

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: <http://www.math.utah.edu/~beebe/>

23 July 2020
Version 4.106

Title word cross-reference

1421 [?]. **1474** [?]. **1500-1815** [?]. **15th** [?].
18 [?]. **1917** [?]. **1938** [?, ?]. **1941** [?]. **1942**
[?]. **1943** [?, ?]. **1944** [?]. **1945** [?]. **1975**
[?]. **1976** [?]. **1977** [?]. **1981** [?]. **1982** [?].
1983 [?, ?, ?]. **1984** [?, ?]. **1985** [?]. **1986**
[?, ?]. **1987** [?, ?, ?]. **1988** [?].
(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 [?]. **0-7248-0274-6** [?].
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 [?].
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. [?]. AAEC [?]. AAEC-6 [?]. abbatis [?, ?, ?]. ABC [?]. Above [?]. Abraham [?]. Absence [?]. absentibus [?, ?]. absolute [?]. Abstract [?, ?, ?, ?, ?, ?, ?, ?, ?]. academic [?]. Academy [?]. accepts [?]. Access [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Account [?, ?, ?, ?]. accuracy [?, ?]. ACE [?]. Achieving [?, ?, ?]. ACM [?, ?, ?, ?, ?]. acontismologia [?]. Acquired [?, ?]. 'Action [?]. Activities [?]. ad [?, ?, ?]. Ada [?, ?]. Adaptive [?]. added [?]. adding [?]. Addition [?]. additional [?, ?]. additive [?]. address [?]. addresses [?, ?]. ADFGVX [?, ?]. Adleman [?, ?, ?, ?]. administrator [?]. 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 [?]. 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 [?, ?]. 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 [?]. Auditing [?]. auffzulosen [?]. August [?, ?, ?, ?, ?]. Austria [?, ?]. aut [?].

Authenticated [?]. Authenticating [?].
 Authentication
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Authenticator [?]. authenticators [?].
 author [?, ?]. Authority [?].
 Authorization [?]. Automata [?, ?].
 automated [?]. Automatic [?, ?].
 Automating [?]. automaton [?, ?, ?].
 Available [?]. avalanche [?]. AVL [?].
 Award [?, ?]. Awards [?].

 B [?, ?, ?]. B.C [?, ?]. B.S.T.J. [?].
 Babbage [?, ?, ?, ?, ?, ?, ?, ?]. Back [?].
 background [?]. backup [?]. Bacon [?, ?].
 Bad [?]. Bahasa [?]. balance [?].
 Balancing [?]. Ballistica [?]. Baltimore
 [?, ?]. Bamford [?]. band [?]. banking [?].
 Banned [?]. Banquet [?]. barbaris [?].
 bars [?]. baru [?]. base [?]. Based
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Bases
 [?, ?, ?, ?]. Basic [?, ?, ?, ?, ?, ?, ?, ?].
 Basic-plus [?]. Batava [?]. Bateman [?].
 battle [?, ?, ?, ?]. battles [?]. Be
 [?, ?, ?, ?]. Bearlagair [?]. been [?].
 Behaviour [?]. Belgium [?, ?]. believe [?].
 Benchmarks [?]. Berkeley [?, ?].
 Bernardini [?]. Bernstein [?].
 Berücksichtigung [?]. besonderer [?].
 Best [?]. Between [?, ?, ?, ?]. Beyond
 [?, ?]. Biased [?]. Bibliography
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Bidirectional
 [?]. bifid [?]. Big [?, ?]. Bijjective [?].
 Binary [?, ?, ?, ?]. Biographical [?].
 Biographies [?]. biology [?]. bipolar [?].
 Birkerød [?]. Birth [?]. Birthday [?, ?].
 BIT [?, ?, ?, ?, ?, ?]. bit-slice [?]. Bits
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Black [?, ?, ?, ?].
 Bletchley [?, ?]. Blind [?]. Block
 [?, ?, ?, ?, ?]. blockcipher [?]. Blocking
 [?]. board [?]. boat [?]. Bodyguard [?].
 Bog [?]. Bog-Latin [?]. Bomba [?].
 Bombe [?]. Book [?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. books
 [?]. Boolean [?, ?]. Bostium [?]. Boston
 [?, ?]. Bosworth [?]. bounds [?].
 Bowditch [?]. box [?]. boxes [?]. Boys [?].
 Brainerd [?]. Braunschweig [?].
 Braunschweig-Luneburg [?]. break
 [?, ?, ?, ?]. Breaking
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. breaks
 [?]. Breakthrough [?]. bridge [?]. Briefs
 [?]. British [?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 broadband [?]. Broke [?, ?, ?, ?]. Broken
 [?, ?, ?, ?, ?, ?]. Brother [?, ?]. Brown [?].
 Bruce [?]. Bruijn [?]. Buddy [?, ?]. bug
 [?]. Buifendam [?]. Build [?]. Built [?].
 Bureau [?, ?, ?, ?, ?]. Bureaus [?]. Burg
 [?]. burst [?]. Byzantine [?, ?, ?, ?].

