A Complete Bibliography of Publications in *Cryptologia*

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA

Tel: +1 801 581 5254

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

01 April 2025
Version 3.79

Title word cross-reference

(t, m) [?]. (t, n) [?, ?]. **$10.00** [?]. **$12.00** [?]. 128 [?]. **$139.99** [?]. **$15.00** [?]. **$16.95** [?, ?]. **$16.96** [?]. **$18.95** [?]. **$24.00** [?]. **$24.00/$34** [?]. **$24.04** [?]. **$24.95** [?, ?]. **$26.95** [?]. **$29.95** [?]. **$30.00** [?]. **$30.95** [?]. **$38.00** [?]. **$39** [?]. **$39.95** [?]. **$43.39** [?]. **$45.00** [?]. **$5.95** [?]. **$54.00** [?]. **$54.95** [?]. **$54.99** [?]. **$6.50** [?]. **$6.95** [?]. **$69.00** [?]. **$69.95** [?]. **$75.00** [?]. **$89.95** [?]. th [?]. A [?]. A^3 [?, ?]. χ [?]. H [?]. k [?, ?, ?]. M [?, ?, ?]. M^3 [?]. n [?, ?, ?]. q [?].

-ary [?]. **-Bit** [?]. **-error** [?]. **-out-of-** [?, ?]. **-sequences** [?]. **-tests** [?].

0 [?]. **000** [?]. **01Q** [?, ?].

1 [?, ?, ?, ?, ?]. **1-4398-1763-4** [?]. **1/2in** [?, ?]. **10** [?]. **100** [?, ?]. **10011-4211** [?]. **10016-8810** [?, ?]. **1221** [?]. **125** [?]. **15.00/$23.60.0** [?]. **15th** [?, ?]. **16th** [?, ?]. **17-18** [?]. **18** [?]. **180-4** [?]. **1812** [?]. **18th** [?, ?, ?, ?, ?, ?]. **18th-Century** [?]. **1930s** [?]. **1939** [?]. **1940** [?, ?]. **1940s** [?]. **1941** [?]. **1942** [?]. **1943** [?]. **1945** [?, ?, ?, ?, ?]. **1946** [?, ?, ?]. **1950s** [?]. **1970s** [?]. **1980s** [?]. **1989** [?]. **19th** [?, ?, ?, ?, ?]. **19th-century** [?].

2 [?, ?, ?]. **200/220** [?]. **2000** [?]. **2004** [?, ?]. **2008** [?]. **2009** [?]. **2011** [?]. **2013** [?, ?]. **2014** [?]. **2017** [?]. **2019** [?]. **2024** [?]. **20755-6886** [?]. **209** [?, ?, ?, ?, ?, ?]. **20th** [?]. **21** [?]. **22** [?]. **220** [?]. **24-Hour** [?, ?, ?]. **25** [?, ?]. **25.00/$39.30** [?]. **25.00/839.30** [?]. **25A1** [?]. **25B** [?]. **26** [?, ?]. **28147** [?]. **28147-89** [?]. **285** [?]. **294** [?]. **2in** [?, ?]. **2nd** [?, ?, ?, ?].

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

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

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

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

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

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

9 [?, ?, ?, ?]. **9/11** [?, ?, ?, ?]. **97** [?, ?, ?]. **9761** [?]. **978** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **978-0-19-874783-3** [?]. **978-0-300-26944-4** [?]. **978-0-7509-7885-9** [?]. **978-0-8218-9883-3** [?]. **978-0-9557164-1-6** [?]. **978-1-3988-1244-4** [?]. **978-1-39908-961-6** [?]. **978-1-4704-1048-3** [?]. **978-1-4711-8679-0** [?]. **978-1-7185-0272-7** [?]. **978-1-78155-759-4** [?]. **978-1-7988-8747-9** [?]. **978-1-7988-8811-7** [?]. **978-3-319-53278-3** [?].

Āryabhata [?].

A-22 [?]. **A-5** [?]. **A.** [?, ?]. **A.6** [?]. **AAAS** [?]. **Abraham** [?]. **Abrutat** [?]. **Abuse** [?]. **Abwehr** [?, ?, ?]. **academic** [?]. **Accelerating** [?]. **Access** [?]. **Accessible** [?]. **Accident** [?]. **Accidental** [?]. **Account** [?, ?]. **Accounts** [?, ?, ?]. **Accumulated** [?]. **Achievements** [?]. **Acoustical** [?]. **Across** [?, ?]. **Act** [?, ?, ?]. **Action** [?]. **Actions** [?]. **Activist** [?]. **Activities** [?]. **Acts** [?]. **Adam** [?]. **adaptive** [?]. **Addendum** [?]. **Additive** [?]. **Additives** [?, ?]. **Addressable** [?]. **addressing** [?]. **ADFGVX** [?]. **adjacent** [?]. **Adlan** [?]. **Administrative** [?]. **Admiral** [?, ?]. **Admiralty** [?]. **Admission** [?]. **Adopts** [?]. **Adults** [?]. **Advanced** [?, ?, ?, ?, ?]. **Advent** [?]. **Adventures** [?]. **Adversarial** [?]. **Advertisements** [?]. **Aerial** [?]. **AES** [?, ?, ?, ?, ?, ?, ?]. **Affair** [?]. **affine** [?]. **Afluisterstation** [?, ?]. **After** [?]. **Aftermath** [?]. **Again** [?, ?]. **Against** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Age** [?, ?, ?, ?, ?]. **Agencies** [?]. **Agency** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Agent** [?]. **Agents** [?, ?]. **Ages** [?]. **Agnes** [?, ?, ?]. **Agreement** [?, ?, ?, ?, ?]. **Aid** [?]. **Aided** [?, ?]. **Air** [?, ?, ?]. **Air-Amphibian** [?]. **Akelarre** [?]. **aktualisierte** [?]. **al** [?, ?, ?, ?, ?, ?]. **al-Qaeda** [?]. **al-Tayyan** [?]. **al.** [?]. **Alain** [?]. **Alan** [?, ?]. **alAsraf** [?]. **Alastair** [?, ?]. **Albert** [?]. **Alberti** [?]. **Alcohol** [?]. **Aldrich** [?]. **Alec** [?]. **Aleutians** [?]. **Alexander** [?, ?]. **Alexis** [?]. **Alf** [?]. **Algebra** [?, ?, ?, ?]. **Algebraic** [?, ?, ?, ?, ?, ?]. **Algorithm** [?, ?]. **Algorithmic** [?, ?, ?, ?]. **Algorithms** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Aligning** [?, ?]. **Alisa** [?]. **All-Or-Nothing** [?]. **allied** [?, ?, ?, ?, ?]. **Allies** [?]. **Alone** [?]. **Alphabet** [?, ?]. **Alphabetical** [?]. **Alphanumeric** [?]. **Amateur** [?]. **Ambush** [?]. **America** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **American** [?, ?]. **Americas** [?]. **amid** [?]. **among** [?]. **Amphibian** [?]. **AMSCO** [?]. **Amy** [?]. **Analysis** [?, ?]. **Analytical** [?]. **Analyzing** [?, ?, ?]. **Ancestral** [?]. **Ancient** [?, ?, ?].

