting [?, ?]. correction [?, ?, ?].
 Corrections [?]. correctness [?, ?, ?].
 Correlated [?]. Correlation [?].
 Correlation-Immunity [?].
 correspondance [?]. Corrigendum [?].
 COST [?, ?]. COST-11 [?]. Council [?].
 counter [?]. counterintelligence [?]. coup
 [?]. Cours [?, ?]. Course
 [?, ?, ?, ?, ?, ?, ?, ?, ?]. Covert
 [?, ?, ?]. crack [?, ?]. cracked [?].
 Cracking [?, ?, ?]. craft [?]. creating [?].
 crime [?]. criteria [?]. Criterion [?].
 Critical [?, ?, ?]. critique [?]. crittografia
 [?, ?]. crossword [?]. crosswords [?].
 crypt [?, ?]. crypt-ology [?].
 Cryptanalysis
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Cryptanalyst [?, ?, ?]. Cryptanalysts
 [?]. Cryptanalytic [?, ?, ?, ?].
 Cryptanalytical [?]. cryptananyis [?].
 cryptic [?, ?]. CRYPTO
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Crypto-ease [?]. Crypto-Functions [?].
 Cryptogram [?]. Cryptograms [?, ?, ?].
 cryptograph [?, ?, ?]. Cryptographer
 [?, ?]. Cryptographia [?, ?, ?].
 Cryptographic
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Cryptographically [?, ?, ?, ?, ?].

Cryptographie
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Cryptography [?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 cryptography
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Cryptologia [?]. Cryptologic [?, ?, ?].
 cryptologist [?, ?]. Cryptology
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 cryptology [?]. cryptomenyitics [?].
 Cryptopak [?]. cryptoprocessor [?].
 Cryptoprotocols [?, ?]. Cryptosystem
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Cryptosystems
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 CTTE [?]. Cuckoo [?]. curiosa [?].
 Current [?]. Curve [?, ?]. Curves [?, ?, ?].
 Curzon [?]. custom [?, ?, ?]. Cyber [?, ?].
 Cycle [?, ?]. Cyclic [?]. Cypher
 [?, ?, ?, ?, ?, ?, ?, ?].
 D [?, ?, ?, ?]. D. [?]. D0L [?]. D0L-T0L
 [?]. D1 [?]. D4 [?]. Dabbling [?].
 Dalgarno [?]. Dallas [?]. damage [?].
 damnata [?]. dan [?]. dans [?]. Dante [?].
 Data [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Data
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].

Dirichlet [?]. **disaster** [?, ?]. **Discrete** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Discretionary** [?, ?, ?]. **discussion** [?]. **disk** [?]. **Dispersal** [?]. **dissertation** [?, ?]. **distance** [?, ?]. **Distributed** [?, ?, ?, ?, ?, ?]. **Distributed-protocol** [?]. **Distribution** [?, ?, ?, ?, ?, ?]. **Dits** [?]. **Divergence** [?]. **Divers** [?]. **Divi** [?]. **Division** [?]. **divisions** [?]. **Dkr** [?]. **Dn** [?, ?]. **do** [?, ?]. **Document** [?]. **documents** [?]. **DOE** [?]. **does** [?]. **DOL** [?]. **Donald** [?]. **Door** [?, ?]. **Doorbell** [?]. **Doran** [?]. **double** [?]. **Dr.** [?]. **Draft** [?, ?]. **Dual** [?]. **Duke** [?]. **Dupont** [?]. **durch** [?]. **during** [?, ?, ?]. **Dutch** [?]. **Dvorak** [?]. **Dynamic** [?, ?, ?]. **dzialan** [?].

E. [?]. Early [?, ?, ?, ?]. Eary [?]. ease [?].
 East [?]. Easy [?, ?, ?]. Eavesdropper [?].
 ECL [?]. écriture [?, ?]. écritures [?].
 ECS [?]. ed [?]. Edgar [?]. Edited [?].
 Editor [?, ?]. Edmonton [?]. EDP [?]. eds
 [?]. Education [?, ?]. Educators [?].
 Edwards [?]. Effects [?]. Efficient
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. efforts
 [?]. EFTs [?]. Egg [?]. Egyptian [?, ?].
 Eighteenth [?]. Eighth [?]. einem [?].
 einiger [?]. Electrical [?]. Electronic
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Electronics
 [?, ?, ?]. Elementary
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Elements [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Elliptic [?, ?, ?, ?, ?]. Elsevier [?, ?].
 elucidation [?]. elusa [?]. Embedding
 [?, ?]. emc [?, ?]. emc/rfi [?, ?]. emp
 [?, ?]. employed [?]. empregados [?].
 emulates [?]. enciphered [?, ?].
 Enciphering [?, ?, ?]. Encipherment
 [?, ?, ?, ?, ?, ?, ?, ?, ?]. Encrypted
 [?, ?, ?, ?, ?]. Encryption
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]