 C [?, ?, ?, ?]. C-36 [?, ?]. C. [?, ?]. CA [?].
 Cable [?]. Caesar [?]. Calculating
 [?, ?, ?]. calculation [?, ?]. Calculator [?].
 California [?, ?, ?, ?, ?, ?]. called [?].
 Calls [?]. Cambridge [?]. Camera [?].
 campaign [?]. Can [?]. Canada [?, ?, ?].
 Cancellation [?, ?]. Capabilities [?, ?].
 capability [?, ?, ?, ?, ?]. capability-based
 [?, ?, ?, ?]. Capacity [?]. Capitol [?].
 Capsule [?, ?, ?, ?, ?]. capta [?].
 caracteres [?]. card [?]. Cardan [?].
 Cardano [?]. cards [?, ?]. Carlo [?, ?].
 Carolina [?]. Carpenter [?]. cartes [?].
 carvings [?]. Cascade [?]. Cascaded
 [?, ?]. Case [?, ?, ?, ?]. catalogue [?].
 category [?]. CBI [?]. CCITT [?, ?]. CD
 [?]. CD-ROM [?]. CEC [?]. Cellular
 [?, ?]. certa [?, ?]. Certain [?, ?, ?, ?, ?, ?].
 certifiable [?]. Certified [?]. Chadwick
 [?]. Chain [?]. chaining [?]. Chaldaicis
 [?]. Challenge [?, ?, ?]. Chamber
 [?, ?, ?, ?]. change [?]. Channel
 [?, ?, ?, ?, ?]. Channels [?, ?, ?].
 Character [?]. characteristic [?].
 characteristics [?]. characters [?].

checkers [?]. checking [?]. Checks [?].
 checksum [?, ?]. chemical [?]. chess [?].
 Chicago [?, ?, ?, ?]. Chifferbyråernas [?].
 chiffrée [?]. 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 [?].
 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 [?, ?]. Cracking [?, ?, ?].
 craft [?]. creating [?]. crime [?]. criteria
 [?]. Criterion [?]. Critical [?, ?, ?].
 crittografia [?, ?]. crossword [?].
 crosswords [?]. crypt [?, ?]. crypt-ology
 [?]. Cryptanalysis
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Cryptanalyst [?, ?, ?]. Cryptanalysts
 [?]. Cryptanalytic [?, ?, ?].
 Cryptanalytical [?]. cryptanagnosis [?].
 cryptic [?, ?]. CRYPTO
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Crypto-ease [?]. Crypto-Functions [?].
 Cryptogram [?]. Cryptograms [?, ?, ?].
 cryptograph [?, ?, ?]. Cryptographer
 [?, ?]. Cryptographia [?, ?, ?].
 Cryptographic
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Cryptographically [?, ?, ?, ?, ?].
 Cryptographie
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Cryptography [?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 D [?, ?, ?]. D. [?]. DOL [?]. DOL-TOL [?].
 D1 [?]. D4 [?]. Dabbling [?]. Dalgarno
 [?]. Dallas [?]. damage [?]. damnata [?].
 dan [?]. dans [?]. Dante [?]. Data
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 data
 [?, ?]. data-flow [?]. Database
 [?, ?, ?, ?, ?, ?]. Datagram [?]. David
 [?, ?, ?, ?]. Davison [?]. Davos [?]. dawn
 [?]. Day' [?]. Days [?, ?]. DBMS [?]. DBS
 [?]. DC [?, ?]. Deavours [?]. Debate [?].
 Dec. [?]. December [?, ?]. deception [?].
 déchiffrement [?, ?]. Dechiffirkunst [?].
 deciferandi [?]. decifrar [?]. Decimal [?].
 Decipherability [?, ?]. Decipherable [?].