Anderson [?, ?]. **Andrew** [?, ?]. **Anglicus** [?]. **Angooki** [?, ?, ?]. **Anguish** [?]. **Anish** [?]. **Ann** [?]. **Annapolis** [?]. **Anne** [?, ?]. **Annealing** [?]. **annihilation** [?]. **Anniversary** [?]. **Annotated** [?, ?]. **Announcement** [?]. **Announcements** [?]. **Announces** [?]. **Annual** [?]. **Anonymity** [?]. **Anonymous** [?]. **años** [?]. **Anson** [?]. **anti** [?]. **anti-submarine** [?]. **Antoinette** [?]. **ANU** [?]. **Anywhere** [?]. **apology** [?]. **Apparatus** [?]. **Appendix** [?, ?]. **Application** [?, ?, ?, ?, ?, ?, ?, ?, ?]. **Applications** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Applied** [?, ?]. **apply** [?]. **Applying** [?, ?]. **Appraisal** [?]. **Approach** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **approved** [?]. **April** [?, ?]. **Arab** [?]. **ARABIA** [?]. **Arabic** [?, ?, ?, ?, ?, ?]. **arbitrary** [?]. **Archaeology** [?]. **Architect** [?, ?]. **Architects** [?]. **Archives** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,

Beurling [?]. **bezet** [?, ?]. **Bhattacharjee** [?]. **Biafra** [?]. **Biafran** [?]. **Bible** [?, ?, ?]. **Bibliander** [?]. **Bibliographer** [?]. **Bibliography** [?, ?]. **Bifid** [?]. **Big** [?]. **Biggest** [?]. **binary** [?, ?, ?]. **Biographical** [?, ?]. **Biographies** [?, ?, ?,

[?, ?, ?, ?, ?, ?, ?]. **Change** [?, ?, ?, ?]. **Changed** [?, ?]. **Changes** [?, ?]. **Channel** [?, ?, ?]. **Chaocipher** [?, ?, ?, ?, ?]. **Chaos** [?, ?, ?]. **chaos-based** [?]. **Chaotic** [?, ?, ?, ?]. **Chapman** [?]. **Chapter** [?]. **characters** [?]. **Charles** [?, ?, ?]. **Charlie** [?]. **Charlotte** [?, ?, ?]. **Charting** [?]. **Chasing** [?, ?]. **Chaum** [?]. **cheating** [?]. **Check** [?, ?]. **Checkers** [?]. **Checksums** [?]. **Cheevers** [?]. **Chi}** [?]. **Chicago** [?]. **Chief** [?]. **Chiffrieren** [?, ?]. **Child** [?]. **children** [?]. **China** [?]. **Chinese** [?, ?, ?, ?]. **Chionna** [?]. **Chosen** [?, ?]. **Chosen-Key** [?]. **Chosen-Plaintext** [?]. **Christian** [?, ?]. **Christof** [?]. **Christopher** [?, ?, ?, ?]. **Chronology** [?]. **Churchill** [?, ?, ?, ?]. **Churchyard** [?]. **Ciarcia** [?]. **Cicco** [?]. **cifra** [?]. **Cilli** [?]. **Cipher** [?, ?, ?, ?, ?, ?,

Communicator [?]. **communist** [?, ?]. **Community** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **commutative** [?]. **Companion** [?]. **Company** [?, ?]. **comparative** [?]. **Comparison** [?, ?]. **Competitions** [?]. **Compiled** [?]. **Complementing** [?]. **Complete** [?, ?, ?, ?]. **Complexity** [?, ?, ?, ?]. **Component** [?, ?]. **Composition** [?]. **Comprehensive** [?, ?]. **Compression** [?]. **Compromise** [?, ?]. **Compromised** [?]. **Compuserve** [?]. **Computation** [?]. **Computations** [?]. **Computer** [?, ?]. **Computer-Aided** [?, ?]. **Computers** [?, ?, ?, ?, ?]. **Computing** [?, ?, ?, ?]. **COMSEC** [?]. **concealed** [?]. **Concept** [?]. **concepts** [?, ?]. **Concern** [?]. **concerns** [?]. **Confederate** [?, ?, ?, ?]. **Conference** [?, ?, ?, ?, ?, ?, ?, ?]. **Confidential** [?]. **Confidentiality** [?, ?]. **Confirmed** [?]. **Confusion** [?]. **Cong** [?]. **Congruential** [?]. **conjecture** [?, ?]. **conjecture-based** [?]. **Connection** [?, ?, ?, ?]. **Connections** [?]. **Conquer** [?, ?]. **Considerations** [?, ?, ?]. **considering** [?]. **Conspiracy** [?]. **Construction** [?, ?, ?, ?, ?]. **Consular** [?]. **Consulates** [?]. **consumer** [?]. **Contemporary** [?, ?]. **Content** [?]. **Contest** [?, ?, ?]. **Context** [?, ?]. **contingency** [?]. **Continues** [?]. **continuous** [?]. **continuous-figure** [?]. **Contributed** [?]. **Contribution** [?, ?]. **Contributions** [?, ?, ?]. **Contributors** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,