?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 encryptions [?]. Encryptor [?].
 encryptors [?]. Encyclopedia [?]. End
 [?, ?, ?, ?]. End-to-End [?, ?, ?]. enemy
 [?]. enforcement [?]. engendered [?].
 Engine [?]. Engineering [?, ?, ?].
 Engineers [?]. England [?]. English [?, ?].
 English-jargon [?]. Enhanced [?].
 Enhancement [?, ?, ?]. ENIAC [?].
 Enigma [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?]. enigmatic [?].
 énigme [?]. Entities [?]. Entring [?].
 Entropy [?]. entry [?]. Enumeration [?].
 Environment [?, ?, ?, ?, ?, ?].
 Environments [?, ?, ?]. Epiphanes [?, ?].
 Equality [?]. Equations [?, ?, ?].
 equidistribution [?]. equipment
 [?, ?, ?, ?, ?, ?, ?, ?, ?]. equivalent [?].
 equivocation [?]. era [?, ?]. Ernst [?].
 eroffnen [?]. Errata [?]. Erratum [?].
 Error [?, ?, ?, ?, ?, ?, ?].
 Error-Correcting [?, ?]. Error-correction
 [?, ?]. ErycI [?]. escrire [?]. escrituras [?].
 Escrow [?]. Espionage [?, ?, ?]. essential
 [?]. est [?, ?]. Established [?]. estimation
 [?, ?]. Etherphone [?]. ethics [?].
 Etruscan [?]. etwas [?]. EUROCRYPT
 [?, ?, ?, ?, ?, ?]. European [?]. evaluate
 [?]. Evaluation [?, ?, ?]. evaluations [?].
 Even [?]. Event [?]. ever [?]. evidence [?].
 evolving [?]. ex [?]. examination [?].
 Examined [?]. Excellence [?]. Excerpts
 [?]. Exchange [?, ?, ?, ?, ?]. Execution [?].
 exercise [?, ?]. Exhaustive [?, ?].
 exhibentur [?]. Exhibit [?]. existence
 [?, ?]. Expanded [?]. Expected [?].
 Experimental [?, ?]. Experiments [?].
 Experts [?]. explicantur [?]. exploiting
 [?, ?, ?]. Exponentiation [?]. Expose [?].
 Extended [?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Extensible [?]. extrapolation [?].
 F [?, ?, ?]. F. [?]. F.E.A.L [?]. fabrication
 [?]. facsimile [?]. factor [?, ?, ?]. factored
 [?]. Factoring [?, ?, ?, ?, ?, ?].
 Factorization [?, ?, ?, ?]. Factorizations
 [?, ?, ?]. Factors [?, ?]. Failure [?]. Fair
 [?]. Fall [?, ?]. family [?]. Famous [?]. Far
 [?]. Fast
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Fault [?, ?, ?]. Fault-Tolerant [?, ?].
 Faults [?]. Fear [?]. February
 [?, ?, ?, ?, ?, ?]. Federal [?]. feedback [?].
 Fellowship [?]. ferrne [?]. Feuerstein [?].
 Field [?]. Fields [?, ?, ?, ?, ?, ?, ?, ?].
 fifteen [?]. fifteenth [?]. Fifth [?, ?].
 figures [?]. File [?, ?, ?, ?, ?, ?]. Files
 [?, ?, ?]. Final [?]. Financial [?]. find [?].
 Finerman [?]. Fingerprinting [?]. Finite
 [?, ?, ?, ?, ?, ?, ?, ?, ?]. Finiteness [?].
 FIPS [?, ?, ?, ?]. First
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. fixed
 [?, ?, ?]. FL [?]. Flaw [?]. Flip [?].
 Flip-Flops [?]. Flipping [?, ?]. Flips [?].
 Flops [?]. Florence [?]. Florida [?]. flow
 [?, ?]. Flowers [?]. forecast [?]. Forlag [?].
 form [?, ?]. formal [?, ?]. formulae [?].
 Forum [?]. Foundations
 [?, ?, ?, ?, ?, ?, ?, ?]. Founding [?]. Four
 [?, ?]. fourteenth [?]. Fourth [?, ?].
 Fraction [?]. fractionating [?].
 Fragmentation [?]. framework [?].
 Framingham [?]. France [?]. Francis [?].
 Francisco [?, ?]. Franksen [?, ?, ?, ?].
 französichen [?]. free [?]. freedom [?].
 French [?, ?, ?, ?, ?, ?, ?, ?, ?].
 Friedman [?, ?]. Führungsprobleme [?].
 Function [?, ?, ?, ?]. Functional [?].
 Functions
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Fundamental [?]. Funds [?, ?, ?]. Further
 [?]. Futrelle [?]. Future [?, ?, ?, ?].