Deciphered [?, ?, ?, ?]. Deciphering [?, ?, ?, ?, ?]. Decipherment [?, ?].
 decision [?]. deck [?]. decoder [?].
 decoders [?]. decree [?, ?]. d'écriture [?].
 Decrypting [?, ?]. Decryption [?, ?, ?, ?, ?, ?, ?]. Dee [?]. defeat [?].
 defies [?]. Defined [?]. definitions [?].
 Degenerate [?]. degree [?]. Degrees [?].
 deinde [?]. Demands [?]. Demonstrating [?].
 demotic [?, ?]. d'encres [?]. denies [?].
 Denmark [?, ?]. Denning [?]. Density [?].
 denudata [?]. DEP [?]. Dependence [?].
 dependency [?]. depositions [?].
 depth [?]. description [?]. d'escire [?].
 desiderata [?]. Design [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 designed [?]. designing [?]. designs [?].
 destination [?]. destroyer [?]. Detecting [?, ?, ?, ?].
 detection [?]. detective [?]. deterioration [?].
 determination [?]. deutschen [?].
 developing [?]. Development [?, ?, ?, ?, ?].
 Developments [?, ?, ?, ?]. Deviates [?, ?].
 device [?, ?]. devices [?, ?, ?]. diagnostic [?].
 Dickson [?, ?]. Dickson-polynomials [?].
 Dickson-scheme [?]. dictionary [?, ?]. diem [?].
 Dierstein [?]. Difference [?, ?]. difficult [?].
 difficulty [?]. Diffusion [?]. digest [?].
 Digital [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Digitalized [?]. Digits [?, ?]. Digraphic [?].
 dimension [?]. Diophantine [?]. diplomacy [?].
 Diplomatic [?, ?, ?]. Direct [?]. Directions [?].
 Directly [?]. 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 [?, ?].
 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** [?]. **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** [?, ?]. **exhibitur** [?].
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**
 [?, ?, ?, ?, ?, ?]. **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** [?, ?, ?, ?].
französischen [?]. **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 [?, ?]. **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** [?]. **Herlestad** [?].
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** [?]. **Illiacc** [?]. **Illinois** [?, ?].
Illus [?, ?, ?, ?]. **illustrata** [?]. **'Ilm** [?]. **im**
 [?]. **Images** [?]. **imaging** [?]. **Imai** [?].
Immanuel [?]. **Immunity** [?]. **Impact**
 [?, ?, ?]. **Imperfect** [?, ?].

Implementation
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
implementations [?, ?, ?]. **Implementing**
 [?, ?, ?, ?, ?, ?, ?, ?]. **implementors** [?].
Implications [?]. **impossibilibus** [?].
Impossible [?, ?]. **improved** [?].
improvement [?]. **improvements** [?].
in-depth [?]. **incendiary** [?]. **including** [?].
'inda [?]. **Independent** [?]. **Index** [?, ?, ?].
indirect [?, ?]. **Indoglottal** [?]. **Indonesia**
 [?]. **industry** [?, ?, ?, ?]. **Inferring**
 [?, ?, ?, ?]. **Infinite** [?, ?]. **Influence**
 [?, ?, ?, ?]. **influenced** [?]. **Inform**
 [?, ?, ?, ?]. **Informatics** [?]. **Information**
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
Initial [?, ?]. **Inmos** [?]. **Inn** [?].
Innovation [?, ?, ?]. **input** [?].