[?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?].
Cryptographer [?, ?, ?]. **Cryptographers** [?]. **Cryptographic** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,

Designs [?, ?, ?]. **Destroyed** [?]. **DESX** [?]. **Detachment** [?]. **details** [?]. **Detecting** [?, ?]. **detection** [?]. **Detective** [?]. **determining** [?]. **Deutsches** [?]. **Development** [?, ?, ?]. **Developments** [?, ?]. **Device** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Devices** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Dewey** [?]. **Dexter** [?]. **DH** [?]. **DH-26** [?]. **Diagonal** [?]. **Dial** [?]. **Diaries** [?]. **Diary** [?, ?, ?]. **Dictionary** [?, ?]. **Did** [?, ?, ?, ?, ?]. **Dienst}** [?]. **Dies** [?, ?]. **difference** [?]. **differencing** [?, ?]. **Different** [?]. **Differential** [?, ?, ?, ?, ?, ?, ?]. **Differential-Style** [?]. **differentials** [?]. **Diffie** [?]. **diffusion** [?]. **Digital** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Digraphic** [?]. **Dilly** [?, ?, ?]. **Dingman** [?]. **Dingyi** [?]. **Diplomacy** [?, ?]. **Diplomat** [?]. **Diplomatic** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Direction** [?]. **Directional** [?]. **Disclose** [?]. **Disclosed** [?]. **disclosure** [?]. **Discovered** [?]. **Discovery** [?, ?, ?]. **discrete** [?]. **discussion** [?, ?]. **Disk** [?, ?]. **Disks** [?, ?]. **Dispatch** [?]. **Display** [?]. **Dispute** [?]. **Dissenting** [?]. **distance** [?]. **Distinguished** [?]. **Distinguishers** [?]. **Distributed** [?, ?, ?]. **Distribution** [?, ?, ?, ?, ?]. **distributions** [?]. **Divide** [?, ?]. **Divide-and-Conquer** [?]. **Divisions** [?]. **DNA** [?]. **DNA-Based** [?]. **Do** [?]. **'Doc** [?]. **Document** [?, ?]. **Documentary** [?, ?]. **Documents** [?, ?, ?]. **Dodgson** [?, ?]. **Dodo** [?]. **does** [?, ?]. **Doing** [?]. **Dominic** [?]. **Donald** [?, ?]. **Dönitz** [?, ?]. **Donovan** [?]. **Don't** [?, ?]. **Dooley** [?, ?, ?]. **Dorabella** [?]. **Dot** [?, ?]. **'Double** [?, ?, ?, ?, ?, ?, ?]. **Double-Base** [?]. **Doubleday** [?]. **Down** [?, ?, ?]. **DPEPE** [?, ?]. **DPJO** [?, ?]. **Dr.** [?, ?, ?]. **Draft** [?]. **Dragon** [?]. **Drawbacks** [?]. **Drazin** [?, ?, ?, ?]. **Dress** [?]. **Driscoll** [?, ?, ?]. **Dropping** [?]. **DSA** [?]. **Duits** [?, ?]. **Duke** [?]. **Dunedin** [?]. **Dunin** [?, ?]. **duplication** [?]. **During** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Dustin** [?]. **Dutch** [?, ?, ?, ?, ?, ?]. **Duties** [?]. **Dynamic** [?, ?, ?, ?].

E. [?]. **Earliest** [?, ?, ?]. **Early** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Easier** [?]. **East** [?, ?, ?]. **Eastcote** [?]. **Easter** [?, ?]. **Eastern** [?]. **Eavesdroppers** [?]. **Eavesdropping** [?, ?, ?, ?, ?, ?, ?]. **ECC** [?]. **Ecclesiastical** [?]. **ECG** [?]. **ECM** [?, ?, ?, ?]. **Economic** [?]. **Ed** [?, ?, ?]. **Edge** [?]. **Edited** [?, ?, ?, ?, ?, ?, ?, ?]. **Edition** [?, ?, ?, ?, ?, ?, ?, ?]. **Editor** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Editorial** [?, ?, ?, ?, ?, ?, ?, ?]. **Editors** [?, ?]. **Eds** [?, ?, ?]. **Educated** [?]. **Education** [?, ?, ?, ?, ?]. **Edward** [?]. **Eespiau** [?]. **Effective** [?]. **Effectiveness** [?]. **Effects** [?]. **Efficient** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Efforts** [?]. **Egypt** [?]. **Egyptologist** [?]. **Eighteenth** [?]. **Eilidh** [?]. **Elder** [?]. **Eldridge** [?]. **Electronic** [?, ?, ?, ?]. **Elegant** [?]. **Elementary** [?, ?, ?, ?, ?, ?, ?]. **ElGamal** [?]. **Elgar** [?]. **elimination** [?]. **Elizebeth** [?, ?, ?, ?, ?]. **Elle** [?]. **Elliot** [?, ?]. **Elliptic** [?, ?, ?]. **Elonka** [?, ?]. **emerged** [?]. **Emergency** [?]. **Emily** [?]. **Emperor** [?, ?]. **Empirical** [?, ?]. **Enable** [?]. **encipher_Algorithm** [?]. **Enciphered** [?, ?]. **Encipherment** [?]. **Enclosed** [?]. **Encode** [?]. **Encoding** [?, ?]. **Encore** [?]. **encounters** [?]. **Encrypted** [?, ?, ?, ?, ?, ?, ?]. **Encrypting** [?]. **Encryption** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,