G [?, ?]. G. [?]. Gaithersburg [?, ?].
 Galland [?]. Gallica [?]. Galois [?]. Game
 [?, ?, ?]. Games [?]. Gardner [?]. Garland
 [?, ?]. Gateways [?]. gaze [?]. Geheime
 [?, ?]. geheimes [?]. Geheimschriften [?].
 Geleitzugschlachten [?]. General
 [?, ?, ?, ?, ?, ?]. generalis [?, ?].
 Generalized [?, ?, ?]. Generals [?, ?, ?, ?].
 Generate [?, ?, ?, ?]. generated [?, ?].
 generating [?]. Generation
 [?, ?, ?, ?, ?, ?, ?, ?]. Generator
 [?, ?, ?, ?, ?, ?, ?, ?]. Generators
 [?, ?, ?, ?, ?, ?, ?, ?]. genere [?]. geometry
 [?]. George [?, ?]. German
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Germanica [?]. Germany [?, ?]. get [?].
 gewiser [?]. Girls [?]. Girolamo [?].
 Global [?, ?]. GLOBECOM [?]. glossary
 [?]. GMD [?]. Godfather [?]. goes
 [?, ?, ?]. gold [?]. Goldstine [?, ?].
 Goldwasser [?].
 Goldwasser-Killian-Atkin [?]. good
 [?, ?, ?, ?, ?]. Gordon [?]. Government
 [?, ?, ?, ?]. Governmental [?]. Graeca [?].
 Graecis [?]. grand [?]. grande [?]. graph
 [?]. greater [?, ?]. greatest [?, ?, ?].
 Greek [?, ?]. Greeks [?]. Group
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 group-oriented [?]. Group-Theoretic [?].
 Groups [?, ?, ?, ?]. Grubb [?].
 Grundlagen [?]. guerre [?]. guess [?].
 GUEST [?]. Guidance [?]. Guide
 [?, ?, ?, ?, ?, ?, ?]. Guidelines [?, ?, ?].
 Gustavus [?].
 H [?, ?, ?, ?, ?]. H. [?, ?]. habita [?].
 Hackers [?]. Hagelin [?, ?]. Hall [?].
 handbook [?]. Happenings [?]. Harbor
 [?, ?]. Hard [?, ?, ?, ?]. hard-core [?].
 harder [?]. Hardware [?, ?, ?, ?, ?, ?, ?, ?].
 Hariot [?]. Harmonia [?]. Harold [?].
 Hartree [?, ?, ?]. Harvard [?]. Hash
 [?, ?, ?, ?, ?, ?, ?, ?]. hash-coding [?].
 Hash-Functions [?]. hashfunctions [?].
 Having [?, ?]. Hayden [?]. heat [?].
 Hebraicis [?]. held [?, ?, ?, ?, ?]. Hellman
 [?, ?, ?, ?, ?, ?, ?]. Hemel [?]. Hempstead
 [?]. Henry [?]. Herlestam [?].
 heterogeneous [?, ?]. heuristic [?]. Hides
 [?, ?]. Hiding [?]. Hierarchical [?].
 Hierarchy [?, ?, ?]. hieroglyphic [?, ?].
 Hieroglyphs [?, ?]. High
 [?, ?, ?, ?, ?, ?, ?]. High-Level [?].
 High-Speed [?, ?]. Hilton [?, ?]. him [?].
 Hinsley [?]. Hisperic [?]. Historical
 [?, ?, ?, ?, ?]. History
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Hitler [?]. hobby [?]. hoc [?, ?].
 Höhepunkt [?]. Holland [?].
 homomorphic [?]. Honest [?, ?]. honours
 [?, ?]. Hord [?]. horizon [?]. horoscope
 [?]. horses [?]. Host [?]. Hotel [?, ?].
 Houghton [?]. Houthalen [?]. hucusq [?].
 Hughes [?]. Humanities [?, ?]. hunc [?].
 Hungarian [?]. Hut [?, ?]. HX.229 [?].
 HX.229/SC122 [?]. Hydraulica [?].
 Hypergrowth [?]. hypothesis [?].
 I. [?]. i.e [?]. IBM [?, ?, ?, ?]. IC [?].
 idempotent [?]. Identification
 [?, ?, ?, ?, ?, ?]. identify [?]. Identifying
 [?]. Identity [?, ?]. Identity-Based [?].
 IEEE [?, ?, ?, ?]. IEEE/IEICE [?].
 IEICE [?]. IFIP [?, ?, ?, ?]. IFIP/Sec'83
 [?, ?]. IFIP/Sec'84 [?]. II
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. III
 [?]. illegal [?]. Illiac [?]. Illinois [?, ?].
 Illus [?, ?, ?, ?]. illustrata [?]. 'Ilm [?]. im
 [?]. Images [?]. imaging [?]. Imai [?].
 Immanuel [?]. Immunity [?]. Impact
 [?, ?, ?]. Imperfect [?, ?].
 Implementation
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 implementations [?, ?, ?]. Implementing
 [?, ?, ?, ?, ?, ?, ?, ?, ?]. implementors [?].
 Implications [?]. impossibilibus [?].
 Impossible [?, ?]. improved [?].
 improvement [?]. improvements [?].

Level [?, ?]. levels [?]. Levy [?]. Library [?, ?, ?, ?]. Libri [?]. libros [?, ?]. lies [?]. life [?, ?]. likelihood [?, ?]. likely [?]. limit [?]. limitations [?]. Limiting [?]. Limits [?]. linéaire [?]. Linear [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. linearly [?]. Lines [?, ?, ?]. linguarum [?]. Link [?, ?]. Linz [?]. lists [?]. Literature [?, ?, ?, ?, ?, ?, ?]. literis [?]. Little [?, ?]. Load [?]. Local [?, ?, ?, ?]. Location [?]. Lock [?, ?]. Log [?]. Log-in [?]. logarithm [?, ?, ?, ?, ?, ?, ?]. logarithmic [?]. Logarithms [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Logic [?, ?, ?, ?, ?, ?]. London [?, ?, ?]. Long [?]. Long-Period [?]. looks [?]. loop [?]. Lord [?]. Low [?, ?, ?]. Low-Density [?]. low-order [?]. LPC [?]. LSI [?, ?]. Lu [?]. Lu-Lee [?]. Lucifer [?]. luck [?]. Lukoff [?]. Luneburg [?].