inquisitionis [?]. Insatser [?]. inscribed
 [?, ?]. Insection [?]. Insecure
 [?, ?, ?, ?, ?, ?, ?]. INSPEC [?, ?, ?].
 Installation [?, ?]. installing [?].
 Institute [?]. institution [?].
 Instrumenta [?]. Instruments [?, ?, ?].
 Insure [?, ?]. integer [?, ?]. integers
 [?, ?, ?]. Integrating [?]. Integration [?].
 Integrity [?, ?, ?]. intellecta [?].
 intellectual [?]. Intelligence
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Interactive [?, ?, ?, ?, ?]. interbank [?].
 Intercept [?]. interception [?]. interface
 [?]. interfaces [?]. internal [?].
 International
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Internet
 [?, ?, ?, ?, ?, ?]. Internetworks [?].
 Interoperability [?, ?, ?, ?].
 Interpretation [?]. Intractability [?, ?].
 Intractable [?]. Intrepid [?].
 Introduction
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Introductory [?, ?]. intruder [?].
 intruder-proof [?]. invented [?]. Inversen
 [?]. Investigation [?]. investigations [?].
 involvement [?]. Ioannis [?, ?]. Iohannis
 [?, ?]. IPS [?]. Ireland [?]. ISBN [?, ?].
 ISDN [?]. Island [?, ?]. ISO [?, ?].
 ISO/CCITT [?]. issue [?, ?]. Issues
 [?, ?, ?, ?]. istikhraj [?]. Italian [?, ?, ?].
 Italica [?]. Italy [?, ?, ?]. item [?].
 Iterated [?, ?, ?, ?, ?, ?]. IV [?, ?, ?].

 J [?, ?, ?, ?]. J. [?, ?, ?, ?, ?]. Jack [?].
 Jacobi [?]. James [?]. January
 [?, ?, ?, ?, ?]. Japan [?, ?]. Japanese [?, ?].
 jargon [?]. Java [?]. Java-based [?].
 Jennifer [?]. Johannes [?, ?]. Iohannis
 [?]. John [?, ?, ?, ?, ?]. Joint [?]. Josef [?].
 Joseph [?]. Journal [?]. Jr [?]. Juan [?].
 juillet [?]. July [?, ?, ?, ?]. June
 [?, ?, ?, ?, ?]. juxta [?].

 Kahn [?, ?, ?, ?]. Keel [?]. Keep [?].
 Keeping [?, ?]. Ken [?]. Kendall [?].
 Kent [?]. Kerberos [?]. Kernel [?, ?, ?, ?, ?].
 Key [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 key [?, ?, ?, ?, ?]. Key-Lock-Pair [?].
 keyed [?, ?, ?]. keyless [?, ?]. Keys
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Killian [?]. kind [?]. kinds [?]. Kingdom
 [?]. Knapsack [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Knapsack-type [?, ?]. Knapsacks [?, ?, ?]. Knowledge
 [?, ?, ?, ?, ?]. knowledge-analysis [?].
 known [?]. Koblitz [?]. kodowania [?].
 Konheim [?]. korekcyjnego [?].
 Kozaczuk [?, ?]. Kruh [?]. kryptografii
 [?]. Kryptographie [?]. Kryptologie [?].
 Kunsten [?].

 L [?, ?, ?]. Laboratories [?]. Laboratory
 [?]. Labs [?]. LAN [?]. land [?]. Lands [?].
 language [?, ?, ?, ?]. languages [?, ?, ?, ?].
 Lapid [?]. Large [?, ?, ?, ?, ?, ?, ?, ?].
 Large-Scale [?]. Lasers [?]. late [?]. Latin
 [?]. Latina [?]. latter [?]. lattice [?, ?].
 Law [?]. Lawrence [?]. Laxenburg [?].
 Layer [?, ?, ?, ?]. Lazy [?, ?]. lead [?].
 leading [?]. learning [?]. least [?].
 Lecture [?]. lectures [?, ?]. Lee [?, ?, ?].
 Lessons [?, ?]. Lett [?, ?, ?]. Letter [?, ?].
 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** [?]. **Lord** [?]. **Low** [?, ?, ?]. **Low-Density** [?].
low-order [?]. **LPC** [?]. **LSI** [?, ?]. **Lu** [?].
Lu-Lee [?]. **luck** [?]. **Lukoff** [?]. **Lunenburg** [?].

M [?, ?, ?, ?]. **M-209** [?]. **M.I.T.** [?].
M1A1 [?]. **M1A2** [?]. **M2A1** [?]. **MA** [?].
Mach [?]. **machen** [?]. **Machine** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
machinery [?, ?]. **Machines** [?, ?, ?, ?, ?, ?, ?, ?]. **Macmillan** [?]. **made** [?]. **magic** [?, ?, ?, ?]. **magica** [?].
magische [?, ?]. **Mail** [?, ?, ?, ?, ?, ?, ?, ?].
Mainframe [?]. **Maintenance** [?, ?, ?].
Majority [?, ?]. **make** [?]. **Making** [?, ?].
Malaysia [?]. **Malcotti** [?]. **Man** [?, ?, ?, ?]. **manageable** [?]. **Management** [?, ?, ?, ?, ?]. **Managing** [?]. **mancherley** [?]. **manier** [?]. **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 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
Mathematicians [?, ?, ?, ?, ?]. **Mathematics** [?, ?, ?, ?].
mathematischen [?]. **Matrices** [?].
Matrix [?, ?, ?]. **Matsumoto** [?]. **matter** [?]. **Matyas** [?]. **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 [?].
 mycénienne [?]. mysteries [?].