[?]. **English** [?, ?, ?]. **enhanced** [?]. **Enhancement** [?, ?]. **Enigma** [?, ?, ?,

Format-preserving [?]. **Forms** [?, ?, ?]. **Forschungsamt** [?]. **Forschungsstelle** [?, ?]. **Fort** [?]. **Forty** [?]. **Forward** [?]. **Forwards** [?]. **Found** [?]. **Foundation** [?]. **Foundations** [?, ?, ?]. **Four** [?, ?]. **Four-Round** [?]. **Fourth** [?, ?]. **Fox** [?, ?, ?]. **Framework** [?, ?]. **France** [?, ?]. **Francis** [?]. **Francisco** [?, ?]. **Francois** [?]. **Frank** [?, ?]. **Fraternal** [?]. **Frederick** [?]. **Fredrik** [?]. **Free** [?, ?]. **Freedom** [?, ?]. **French** [?, ?, ?, ?, ?, ?, ?, ?]. **Frequency** [?]. **Friederich** [?]. **Friedman** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Friedmans** [?]. **Friedrich** [?]. **Friend** [?]. **Friends** [?]. **front** [?, ?, ?]. **Fuensanta** [?]. **Full** [?, ?]. **fun** [?]. **Function** [?, ?, ?, ?, ?, ?, ?, ?]. **Functions** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Fundamentals** [?]. **Funny** [?]. **Further** [?, ?, ?, ?, ?]. **Futility** [?]. **Future** [?, ?]. **fuzzy** [?, ?]. **fuzzy-image** [?].

G [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **G-312** [?]. **G-OTP** [?]. **G.2** [?]. **Gallagher** [?, ?]. **Gallehawk** [?]. **Galois** [?, ?]. **Galore** [?]. **Game** [?, ?, ?, ?, ?]. **games** [?]. **Gang** [?, ?]. **Gangbuster** [?]. **Gannon** [?]. **Garbles** [?]. **García** [?]. **Gard** [?, ?]. **Garden** [?]. **GC** [?]. **GCHQ** [?, ?, ?, ?]. **Gehaimnussen}** [?]. **Geheimschreiber** [?, ?, ?, ?]. **Gen.** [?]. **General** [?, ?, ?, ?, ?]. **Generalised** [?]. **generalization** [?]. **Generalized** [?, ?, ?, ?, ?, ?]. **Generalized-Multisignature** [?]. **Generated** [?, ?, ?]. **generating** [?]. **Generation** [?, ?, ?]. **Generator** [?, ?, ?, ?]. **Generators** [?, ?, ?]. **Genesis** [?, ?, ?]. **Genetic** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Geneva** [?]. **Genevieve** [?, ?]. **Genie** [?]. **Geniuses** [?]. **Gentlemen** [?]. **Genuine** [?]. **geographically** [?]. **George** [?, ?, ?, ?]. **Georges** [?]. **Georges-Jean** [?]. **Georgiyev** [?]. **Gerald** [?]. **German** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,

harmonious [?]. **Harold** [?, ?]. **Harvard** [?]. **Hasenjaeger** [?]. **Hash** [?, ?, ?, ?, ?, ?, ?]. **hashing** [?]. **Hassan** [?]. **hasta** [?]. **Haven** [?]. **Haystacks** [?]. **HC** [?, ?, ?, ?]. **HC-520** [?]. **HC-9** [?, ?, ?]. **Headaches** [?]. **healthcare** [?]. **Hebern** [?, ?, ?]. **Heer** [?]. **Heights** [?]. **Heiko** [?]. **Heinz** [?]. **Held** [?, ?]. **Hell** [?, ?]. **Hellman** [?, ?]. **Helmich** [?]. **Helped** [?, ?]. **Helquist** [?]. **Hen-House** [?]. **Henryk** [?]. **Heraldry** [?, ?]. **Herbert** [?, ?, ?, ?, ?]. **Herivel** [?, ?]. **Herivelismus** [?, ?]. **Herodotus** [?]. **Heroes** [?, ?, ?, ?]. **HF** [?]. **Hidden** [?, ?, ?, ?, ?]. **Hiding** [?, ?, ?, ?]. **hierarchical** [?]. **High** [?, ?, ?, ?]. **High-Grade** [?]. **High-Security** [?]. **High-Speed** [?, ?]. **Higher** [?, ?]. **Higher-Order** [?]. **Hill** [?, ?]. **hill-climbing** [?]. **Hilton** [?]. **Him** [?]. **Hinsley** [?]. **Histoire** [?]. **historia** [?]. **Historians** [?]. **Historic** [?, ?, ?]. **Historical** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Histories** [?, ?]. **History** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,

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

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

Kaczynski [?]. **Kahn** [?, ?, ?, ?, ?, ?]. **Kalina** [?]. **Kapera** [?, ?, ?, ?]. **Kappa** [?, ?]. **Karl** [?]. **Kasiski** [?]. **Kassel** [?]. **Kate** [?]. **Katherine** [?]. **Kean** [?, ?]. **KECCAK** [?]. **Keen** [?]. **Keeping** [?]. **Keith** [?]. **'Keiti** [?]. **Ken** [?]. **Kennedy** [?]. **Kenyon** [?, ?]. **Kerckoff** [?]. **Kern** [?]. **Kerry** [?]. **Key** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,