M [?, ?, ?, ?]. M-209 [?]. M.I.T. [?]. M1A1 [?]. M1A2 [?]. M2A1 [?]. MA [?]. Mach [?]. machen [?]. Machine [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. machine-to-machine [?]. machinery [?, ?]. Machines [?, ?, ?, ?, ?, ?, ?]. Macmillan [?]. made [?]. magic [?, ?, ?, ?, ?]. magica [?]. magische [?, ?]. Mail [?, ?, ?, ?, ?, ?, ?]. Maine [?]. Mainframe [?]. Maintenance [?, ?, ?]. Majority [?, ?]. make [?]. Making [?, ?]. Malaysia [?]. Malcotti [?]. Man [?, ?, ?, ?]. manageable [?]. Management [?, ?, ?, ?, ?]. Managing [?]. mancherley [?]. manier [?]. manieres [?]. Manipulations [?]. Manitoba [?]. manner [?]. Manual [?, ?, ?, ?, ?, ?, ?, ?, ?]. Manuale [?, ?]. Manuel [?]. manuscripts [?]. mapping [?, ?]. Maratea [?]. March [?, ?, ?]. Markers [?]. market [?]. markets [?, ?]. Markoff [?]. Markov [?]. Mary [?]. Maryland [?, ?, ?]. Marz [?]. Marzolla [?]. Masani [?]. Maskhutah [?]. Massachusetts [?]. Massey [?]. Master [?, ?, ?, ?, ?, ?]. match [?]. matched [?]. Matching [?, ?]. Math [?]. Mathematica [?]. Mathematical [?, ?, ?, ?, ?, ?, ?, ?, ?]. Mathematiques [?, ?, ?, ?, ?]. Mathematicians [?, ?, ?, ?, ?]. Mathematics [?, ?, ?, ?]. mathematischen [?]. Matrices [?]. Matrix [?, ?, ?]. Matsumoto [?]. matter [?]. Matyas [?]. Maurice [?]. Maverick [?]. Maximen [?]. maxims [?]. Maximum [?, ?]. May [?, ?, ?, ?, ?, ?, ?, ?, ?]. Maze [?]. McEliece [?, ?, ?]. McLean [?]. MD [?]. measure [?]. Measurement [?]. Measures [?, ?]. MEBAS [?]. Mechanica [?]. Mechanism [?, ?]. Mechanisms [?, ?, ?, ?, ?]. medieval [?]. Mediterranean [?]. Meetings [?]. members [?]. Memorandum [?]. Memories [?]. Memory [?, ?]. mensuris [?]. Mental [?, ?, ?]. Mercury [?]. merit [?]. Merkle [?, ?, ?]. Mersenne [?, ?]. Message [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Messages [?, ?, ?, ?, ?, ?]. Messenger [?]. metamodel [?]. metatheory [?]. Meteor [?]. Method [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Methods [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Meyer [?]. microcomputer [?, ?, ?, ?]. Microcomputers [?, ?, ?]. Microelectronics [?]. microprocessor [?, ?]. microprocessor-based [?, ?]. Microsoft [?]. Midway [?]. Mifflin [?]. Migration [?]. Militaire [?, ?]. Military [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Millikin [?]. Million [?, ?]. millions [?]. Mind [?]. mini [?]. mini- [?]. Minister [?]. Minneapolis [?]. Minnesota [?]. Mirror [?]. missing [?]. Model [?, ?]. Models [?, ?, ?]. Modern [?, ?, ?, ?, ?, ?, ?, ?]. moderne [?]. Modes [?, ?, ?]. modification [?]. Modular [?, ?, ?, ?, ?]. modules [?, ?, ?]. modulo [?, ?, ?]. modulus [?]. monoalphabetic [?].

monograph [?]. Monte [?, ?]. Monterey [?]. Monthly [?]. morphisms [?, ?, ?]. MOS [?, ?]. Most [?, ?, ?, ?, ?, ?]. movable [?]. MPJ [?]. MPQS [?, ?]. MPQS-factoring [?, ?]. MR [?, ?, ?, ?, ?, ?]. Mr. [?, ?, ?, ?, ?, ?]. mu'amma [?]. Multi [?, ?, ?, ?]. multi-address [?]. Multi-destination [?]. Multi-Player [?]. Multi-Prover [?]. Multics [?, ?]. multilevel [?]. Multiparty [?, ?]. Multiple [?, ?, ?, ?, ?, ?]. Multiplication [?, ?, ?, ?]. Multiplication-permutation [?]. multiplicative [?, ?]. Multipliers [?]. multiply [?, ?]. Multisignature [?]. Mummy [?]. Museum [?, ?, ?, ?]. must [?]. mutual [?]. Mycenaean [?]. mycéniennne [?]. mysteries [?].