N [?]. nahe [?]. name [?, ?, ?].
 name-stamp [?, ?]. National
 [?, ?, ?, ?, ?, ?, ?, ?, ?]. nature [?].
 naturliche [?, ?]. Naval [?]. navigandi [?].
 Navigation [?]. Navy [?]. Nazi [?]. NBS
 [?, ?, ?, ?, ?, ?]. NC [?]. Neal [?]. NEC
 [?, ?]. necromantica [?]. negeri [?].
 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/Comcon [?].
 Paradoxical [?]. paradoxis [?]. Parallel
 [?, ?, ?, ?, ?]. Parameters [?]. Paris [?].
 Park [?, ?, ?]. Part
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Partial
 [?, ?, ?, ?, ?]. partial-match [?].
 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 [?]. pneumatica [?].
 Poe [?]. poems [?]. Point [?, ?]. points
 [?]. Poker [?, ?, ?]. policies [?]. Polish
 [?, ?, ?, ?]. polyalphabetic [?, ?, ?].
 Polygraphia [?]. Polygraphiae [?].
 polygraphic [?]. Polynomial
 [?, ?, ?, ?, ?, ?, ?, ?]. polynomial-time [?].
 polynomial-tuples [?]. polynomials
 [?, ?, ?]. ponderibus [?]. 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
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Proceeedings [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 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 [?, ?].
 Pseudoprimes [?]. Pseudorandom
 [?, ?, ?, ?, ?, ?]. Ptolemy [?, ?]. PUB
 [?, ?, ?, ?]. Public
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Publications [?, ?, ?]. Publishers
 [?]. Publishing [?, ?, ?, ?]. Puerto [?].
 Pugh [?]. Purple [?, ?, ?, ?]. Puteani [?].
 puzzle [?, ?]. puzzles [?, ?].

Quadratic [?, ?, ?]. quae [?, ?].
 quaesquer [?]. quality [?]. Quantum
 [?, ?, ?]. Quasi [?]. Quasi-Random [?].
 que [?]. Queries [?, ?]. quest [?].
 quocunque [?]. quosdam [?].

R [?, ?]. R. [?, ?]. rôle [?]. Rabin
 [?, ?, ?, ?, ?]. radar [?]. Radio
 [?, ?, ?, ?, ?, ?]. Ralph [?, ?]. Ramp [?].
 Random
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Randomized [?, ?, ?]. randomness [?].
 Rang [?]. rates [?, ?]. Read [?, ?, ?, ?, ?].
 reading [?]. Readings [?, ?]. Real [?].
 Realistic [?]. realizacja [?]. Realization
 [?]. realizing [?]. really [?]. Receive [?].
 reception [?]. reciprocal [?].
 Reconstructing [?]. record [?]. records
 [?]. recurrences [?]. Recursiveness [?].
 Red [?, ?]. Rédei [?, ?]. Rédei-scheme
 [?, ?]. Reden [?]. reduced [?]. reducing
 [?, ?, ?]. reduction [?]. Redundancy
 [?, ?, ?, ?]. Reed [?]. Reference [?, ?, ?, ?].
 Reflections [?, ?, ?, ?]. regarding [?, ?].
 Register [?, ?, ?, ?]. règles [?]. Reimann
 [?]. rejecta [?]. Related [?, ?, ?, ?].
 Relational [?]. relativized [?]. Relaxation
 [?, ?]. rely [?]. remainder [?]. remainders
 [?]. Remark [?]. Remarks [?, ?, ?, ?, ?].
 Remember [?]. Remote [?, ?, ?]. Remove
 [?]. Renaissance [?]. Reno [?]. repairer
 [?, ?]. Repetitions [?]. Report
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. reports [?].
 reprieve [?]. Request [?]. Requirements
 [?, ?, ?, ?, ?, ?]. Requiring [?].
 Research [?, ?, ?, ?]. reserata [?].
 resource [?]. Reste [?]. Restraints [?].
 Results [?, ?, ?, ?, ?, ?, ?, ?]. Retail [?].
 Retrieval [?, ?, ?, ?]. Retrofitting [?].
 Retrospect [?]. return [?, ?]. revealed [?].
 Revealing [?, ?]. revelada [?]. reversal
 [?]. Review [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Reviews