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

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

Media [?]. **Medical** [?]. **Medicine** [?]. **Medieval** [?, ?]. **Mediterranean** [?]. **Meer** [?]. **Meeting** [?, ?, ?]. **Meetings** [?]. **mej** [?]. **Mellen** [?, ?]. **members** [?]. **Memo** [?]. **memoirs** [?]. **Memorandum** [?, ?]. **Memoria** [?]. **Memorial** [?]. **Memoriam** [?, ?, ?, ?, ?]. **memorie** [?, ?]. **Memorieren** [?, ?]. **Memories** [?, ?, ?, ?, ?, ?]. **Memory** [?, ?, ?, ?]. **Men** [?, ?, ?, ?]. **Mendelsohn** [?]. **Mensajes** [?]. **mental** [?]. **Mentors** [?]. **Menzel** [?]. **Meritocracy** [?]. **Merkle** [?]. **Message** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Messages** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **messaging** [?]. **Method** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **méthode** [?]. **Methods** [?, ?]. **Mexican** [?, ?]. **Meyer** [?, ?, ?, ?]. **MFA** [?]. **MGR** [?]. **MI** [?]. **MI-8** [?]. **Michael** [?, ?, ?, ?, ?, ?]. **Microcomputer** [?]. **Microcomputers** [?]. **Microprocessor** [?]. **Mid** [?]. **Mid-Victorian** [?]. **Middle** [?, ?]. **Midway** [?, ?, ?, ?, ?]. **Milestone** [?, ?]. **Military** [?, ?]. **Miller** [?, ?]. **Millward** [?]. **Milton** [?, ?]. **Mimic** [?]. **Mind** [?]. **mine** [?]. **Mines** [?]. **Mini** [?, ?, ?]. **Mini-AES** [?, ?]. **minimal** [?]. **Mirrors** [?, ?]. **Misidentified** [?]. **missed** [?, ?]. **Missile** [?]. **Missing** [?]. **Mission** [?, ?]. **Mitchell** [?]. **Mixing** [?]. **MK8** [?, ?]. **Mobile** [?]. **Mobilizes** [?]. **Mock** [?]. **Mode** [?, ?]. **Model** [?, ?, ?]. **Models** [?, ?]. **Modern** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Modes** [?, ?, ?]. **Modifications** [?, ?]. **Modified** [?]. **Modifying** [?]. **Modulated** [?]. **Modulo** [?]. **Modulus** [?]. **Mohamad** [?]. **Monge** [?]. **Mono** [?]. **Mono-Alphabetical** [?]. **Monopoly** [?]. **Mons** [?]. **Monte** [?]. **Monument** [?, ?]. **Moon** [?]. **Morland** [?]. **Morocco** [?, ?]. **Most** [?, ?, ?, ?, ?, ?, ?, ?, ?]. **Moti** [?]. **Movie** [?]. **Mowry** [?]. **Mr.** [?, ?, ?, ?]. **Mrayati** [?]. **Mrs.** [?]. **Mucklow** [?]. **multi** [?, ?]. **multi-document** [?]. **multi-prime** [?]. **multicast** [?]. **Multics** [?]. **Multiloop** [?]. **Multimedia** [?]. **multinomial** [?]. **Multiple** [?, ?, ?, ?, ?]. **Multiple-Key** [?, ?]. **Multiplex** [?, ?, ?]. **Multiplication** [?]. **Multisignature** [?]. **multivariable** [?]. **Mundy** [?]. **Munich** [?]. **Munson** [?]. **Murray** [?]. **Museum** [?, ?, ?, ?, ?]. **Museumsforum** [?]. **Music** [?, ?]. **music-based** [?]. **Musical** [?, ?, ?]. **Mutual** [?]. **My** [?, ?, ?, ?, ?, ?, ?]. **Myers** [?]. **Mysteries** [?]. **Mysterious** [?, ?, ?, ?, ?]. **Mystery** [?, ?, ?, ?, ?, ?]. **Mystic** [?, ?, ?, ?]. **Myth** [?].

N [?]. **Naccache** [?]. **Names** [?]. **Nancy** [?]. **Nara** [?]. **National** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Nationalist** [?]. **Nations** [?]. **Nature** [?]. **Navajo** [?]. **Navajos** [?]. **Naval** [?, ?]. **Navies** [?]. **Navy** [?, ?]. **Nazi** [?, ?]. **Nazis** [?]. **Neal** [?]. **necessarily** [?]. **Nederland** [?, ?]. **Needed** [?, ?]. **Needles** [?]. **Needs** [?]. **Neglected** [?, ?]. **Neglecting** [?]. **Negotiations** [?]. **Neil** [?, ?]. **NEMA** [?]. **Nemeses** [?]. **Nesbit** [?]. **Netherlands** [?, ?, ?]. **Network** [?, ?, ?, ?, ?]. **Networks** [?, ?, ?]. **Neuro** [?]. **Neuro-Identifier** [?]. **Never** [?]. **NEWDES** [?]. **News** [?, ?, ?]. **Nez** [?]. **Niagara** [?, ?]. **Nicholas** [?, ?]. **Nickles** [?]. **Nicodemus** [?]. **Nineteenth** [?, ?, ?, ?]. **nineteenth-century** [?]. **Ninth** [?]. **Ninth-Century** [?]. **NIST** [?, ?, ?]. **Nixdorf** [?]. **NJ** [?, ?]. **NKU** [?]. **No** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Noblest** [?]. **Nomenclator** [?]. **nomenclatures** [?]. **Non** [?, ?, ?, ?, ?, ?, ?]. **Non-Cryptanalytic** [?]. **Non-English** [?].

Non-Governmental [?]. **non-linearity** [?]. **non-matching** [?]. **Non-Military** [?]. **Non-Secret** [?]. **Noncryptanalytic** [?]. **Nongovernmental** [?]. **Noninvertible** [?]. **Nonlinear** [?, ?, ?, ?, ?, ?, ?]. **Noordwijkerhout** [?]. **Norm** [?]. **North** [?, ?]. **Northwest** [?]. **Norwegian** [?]. **Note** [?, ?, ?, ?, ?, ?]. **Notebook** [?, ?]. **Notes** [?, ?, ?]. **Nothing** [?]. **Notices** [?, ?]. **Noticing** [?]. **Novel** [?, ?, ?, ?]. **November** [?, ?, ?]. **NSA** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **NSA.gov** [?]. **NSASAB** [?]. **NSUCRYPTO** [?, ?]. **Nuboer** [?]. **Nuggets** [?, ?]. **Nui** [?]. **Null** [?]. **Number** [?, ?]. **number-theoretic** [?]. **Numbers** [?, ?, ?, ?, ?]. **Numbers-Only** [?, ?]. **Numerical** [?, ?]. **NY** [?, ?, ?].