N [?]. nahe [?]. name [?, ?, ?]. name-stamp [?, ?]. National [?, ?, ?, ?, ?, ?, ?, ?, ?]. nature [?]. naturliche [?, ?]. Naval [?]. navigandi [?]. Navigation [?]. Navy [?]. Nazi [?]. NBS [?, ?, ?, ?, ?, ?, ?, ?]. NC [?]. Neal [?]. NEC [?, ?]. necromantica [?]. negerii [?]. nemine [?]. Nero [?]. Netherlands [?, ?]. Network [?, ?, ?, ?, ?, ?, ?, ?]. Networks [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Neumann [?]. Nevada [?]. Newbold [?]. News [?, ?, ?, ?]. nihil [?]. nine [?]. nineteenth [?]. Niv [?]. NJ [?]. No [?, ?, ?, ?, ?, ?, ?, ?]. nominibus [?]. Non [?, ?, ?, ?, ?, ?]. Non-Cryptographic [?]. Non-Governmental [?]. Non-homomorphic [?]. Non-Interactive [?, ?]. non-pattern [?]. Noncryptographic [?, ?]. Nonlinear [?, ?, ?]. nonrandomness [?]. Nonsingular [?]. Norbert [?]. Normal [?, ?, ?]. Normandy [?]. Norris [?]. Norse [?]. North [?]. North-Holland [?]. Notation [?]. Note [?, ?, ?, ?, ?, ?, ?, ?, ?]. Notes [?, ?]. Notice [?, ?]. Notices [?, ?]. notion [?, ?]. Nov [?]. nova [?, ?]. Novel [?]. November [?, ?, ?]. NP [?, ?]. NP-Completeness [?]. NSA [?, ?]. Number [?, ?, ?, ?, ?, ?, ?, ?]. Numbers [?, ?, ?, ?, ?, ?]. Numerical [?, ?, ?]. nummis [?]. nunc [?].

O [?]. O. [?, ?]. Oakland [?, ?, ?]. Object [?]. Objects [?]. oblivious [?, ?]. obscuras [?]. obscure [?]. Observability [?, ?]. observation [?]. Observations [?]. obsolete [?]. Obtaining [?, ?, ?]. occultam [?, ?]. occulte [?]. Oct [?]. October [?, ?, ?, ?, ?, ?, ?, ?, ?]. off [?]. Office [?]. official [?]. Ogham [?]. Oh [?]. Okamoto [?]. old [?]. Ole [?]. ology [?]. Omura [?]. One [?, ?, ?, ?, ?, ?, ?, ?]. One-Chip [?]. one-time [?]. One-Way [?, ?, ?, ?, ?, ?, ?, ?, ?]. Only [?]. Ontario [?]. Open [?, ?]. OpenBSD [?]. Operating [?, ?, ?, ?]. Operation [?, ?, ?, ?, ?]. operations [?, ?, ?, ?, ?]. Optimal [?, ?]. Optimization [?, ?]. Options [?]. order [?]. ordered [?]. Orderly [?]. orders [?]. Organization [?]. Organizational [?]. Organizations [?, ?]. organized [?]. oriented [?]. Origin [?, ?, ?, ?]. Origins [?, ?]. Orlando [?]. Orleans [?]. ornithological [?]. Osborne [?]. Other [?, ?, ?, ?]. output [?]. Outputs [?]. outstanding [?]. overflow [?]. Overview [?, ?, ?, ?].

P [?, ?]. package [?, ?, ?, ?]. packet [?]. Packings [?]. pad [?]. pages [?, ?, ?, ?, ?]. Pair [?]. palace [?, ?]. Palindromic [?]. Paper [?, ?, ?, ?, ?]. paperback [?]. Papers [?, ?, ?, ?]. papers/Compcon [?]. Paradoxical [?]. paradoxis [?]. Parallel [?, ?, ?, ?, ?]. Parameters [?]. Paris [?]. Park [?, ?, ?]. Part