[?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. revisited [?].
 Revolution [?]. rewriting [?]. RFC
 [?, ?, ?, ?, ?, ?, ?, ?, ?]. rfi [?, ?]. Rhode [?].
 Rico [?]. rings [?, ?]. Rise [?]. Riverbank
 [?]. Rivest [?, ?, ?]. RNG [?]. robust [?].
 Rochelle [?]. Roger [?]. Roland [?]. role
 [?, ?]. ROM [?]. Romaine [?]. Rome [?].
 Ronald [?]. roots [?, ?]. Rosetta [?, ?, ?].
 rotating [?]. Rotation [?]. rotations [?].
 Round [?, ?]. Rounds [?, ?, ?]. Route [?].
 Routing [?]. Rowland [?]. RSA
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 RSA-cryptosystem [?, ?].
 RSA-cryptosystems [?]. RSA/Rabin
 [?, ?]. RTS [?]. Rudiger [?]. Rules
 [?, ?, ?]. runic [?]. running [?].

S [?, ?, ?, ?, ?]. S-box [?]. S-boxes [?]. S.
 [?]. Saer [?]. safe [?, ?]. Safeguarding
 [?, ?]. safety [?]. Saga [?]. sampling [?].
 Sampson [?]. San [?, ?, ?, ?]. Sandia [?].
 Satellite [?, ?, ?]. satisfying [?]. Saved [?].
 SB [?]. SC122 [?]. Scale [?, ?]. Scheme
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 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-key [?]. Secretdisk [?]. secrète [?].

secrètement [?]. secrètes [?]. Secrets
 [?, ?, ?, ?, ?, ?, ?, ?, ?]. Section [?, ?].
 sector [?]. secundum [?]. Secure
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. Security
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Security-related [?, ?]. sed [?]. seed [?].
 seen [?]. Seev [?]. seiao [?]. 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 [?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 signature-verification [?]. 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 [?, ?, ?, ?]. 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 [?]. spirituum [?]. Sprache [?].
 spread [?]. spring [?]. Spy [?, ?]. spying
 [?]. square [?, ?]. staff [?]. stamp [?, ?].
 Standard [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
 ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Standardization [?]. Standards
 [?, ?, ?, ?, ?]. Stars [?]. State [?, ?].
 States [?, ?, ?, ?, ?, ?, ?]. Statistical
 [?, ?, ?, ?, ?]. statistically [?]. Statistics
 [?]. status [?]. Steganographia
 [?, ?, ?, ?, ?, ?]. Steganographiae [?, ?].
 steganographica [?]. steganographicos
 [?, ?]. Steganologia [?, ?]. stelae [?]. Step
 [?]. Stockholm [?]. Stokes [?]. Stone
 [?, ?, ?]. Storage [?, ?]. storage/backup
 [?]. Stored [?]. stories [?, ?]. Storing [?].
 Story [?, ?, ?, ?, ?, ?, ?, ?, ?].
 Strandberg [?]. Strandbergs [?].
 strategy [?, ?, ?]. Stream [?, ?, ?]. Strong
 [?, ?, ?, ?]. Structure [?, ?]. Structured
 [?, ?, ?]. structures [?]. studies [?]. Study
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].