O [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **O-2** [?]. **O.** [?]. **Oberschelp** [?]. **Objects** [?]. **Oblivious** [?, ?, ?, ?]. **Obscure** [?]. **Observations** [?, ?]. **Obtain** [?]. **Obtained** [?]. **OCB** [?, ?]. **occupied** [?]. **OCFB** [?]. **Oct** [?]. **October** [?]. **Oddziału** [?]. **Oded** [?]. **odyssey** [?]. **Off** [?, ?]. **offer** [?]. **Offers** [?]. **Office** [?, ?, ?, ?]. **Officer** [?, ?]. **Officers** [?, ?]. **Official** [?, ?, ?]. **Officially** [?]. **offset** [?]. **Ohio** [?]. **O'Keefe** [?]. **OKW** [?]. **Old** [?, ?, ?, ?, ?]. **Olum** [?, ?]. **Olympiad** [?, ?, ?]. **On-the-Roof** [?, ?]. **One** [?, ?]. **One-Time** [?, ?, ?, ?, ?]. **One-Time-Pad** [?]. **One-Way** [?, ?]. **Online** [?, ?]. **Only** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **OP** [?, ?]. **OP-20-G** [?, ?]. **Open** [?]. **Openness** [?]. **Opens** [?]. **Operating** [?]. **Operation** [?, ?, ?, ?, ?, ?, ?, ?, ?]. **Operational** [?]. **Operations** [?, ?, ?, ?, ?, ?]. **Operator** [?, ?, ?]. **Opinion** [?, ?]. **Opportunities** [?]. **Optimal** [?]. **Optimization** [?]. **Optimized** [?]. **oracle** [?]. **Oral** [?]. **Order** [?, ?, ?, ?]. **Organisational** [?]. **Organization** [?, ?, ?, ?, ?, ?]. **Organizations** [?]. **organized** [?]. **Orient** [?]. **Oriental** [?]. **Origin** [?, ?, ?]. **Original** [?, ?]. **Origins** [?, ?, ?, ?, ?, ?]. **OSS** [?]. **Other** [?, ?, ?, ?, ?, ?, ?]. **OTP** [?, ?]. **Ottoman** [?, ?]. **Out-of-Band** [?]. **Outdated** [?]. **Outline** [?]. **Outreach** [?]. **Outstanding** [?]. **Outstations** [?]. **outwitted** [?]. **Overlapping** [?]. **Overlaps** [?]. **Overview** [?, ?, ?, ?, ?]. **Own** [?, ?, ?]. **Oxford** [?].

P [?, ?, ?, ?, ?, ?, ?, ?, ?]. **Pacific** [?, ?, ?, ?, ?, ?, ?]. **Package** [?]. **Packages** [?]. **Pad** [?, ?, ?, ?, ?, ?]. **Pads** [?]. **Pages** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Painvin** [?]. **Pairing** [?]. **Palatino** [?]. **Pantelimon** [?]. **papal** [?, ?, ?]. **Paper** [?, ?, ?, ?]. **Paperback** [?, ?, ?, ?, ?, ?, ?]. **Papers** [?, ?, ?]. **Parallel** [?, ?, ?]. **Paranoid** [?]. **Parisian** [?]. **parity** [?]. **parity-check** [?]. **Park** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,

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

Q. [?]. **Qaeda** [?]. **QR** [?]. **Quadratic** [?, ?, ?, ?]. **Quantum** [?, ?, ?, ?, ?]. **Quasigroups** [?, ?, ?, ?, ?, ?]. **quaternions** [?]. **Queen** [?]. **quest** [?]. **Question** [?]. **Questions** [?]. **Quick** [?]. **Quinn** [?]. **Quirantes** [?]. **Quisquater** [?]. **Quote** [?, ?]. **quotients** [?].