[?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Partial
 [?, ?, ?, ?, ?]. partial-match [?].
 participants [?]. Partitioned [?].
 partitioning [?]. partly [?]. Parts [?].
 party [?]. Pascal [?]. Pass [?].
 Pass-Algorithms [?]. passa [?]. passim
 [?]. Password [?, ?, ?, ?, ?, ?, ?, ?]. past
 [?]. past/present/future [?]. patents [?].
 Pattern [?, ?]. Patterson [?]. payments
 [?]. PC [?, ?]. Peapolitani [?]. Pearl [?, ?].
 Pegawai [?]. Pennings [?]. perfectly [?].
 Performance [?, ?, ?]. Period [?, ?].
 Permutation [?, ?, ?, ?, ?, ?].
 Permutations [?, ?, ?, ?, ?, ?, ?].
 perniciosa [?]. Personal [?, ?, ?, ?, ?, ?].
 Peter [?]. Peters [?]. PGP [?].
 phaenomena [?]. Philippum [?, ?].
 Physica [?]. Physica-Mathematica [?].
 physical [?, ?, ?]. Physics
 [?, ?, ?, ?, ?, ?, ?, ?]. Picking [?].
 picture [?]. Pieprzyk [?]. Pioneer [?].
 Pioneered [?]. Pioneers [?]. pipeline [?].
 placing [?, ?, ?]. Plaintext [?, ?]. plane
 [?]. platform [?]. Play [?, ?]. Player [?].
 Playfair [?]. plays [?, ?]. Pless [?]. plus
 [?, ?]. PN [?]. pneumatika [?]. Poe [?].
 poems [?]. Point [?, ?]. points [?]. Poker
 [?, ?, ?]. policies [?]. Polish [?, ?, ?, ?].
 polyalphabetic [?, ?, ?]. Polygraphia [?].
 Polygraphiae [?]. polygraphic [?].
 Polynomial [?, ?, ?, ?, ?, ?, ?].
 polynomial-time [?]. polynomial-tuples
 [?]. polynomials [?, ?, ?]. Pond [?].
 ponderibus [?]. Pope [?]. Portland
 [?, ?, ?]. Portrait [?]. Portuguese [?].
 position [?, ?]. Positions [?]. possession
 [?]. post [?]. postales [?]. potential [?].
 pour [?, ?]. Power [?]. Powerful [?]. pp
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. practica
 [?]. Practical [?, ?, ?, ?, ?, ?, ?]. Practice
 [?, ?, ?]. praecipue [?]. Pre [?]. Pre-RSA
 [?]. Precautions [?, ?]. predicate [?].
 Preliminary [?, ?, ?]. Prentice [?].
 Prentice-Hall [?]. prepared [?]. Presence
 [?]. present [?]. presents [?, ?]. Press [?].
 Prevent [?]. Price [?]. Primality
 [?, ?, ?, ?, ?, ?]. prime [?, ?, ?]. Primer
 [?, ?, ?]. Primes [?, ?, ?]. primo [?].
 Principem [?, ?]. Principles
 [?, ?, ?, ?, ?, ?]. Printers [?]. Printing [?].
 Prisoner [?]. Privacy
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Private [?, ?, ?]. Private-key [?, ?, ?].
 pro [?]. Probabilistic [?, ?, ?, ?, ?, ?, ?, ?].
 Probability [?, ?, ?, ?, ?, ?]. Probable
 [?, ?]. Probable-Word-Proof [?].
 Problem [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Problems
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 procédés [?]. Procedure [?, ?, ?].
 Procedures [?, ?, ?, ?, ?, ?]. Proceedings
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Process
 [?, ?, ?]. Processing [?, ?, ?, ?]. Processor
 [?, ?, ?]. Produced [?, ?, ?]. Producing
 [?]. product [?]. products [?]. program
 [?]. Programming [?, ?, ?, ?, ?, ?].
 Programowa [?]. Programs [?, ?, ?].
 Progressions [?]. Project [?, ?].
 projections [?]. promissa [?]. Proof
 [?, ?, ?, ?]. Proofs [?]. Propagation [?].
 properties [?]. property [?]. proposal [?].
 Proposed [?, ?, ?, ?]. propositional [?].
 Prospective [?, ?, ?]. protect [?].
 Protecting [?]. Protection [?, ?, ?, ?, ?, ?].
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 protein [?]. Protocol
 [?, ?, ?, ?, ?, ?, ?, ?]. Protocols [?, ?, ?].
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Prototype [?, ?]. Provable [?]. provably
 [?, ?]. prove [?]. proven [?]. Prover [?].
 provided [?]. Providence [?]. provides
 [?]. Proving [?]. Pseudo
 [?, ?, ?, ?, ?, ?, ?, ?].
 Pseudo-Inversen [?]. Pseudo-Random
 [?, ?, ?, ?, ?, ?, ?, ?]. pseudoinverses [?].
 pseudonym [?]. pseudonyms [?, ?].