subcategory [?]. subexponential [?, ?].
 subexponential-time [?]. subkey [?, ?].
 Subkeys [?]. Subliminal [?, ?, ?].
 Subscript [?]. subsequences [?].
 Subset [?, ?]. Substitution
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 substitution-permutation [?, ?].
 substitutions [?, ?]. subtile [?]. subtle [?].
 Subtractive [?]. sui [?, ?]. Suitable [?].
 Sum [?, ?]. summary [?]. summe [?].
 Summer [?, ?, ?, ?]. sunt [?].
 Supercomputing [?, ?]. Superincreasing
 [?]. Support [?, ?, ?]. suppositia [?].
 surveillance [?]. Survey [?, ?, ?, ?, ?].
 Sweden [?]. Swedish [?]. Swift [?].
 Switching [?]. Switzerland [?]. SX [?, ?].
 SX-2 [?, ?]. Symmetric [?, ?, ?].
 symmetry [?, ?]. sympathiques [?].
 Symposium [?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Synchronizing [?].
 Synthese [?]. synthesis [?]. System
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Systems [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 System/38 [?]. systèmes [?]. Systems
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 T [?, ?]. T. [?, ?]. TOL [?]. Täfelingen [?].
 take [?]. tale [?, ?, ?, ?, ?]. Talk [?, ?].
 Tall [?]. ta'miyah [?]. tampering [?].
 tandem [?]. Tanis [?]. tap [?]. Tar [?].
 task [?]. Tassiana [?]. Teaching [?].
 Technical [?, ?, ?, ?, ?]. technique [?].
 technique [?, ?]. Techniques
 [?, ?, ?, ?, ?, ?, ?, ?, ?]. technologies [?].
 Technology [?, ?, ?, ?, ?, ?, ?, ?].
 Telecommunications [?, ?].
 Telecryptograph [?]. telegram [?, ?].
 Telegraph [?]. Telegraphic [?].
 Telegraphing [?]. Teleinformatics [?].
 Telephone [?, ?, ?, ?, ?]. telephones [?].
 Telephoning [?]. Teletrust [?]. television
 [?]. telex [?]. Templars [?]. Ten [?, ?]. ter
 [?]. Term [?]. Terminal [?]. terrorism [?].
 Test [?, ?, ?]. Testing [?, ?, ?, ?, ?]. tests
 [?]. Text [?, ?, ?, ?, ?, ?, ?]. texts [?, ?, ?].
 th [?]. TH1 [?]. TH1/TH4 [?]. TH4 [?].
 Their
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Theorem [?, ?]. Theorems [?, ?].
 Theoretic [?, ?]. theorica [?]. theories [?].
 Theory [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 Theory/Coding [?]. there [?]. thieves [?].
 Thinking [?, ?]. Third [?, ?]. Thomas [?].
 Thompson [?]. Thousands [?]. threat [?].
 Three [?, ?]. Threshold [?, ?, ?].
 throughout [?]. Thwarting [?]. tilings [?].
 Till [?]. Time
 [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
 time-luck [?]. Time-sharing [?, ?, ?].
 timely [?]. Times [?, ?]. tips [?]. tissue
 [?]. titles [?]. TLP [?]. TMS7500 [?].
 TMS75C00 [?]. today [?, ?]. tokens [?].
 Tokyo [?]. Tolerance [?]. Tolerant [?, ?].
 tomorrow [?]. tool [?]. Toolbox [?]. Tools
 [?, ?, ?]. Top [?, ?, ?, ?]. top-secret [?].
 Topic [?, ?]. Tore [?]. Toronto [?, ?].
 totally [?]. Tracking [?]. tract [?].
 Tractatus [?]. tradeoff [?]. traduzir [?].
 Traffic [?, ?, ?, ?]. 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** [?, ?, ?, ?, ?].

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** [?]. **Verschlüsselungsabbildungen** [?]. **version** [?]. **versions** [?]. **versus** [?, ?]. **verwandter** [?]. **Very** [?, ?, ?]. **via** [?]. **Vienna** [?]. **view** [?, ?]. **viewpoint** [?, ?]. **VIII** [?, ?, ?]. **vindicata** [?]. **vindicias** [?]. **viruses** [?]. **Visible** [?]. **VLSI** [?, ?, ?, ?, ?, ?]. **vnd** [?]. **vne** [?]. **vnmd** [?, ?]. **vocabulary** [?]. **Voice** [?, ?, ?, ?, ?, ?, ?]. **Vol** [?, ?]. **voluntatem** [?, ?]. **vs** [?]. **vulnerable** [?].

W [?, ?, ?]. **W.** [?, ?]. **wa** [?]. **wa-istikhraj** [?]. **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** [?]. **will** [?]. **William** [?, ?, ?, ?]. **Williams** [?]. **Wire** [?, ?]. **Wire-tap** [?]. **within** [?]. **Without** [?, ?, ?, ?, ?, ?, ?]. **wits** [?]. **Wizard** [?]. **Wolfe** [?]. **woln** [?]. **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** [?].