R [?, ?, ?, ?]. **Rabid** [?]. **Rabin** [?]. **Race** [?, ?]. **Rackoff** [?]. **Radio** [?, ?, ?, ?, ?, ?, ?, ?, ?]. **Rail** [?]. **Ralph** [?, ?]. **RAM** [?]. **Ramón** [?]. **Ramsden** [?]. **Random** [?, ?]. **Random-Key** [?]. **Randomness** [?]. **Randy** [?]. **rank** [?]. **Rapa** [?]. **Rapid** [?, ?]. **Rasterschlüssel** [?, ?]. **Ratcliff** [?]. **Raton** [?]. **Raymond** [?]. **RC4** [?]. **Re** [?, ?, ?]. **Re-Run** [?]. **Read** [?, ?]. **Reader** [?]. **Reading** [?, ?, ?, ?]. **Ready** [?]. **Ready-Made** [?]. **Real** [?, ?, ?, ?, ?, ?, ?, ?]. **Real-Time** [?]. **Realizing** [?, ?]. **Rear** [?]. **Rebecca** [?]. **Rebus** [?]. **Receive** [?]. **Reciprocal** [?, ?]. **Reciprocity** [?]. **Recoding** [?]. **Recognition** [?, ?, ?, ?, ?]. **Recognized** [?]. **Recognizing** [?]. **Recollections** [?]. **Recommendation** [?]. **recommendations** [?]. **Reconciliation** [?]. **reconstructed** [?]. **Reconstruction** [?, ?, ?, ?]. **Record** [?, ?, ?, ?, ?]. **Records** [?, ?, ?, ?, ?, ?]. **Recovered** [?, ?, ?]. **Recovering** [?, ?]. **Recovery** [?, ?, ?]. **Recursive** [?, ?, ?, ?, ?]. **Red** [?]. **Redditch** [?]. **Reducing** [?]. **Redundancy** [?, ?, ?, ?]. **Reed** [?]. **Reeds** [?]. **Reference** [?, ?]. **Reflections** [?, ?, ?, ?]. **Reflective** [?]. **Reflector** [?, ?, ?, ?]. **Reform** [?]. **Regarding** [?, ?]. **Register** [?, ?, ?, ?, ?]. **registers** [?]. **Reich** [?, ?]. **Reihenschieber** [?]. **Reintroduction** [?]. **Rejewski** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Related** [?, ?, ?, ?]. **Related-key** [?]. **Relation** [?]. **Relationship** [?, ?]. **Relative** [?, ?]. **Relatives** [?]. **Relaxation** [?]. **Release** [?]. **releases** [?]. **Remark** [?]. **Remarkable** [?, ?]. **Remarks** [?, ?, ?, ?, ?, ?]. **REME** [?]. **Remember** [?]. **remembered** [?]. **Reminiscence** [?]. **Reminiscences** [?]. **Remote** [?, ?, ?, ?]. **Rempe** [?]. **Rempe-Gillen** [?]. **Renaissance** [?, ?]. **Rent** [?]. **Reorganization** [?]. **repeats** [?]. **Repetitions** [?, ?]. **Replica** [?]. **Reply** [?]. **Report** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Reporter** [?]. **Reports** [?, ?, ?, ?]. **reprint** [?]. **Republic** [?, ?]. **Rescuing** [?]. **Research** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **researching** [?, ?]. **Residue** [?, ?, ?]. **Residues** [?, ?]. **Resource** [?]. **resources** [?]. **Respector** [?]. **Restoration** [?]. **Restraints** [?]. **Results** [?, ?]. **Resurrecting** [?]. **Resurrection** [?]. **Ret** [?]. **retrieved** [?]. **Reunion** [?]. **Reveal** [?]. **Revealed** [?, ?]. **Revealing** [?]. **Reveals** [?, ?]. **Revelation** [?, ?]. **Reveling** [?]. **Reversible** [?]. **Review** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,

Rites [?]. **Ritz** [?]. **River** [?, ?]. **Riverbank** [?, ?, ?, ?, ?, ?, ?]. **Riyadh** [?]. **Różycki** [?, ?]. **Road** [?, ?, ?, ?]. **roaming** [?]. **Rob** [?]. **Robert** [?, ?, ?]. **Roberts** [?]. **Robin** [?, ?, ?]. **Robust** [?]. **Rochefort** [?, ?, ?]. **Rochford** [?]. **Rockex** [?]. **Roger** [?]. **Rohaly** [?, ?]. **Rohonc** [?, ?, ?]. **Role** [?, ?]. **Romanian** [?]. **Ron** [?]. **Ronald** [?]. **rongorongo}** [?, ?, ?, ?, ?]. **Roof** [?, ?]. **Room** [?, ?, ?, ?, ?]. **Roosevelt** [?, ?, ?]. **Roper** [?]. **Rosario** [?]. **Rose** [?, ?]. **Ross** [?, ?]. **rotation** [?, ?]. **ROTERM** [?]. **Roth** [?]. **Rotor** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Rotors** [?, ?, ?]. **Round** [?, ?]. **Row** [?]. **Roy** [?]. **Royal** [?, ?]. **RSA** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **RSA-cryptosystem** [?]. **RT** [?, ?]. **RT-OCFB** [?]. **Rubik** [?]. **Rudyard** [?]. **Rule** [?, ?]. **Ruled** [?]. **Rules** [?, ?]. **Run** [?, ?]. **Runic** [?, ?]. **Running** [?, ?, ?, ?, ?]. **Russell** [?]. **Russia** [?, ?]. **Russian** [?, ?, ?, ?, ?, ?, ?]. **Russo** [?]. **Ryan** [?].

S [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **S-Box** [?, ?]. **S-boxes** [?]. **S.** [?]. **S./CB** [?]. **SA** [?]. **Sacco** [?]. **Saddle** [?, ?]. **Safford** [?, ?]. **Saga** [?, ?]. **Sale** [?]. **Salvo** [?]. **same** [?, ?]. **same-letter** [?]. **Samples** [?]. **Samuel** [?, ?, ?]. **San** [?]. **Sanborn** [?]. **'Santiago** [?]. **Sarah** [?]. **Sarasvatī** [?]. **SAS** [?]. **SAS-SIP** [?]. **Satire** [?, ?]. **Sator** [?]. **SAUDI** [?]. **Savage** [?]. **say** [?]. **Sayers** [?]. **SCAG** [?]. **Scalar** [?]. **SCAMP** [?]. **scan** [?]. **Scatter** [?]. **Scavenger** [?]. **scenario** [?, ?]. **scenarios** [?]. **Schedules** [?]. **Scheme** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Schemes** [?, ?, ?, ?]. **Scheuble** [?]. **Schieber** [?]. **Schmeh** [?, ?, ?]. **Scholarship** [?]. **Scholastic** [?]. **School** [?, ?, ?]. **Schriften** [?, ?]. **Schuster** [?, ?]. **Schwartz** [?]. **Science** [?]. **Scientific** [?]. **Score** [?]. **Scotch** [?]. **Scott** [?, ?]. **Script** [?, ?, ?, ?]. **Sea** [?, ?]. **Seahorse** [?]. **Seal** [?]. **Seals** [?]. **Search** [?, ?, ?, ?, ?, ?]. **Searching** [?, ?]. **Seas** [?]. **SEC** [?]. **SEC-36** [?]. **Second** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Secrecy** [?, ?, ?]. **Secret** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,