?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Schemes [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Schimpff [?]. Schlacht [?]. Schneider [?].
 School [?, ?, ?]. Schreiben [?, ?].
 Schreibkunst [?, ?]. Schriften [?].
 Science [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Scientific [?, ?, ?].
 Scientists [?, ?]. Scrambling [?, ?]. Script
 [?, ?]. scripta [?]. scripti [?]. scripturam
 [?, ?]. sea [?]. seal [?, ?]. Sealing [?, ?].
 Search [?, ?, ?, ?, ?, ?, ?]. Seattle [?].
 Seberry [?]. Sec'83 [?, ?]. Sec'84 [?].
 Second [?, ?, ?]. secondary [?, ?, ?].
 Secrecy [?, ?, ?]. Secret
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Secret [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 secret-key [?]. Secretdisk [?]. secrète [?].
 secrètement [?]. secrètes [?, ?]. Secrets
 [?, ?, ?, ?, ?, ?, ?, ?]. Section [?, ?].
 sector [?]. secundum [?]. Secure
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Security [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Security-related [?, ?]. sed [?]. seed
 [?]. seen [?]. Seev [?]. sejao [?]. Select [?].
 Selected [?, ?]. Selenus [?]. Self [?, ?].
 self-similarity [?]. Self-Synchronizing [?].
 Selfcipher [?]. Selfridge [?]. semigroups
 [?]. Seminar [?, ?]. Seminumerical [?, ?].
 Senate [?]. Senior [?, ?]. sententiam [?].
 Sentinel [?]. September [?, ?, ?].
 Sequence [?, ?, ?, ?]. Sequences
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Serenissimum [?, ?]. server [?]. Service
 [?, ?, ?, ?, ?]. Services [?, ?, ?, ?]. ses [?].
 Set [?, ?, ?]. seventeenth [?]. Sex [?].
 Shakespeare [?, ?, ?, ?]. Shakespearean
 [?]. Shamir [?, ?, ?, ?, ?]. Shaped [?].
 Share [?]. Shared [?, ?]. Sharing
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Shelta
 [?]. Shift [?, ?, ?, ?]. shift-register [?].
 short [?]. shortcut [?, ?]. Should [?, ?].
 shuffling [?]. Shulman [?, ?]. SIAM [?].
 sic [?]. Sieve [?, ?]. signal [?, ?, ?].
 Signaling [?]. signalling [?]. Signals
 [?, ?, ?]. Signature [?, ?, ?, ?, ?, ?, ?, ?, ?].
 Signatures [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 signes [?]. significance [?, ?]. significant
 [?]. significantibus [?]. signing [?].
 similarity [?]. Simonetta [?]. Simple
 [?, ?, ?, ?, ?]. simplification [?].
 Simplified [?]. Simulate [?]. Simulating
 [?]. Simulation [?, ?, ?]. Simultaneity
 [?, ?]. simultaneous [?]. Singer [?]. Single
 [?, ?, ?, ?, ?]. Single-board [?].
 single-chip [?]. Singular [?]. Sinkov [?].
 sive [?, ?]. Six [?, ?, ?]. size [?]. skill [?].
 skonczonych [?]. slice [?]. slide [?]. Small
 [?]. Smart [?, ?]. Society [?, ?, ?, ?]. sofic
 [?]. Software [?, ?, ?, ?, ?, ?, ?, ?, ?].
 software-based [?]. Soldier [?]. Solomon
 [?]. Solution
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 solutions [?, ?, ?, ?]. solver [?]. solves
 [?]. Solving [?, ?, ?, ?, ?]. solvuntur
 [?]. Some [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 sonderlichen [?]. Sons [?]. sophisticated
 [?]. Sorting [?]. Sound [?]. Source [?, ?].
 Sources [?, ?, ?]. South [?]. Space [?].
 Spanheimensis [?, ?, ?]. spawned [?].
 Speaks [?]. Special [?, ?, ?, ?, ?].
 spécialement [?]. specialist [?].
 specialties [?]. Specification [?]. Spectral
 [?, ?]. Spectroscope [?]. spectrum [?].
 Speech [?, ?, ?, ?]. Speed [?, ?, ?].
 Sphere [?]. Spirit [?]. spirituum [?].
 Sprache [?]. spread [?]. spring [?]. Spy
 [?, ?]. spying [?]. square [?, ?]. staff [?].