Siemens [?, ?, ?, ?, ?]. **SIGABA** [?, ?, ?, ?, ?]. **SIGABA/ECM** [?, ?]. **SIGCUM** [?]. **SIGINT** [?, ?, ?, ?, ?, ?, ?]. **Signal** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Signaling** [?]. **Signalling** [?]. **Signals** [?, ?, ?, ?, ?, ?, ?, ?, ?]. **Signature** [?, ?, ?, ?, ?, ?, ?]. **Signatures** [?, ?]. **Signboard** [?]. **signcryption** [?]. **Significance** [?, ?]. **Signs** [?]. **Silence** [?, ?]. **Silk** [?]. **Silverman** [?]. **Silvestri** [?]. **Silvio** [?]. **Similar** [?, ?]. **Simon** [?, ?]. **Simonetta** [?]. **Simple** [?, ?, ?, ?, ?, ?, ?, ?]. **Simpliciana** [?, ?]. **Simplified** [?, ?, ?, ?, ?, ?, ?]. **Simpson** [?]. **Simulated** [?, ?]. **Simulating** [?]. **Simulation** [?, ?, ?]. **Sinclair** [?, ?, ?]. **Singular** [?]. **Sinkov** [?, ?, ?, ?]. **Sino** [?, ?]. **Sino-American** [?]. **SIP** [?]. **Sir** [?, ?]. **Sirius** [?, ?]. **SIS** [?]. **Situations** [?]. **six** [?]. **Sixty** [?]. **Sizzlers** [?]. **Sketches** [?]. **Skinner** [?]. **Skipjack** [?]. **SKS** [?]. **Skytale** [?, ?]. **Slide** [?, ?]. **Slidex** [?]. **Sliding** [?]. **Slimming** [?, ?]. **Slippery** [?]. **Sloan** [?]. **Slovakia** [?]. **Small** [?, ?]. **Smart** [?, ?, ?]. **Smashed** [?]. **Smith** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Smithsonian** [?, ?]. **Smolenice** [?]. **Smoot** [?, ?]. **SMS** [?]. **Social** [?]. **Societies** [?]. **Society** [?, ?, ?]. **Softcover** [?]. **Software** [?, ?, ?, ?, ?]. **Software-Based** [?]. **Sois** [?]. **Soler** [?]. **SOLO** [?]. **Solomon** [?]. **Solution** [?, ?]. **Solutions** [?, ?, ?, ?, ?, ?]. **Solve** [?]. **Solved** [?, ?, ?, ?, ?, ?, ?]. **Solving** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Some** [?, ?]. **Somerton** [?]. **Soni** [?]. **Sought** [?]. **sound** [?]. **Source** [?, ?]. **Sources** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **South** [?, ?]. **Southampton** [?]. **Soviet** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Space** [?, ?]. **Spain** [?]. **Spanish** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Spanning** [?]. **Speaks** [?]. **Special** [?, ?, ?, ?, ?, ?, ?, ?]. **specific** [?]. **specification** [?]. **Spectral** [?]. **Speech** [?, ?, ?]. **Speed** [?, ?]. **Speeding** [?]. **Spell** [?]. **Spelling** [?]. **Spies** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Spigot** [?]. **Spilled** [?]. **Spillman** [?]. **spoils** [?]. **Spread** [?]. **Sprevak** [?]. **Springer** [?, ?, ?]. **Springer-Verlag** [?, ?]. **SPSIS** [?]. **SPSIS-1** [?]. **Spy** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Square** [?, ?]. **squares** [?]. **SRH** [?]. **SRH-50** [?]. **SS** [?]. **St.** [?]. **Stadholder** [?]. **Stadtholders** [?]. **Staff** [?, ?, ?]. **Stage** [?]. **stake** [?]. **Stand** [?]. **Standard** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Standardisation** [?]. **Standards** [?, ?, ?]. **Stanica** [?]. **Stanley** [?]. **Stanoyevitch** [?]. **Starch** [?]. **State** [?, ?]. **Statement** [?]. **States** [?, ?, ?, ?, ?]. **Statesman** [?]. **Station** [?, ?, ?, ?, ?, ?, ?]. **Stations** [?]. **Statistical** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?]. **Statistics** [?, ?, ?, ?]. **Stealing** [?]. **Steganografie** [?, ?, ?]. **Steganographia** [?, ?]. **Steganography** [?, ?, ?, ?, ?, ?, ?]. **Stephen** [?, ?, ?]. **Stepping** [?, ?]. **Steps** [?]. **Sterling** [?, ?]. **Steven** [?]. **Stevenhagen** [?]. **Still** [?]. **Stimson** [?, ?, ?]. **Stinson** [?]. **Stonka}** [?]. **storage** [?]. **Stories** [?]. **Story** [?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,

Style [?]. **Stylometric** [?]. **submarine** [?]. **submarines** [?]. **Submitted** [?]. **Substitution** [?, ?, ?,

[?]. **Treatise** [?, ?]. **Treatment** [?]. **Treaty** [?]. **Tree** [?]. **Trevor** [?]. **Trevor-Roper** [?]. **Trial** [?]. **Tribute** [?, ?, ?, ?]. **Tricks** [?, ?]. **Tries** [?]. **Trigraph** [?]. **Trip** [?]. **Triples** [?]. **Trist** [?]. **Trithemius** [?, ?, ?]. **Triumph** [?, ?, ?]. **triumphant** [?]. **tropical** [?]. **Trove** [?]. **TRS** [?, ?]. **TRS-80** [?, ?]. **True** [?, ?]. **Truman** [?]. **Truppenschlüssel** [?]. **Trussoni** [?]. **Trust** [?, ?]. **Trusted** [?]. **truth** [?]. **Tsarist** [?, ?]. **TST** [?, ?]. **TST-1221** [?]. **Tuchman** [?]. **Tunny** [?]. **Turing** [?, ?, ?,

War [?, ?, ?,