TMS75C00 [?]. today [?, ?]. tokens [?].
 Tokyo [?]. Tolerance [?]. Tolerant [?, ?].
 tomorrow [?]. tool [?]. Toolbox [?]. Tools
 [?, ?, ?]. Top [?, ?, ?, ?]. top-secret [?].
 Topic [?, ?]. Tore [?]. Toronto [?, ?].
 totally [?]. Tracking [?]. tract [?].
 Tractatus [?]. tradeoff [?]. traduzir [?].
 Traffic [?, ?, ?, ?]. Traicté [?]. trails [?].
 Trainer [?]. Traité [?, ?]. Trans [?].
 transaction [?, ?]. Transactional [?].
 transcendental [?]. Transfer
 [?, ?, ?, ?, ?, ?]. Transformation [?, ?, ?].
 transformations [?]. transformed [?].
 Transition [?]. translating [?].
 translations [?]. transmission [?].
 transparent [?]. Transport [?].
 Transposition [?, ?, ?]. Trap [?, ?].
 Trap-Door [?]. Trapdoor [?, ?, ?, ?].
 trapdoor-knapsack [?]. Trapdoors [?].
 TRASEX [?]. Trattati [?]. Treatise
 [?, ?, ?, ?]. Treatises [?]. Treaty [?, ?].
 tree [?, ?]. Trees [?, ?, ?, ?]. trend [?].
 tres [?]. tres-subtile [?]. Trial [?].
 Triangle [?]. trifid [?]. Triple [?]. triplex
 [?, ?]. Trithemii [?, ?]. Trithemij
 [?, ?, ?, ?]. Trithemio [?]. Trithemius
 [?, ?]. Trojan [?]. Troubled [?]. truly
 [?, ?]. truncated [?, ?]. Trust [?, ?].
 Trusted [?, ?, ?]. Trusting [?, ?].
 Trustworthy [?, ?]. Tsarist [?]. tube [?].
 Tubes [?]. Tunny [?]. tuples [?]. Turing
 [?, ?, ?, ?]. tutorial [?, ?]. TV [?]. TVROs
 [?]. twentieth [?]. Twenty [?, ?, ?].
 twenty-fourth [?]. Two
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 two-part [?, ?]. two-party [?]. TX [?].
 Type [?, ?, ?, ?, ?]. types [?].
 U [?]. U-boat [?]. U.S. [?, ?]. ubi [?]. ue
 [?]. ultimate [?]. ultra
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. ultrasound
 [?]. unabridged [?]. Unbiased [?, ?].
 Unclassified [?]. Unconditionally [?].
 Undergraduate [?]. Uniform [?]. Unique
 [?, ?, ?, ?]. Uniquely [?]. United
 [?, ?, ?, ?, ?, ?, ?, ?, ?]. Universal
 [?, ?, ?, ?, ?]. University [?, ?, ?, ?].
 UNIX [?, ?, ?, ?, ?]. Unknown [?].
 Untraceable [?, ?, ?]. Untrusted [?].
 Update [?, ?]. upgrading [?]. Upon
 [?, ?, ?]. urgent [?]. USA [?, ?, ?, ?, ?, ?].
 Usage [?, ?]. Use
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. used
 [?, ?, ?, ?]. useful [?]. Usenix [?]. User
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 user-controlled [?]. users [?, ?, ?]. Uses
 [?, ?, ?, ?]. Using [?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. ut [?].
 utility [?].
 V [?, ?, ?]. vacuum [?]. vacuum-tube [?].
 Validating [?, ?]. Validation [?]. valuable
 [?]. Value [?, ?]. value-adding [?]. Valves
 [?]. Variable [?]. variables [?, ?]. Variants
 [?]. variations [?, ?, ?]. varieties [?].
 Världskriget [?]. Vehicle [?]. verbis [?].
 verborgene [?]. verborgens [?].
 Verfahren [?]. verifiability [?]. Verifiable
 [?, ?, ?]. verification [?, ?, ?, ?, ?]. verified
 [?]. Verify [?, ?]. Verifying [?]. Vernam
 [?]. Verschlüsselungsabbildungen [?].
 version [?]. versions [?]. versus [?, ?].
 verwandter [?]. Very [?, ?, ?]. via [?].
 Vienna [?]. view [?, ?]. viewpoint [?, ?].
 Vigenère [?]. VIII [?, ?, ?]. vindicata [?].
 vindicias [?]. viruses [?]. Visible [?].
 VLSI [?, ?, ?, ?, ?, ?]. vnd [?]. vne [?].
 vnnd [?, ?]. vocabulary [?]. Voice
 [?, ?, ?, ?, ?, ?, ?, ?]. Vol [?, ?].
 voluntatem [?, ?]. vs [?]. vulnerable [?].
 W [?, ?, ?]. W. [?, ?]. wa [?]. wa-istikhray
 [?]. Wagstaff [?]. War [?, ?, ?, ?, ?, ?, ?, ?].
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 warfare [?, ?]. Wars [?, ?]. Was
 [?, ?, ?, ?]. Washington [?, ?, ?]. watch
 [?]. Waterman [?]. Watermark [?, ?].

Watermark-based [?, ?]. watermarks [?].
 Waveform [?]. Waves [?]. Way
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Wayne
 [?]. Wayner [?]. weak [?, ?]. weaken [?].
 weaknesses [?, ?, ?]. weapon [?]. Web [?].
 Weber [?, ?]. Webster [?]. Wednesday
 [?, ?]. Weiss [?]. Welchman [?]. West
 [?, ?]. Wexelblat [?]. WG [?]. whatever
 [?]. wheels [?]. where [?]. wherein [?, ?].
 Which [?, ?, ?]. Whitehall [?]. Who
 [?, ?, ?]. Whole [?]. wholesale [?]. whose
 [?]. Wide [?, ?]. wie [?]. Wiener [?].
 Wiley [?, ?]. Wiley-Teubner [?]. will [?].
 William [?, ?, ?, ?]. Williams [?]. Wire
 [?, ?]. Wire-tap [?]. within [?]. Without
 [?, ?, ?, ?, ?, ?, ?, ?]. wits [?]. Wizard [?].
 Wolfe [?]. wohn [?]. Word
 [?, ?, ?, ?, ?, ?, ?, ?]. WordPerfect [?].
 words [?]. Work [?]. working [?]. Works
 [?]. Workshop
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Workstations [?]. World [?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 worldwide [?, ?]. Worthy [?]. would [?].
 Writing [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?]. writings [?, ?, ?]. wrong
 [?]. wrote [?]. WW [?]. Wyner [?, ?].

X.509 [?]. X3 [?]. X9.23 [?]. xiv [?]. xvi
 [?, ?]. xviii [?, ?].

year [?, ?]. Years [?, ?, ?, ?]. Yeheskel [?].
 yesterday [?]. York [?, ?, ?, ?, ?, ?, ?, ?].
 York/London [?, ?]. yourself [?].

Z [?]. zastosowan [?]. Zeit [?]. Zendian [?].
 Zero [?, ?]. zero-knowledge [?]. Zimmer-
 mann [?, ?]. zone [?]. Zufallsgeneratoren
 [?]. Zur [?].