Evaluations of sources

|  |  |  |  |
| --- | --- | --- | --- |
| Source | Type of source | Evaluation | Usable? |
| Section 1 – History of Cryptography | | | |
| Simon Singh, The Cracking Codebook, 2001 | Book | Singh is a physicist and has written other mathematical books. Therefore, to have written multiple books his writing must be reasonably accurate and his mathematical background may give him cryptographical expertise. | Yes |
| Steve Burnett, Stephen Paine, RSA Security’s Official Guide to Cryptography, 2001 | Book | RSA Security is a computer and network company, focusing on encryption. Therefore it is likely that the book they produce will reflect this expertise. | Yes |
| Thales Group, “https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption”, 1 Feb 2023 [Online] | Website article | Thales Group is an IT company that works in encryption and so would likely have greater expertise in this field than average. | Yes |
| Fauzan2001, “https://cryptozine.blogspot.com/2008/05/brief-history-of-cryptography.html”, 20 May 2008 [Online] | Blog | This source is an online blog written by someone who may not have any professional expertise in this subject and so may not be completely reliable or accurate. | No |
| Dan Froomkin and Amy Branson, “https://www.washingtonpost.com/wp-srv/politics/special/encryption/encryption.htm”, 8 May 1998 [Online] | Online edition of a newspaper. | This piece is produced by a newspaper, the Washington Post and so it may not be totally accurate.  The source is also quite old. However, since it is being used to write about historical encryption this is not a concern. | Yes |
| Tresorit, “https://tresorit.com/blog/the-history-of-encryption-the-roots-of-modern-day-cyber-security/”, 14 Jan 2022 [Online] | Website article | Tresorit is an IT Cloud company which uses encryption in their products and so would likely have greater expertise in this field than average. | Yes |
| RedHat (Huzaifa Sidhpurwala), “https://www.redhat.com/en/blog/brief-history-cryptography”, 12 Jan 2023 [Online] | Blog | The author is a Principal Product Security Engineer for Red Hat Products (an open source technologies company) , implying he has some knowledge of the subject matter (as this would be part of security). | Yes |
| S.M. Naser “https://www.researchgate.net/publication/353999208\_CRYPTOGRAPHY\_FROM\_THE\_ANCIENT\_HISTORY\_TO\_NOW\_IT'S\_APPLICATIONS\_AND\_A\_NEW\_COMPLETE\_NUMERICAL\_MODEL”, July 2021 [Online] | Journal Article | I have decided not to use this source due to consistently poor grammar (so it may be hard to find a quote without an error) and this lack of care for grammar may suggest a lack of quality throughout. | No |
| GIAC (Roger A. Prichard), “https://www.giac.org/paper/gsec/1555/history-encryption/102877”, 26 Jan 2002 [Online] | PDF document | GIAC is a cyber security body that trains and certifies people and therefore would have expertise in the field of encryption as it forms a part of that field. However, this source does sometimes have poor grammar which could indicate a lack of care for quality. | Yes |
| Axel, “https://www.axel.org/2021/05/28/history-of-encryption/”, 28 May 2021 [Online] | Website article | Axel is a computing and networks company. However, it does not appear to have any particular expertise in encryption, and I believe the source is aimed at quite an uneducated reader, making it less useful. | Yes |
| R.A. Mollin, “https://cubo.ufro.cl/ojs/index.php/cubo/article/view/1645/1496”, March 2004 [Online] | Journal Article | This article was submitted to a mathematical journal, who would have checked that it was accurate and good quality before running it. | Yes |
| Milica Djekic, “http://ozscience.com/technology/a-scytale-cryptography-of-the-ancient-sparta/“, 2013 [Online] | Website article | The website is run by the independent initiative for advancement of science and research in Australia. The writer of this particular article also has knowledge of data security and mathematics suggesting they are capable of dealing with the subject matter well. | Yes |
| April Lia Hananto, Arip Solehudin, Agung Susilo Yuda Irawan and Bayu Priyatna, “https://arxiv.org/abs/1912.04519”, 10 Dec 2019 [Online] | Journal Article | This article was published in the International Journal of Computer Techniques, who would have reviewed and edited the article to correct any mistakes or inaccuracies before running it, making the source more reliable. | Yes |
| Yumnam Kirani, “https://www.researchgate.net/profile/Yumnam-Kirani/publication/235741546\_Generalization\_of\_Vigenere\_cipher/links/0fcfd51304111ad522000000/Generalization-of-Vigenere-cipher.pdf”, Jan 2012 [Online] | Journal Article | This article was published in the ARPN Journal of Engineering and Applied Sciences. It is likely that they would have reviewed the article and checked the information, making the source more reliable. | Yes |
| Dirk Rijmenants, “https://www.ciphermachinesandcryptology.com/papers/is\_one\_time\_pad\_history.pdf”, May 2022 [Online] | Website Article | The website this article is hosted on is dedicated to technical and historical information about cipher machines and cryptology. Therefore, they would have knowledge of the subject matter and while the article is intended partly to be persuasive, I do not intend to reference the persuasive parts in my essay so this will not be a problem. | Yes |
| Alex Biryukov, Christophe De Canniere, “https://orbilu.uni.lu/bitstream/10993/17076/1/Data-Encryption-Standart-DES-Encyclopedia-article.pdf“, 2011 [Online] | PDF document | The authors have written a second article on cryptography, suggesting they have expertise in the subject matter (one works in Communications Research Unit at the University of Luxembourg) and their knowledge means that this source is more likely to be accurate and reliable. | Yes |
| Kefa Rabah, “https://www.researchgate.net/profile/Kefa-Rabah-2/publication/45949430\_Theory\_and\_Implementation\_of\_Data\_Encryption\_Standard\_A\_Review/links/02e7e51af7fd2a3cbb000000/Theory-and-Implementation-of-Data-Encryption-Standard-A-Review.pdf”, April 2005 [Online] | Journal Article | This article was published in the Information Technology Journal, so it is likely that it would have been inspected for errors and that it is a credible and accurate piece of writing. | Yes |
| Susan Landau, “https://www.ams.org/journals/notices/200003/fea-landau.pdf?trk=200003fea-landau&cat=collection”, Mar 2000 [Online] | Journal Article | This article was published in the American Mathematical Society. The topic it discusses in detail the mathematics, and so it is likely to be more accurate than a source of less mathematical origin. | Yes |
| Evgeny Milanov, “https://pdfdirectory.com/pdf/0702-the-rsa-algorithm.pdf”, 3 Jun 2009 [Online] | PDF document | This document was submitted to the University of Washington, who would have checked it for quality and accuracy, making it more reliable. | Yes |
| Vivek Kapoor, Vivek Sonny Abraham, Ramesh Singh, “https://dl.acm.org/doi/pdf/10.1145/1386853.1378356”, May 2008 [Online] | Journal Article | The source was published in a journal run by the Association for Computing Machinery. This would include encryption the source discusses as it is carried out using computers, and so is within their expertise, making the source more trustworthy. | Yes |
| Douglas Selent, “https://www2.rivier.edu/journal/roaj-fall-2010/j455-selent-aes.pdf”, Fall 2010 [Online] | Journal Article | This article was published in the Rivier Academic Journal. This journal has no particular expertise in cryptography or even computing, so it may be less accurate. However, the work should still be to a reasonably high standard for a journal to accept it. | Yes |
| Kuriakkottu Amalraj Rajan, “https://journal.ijresm.com/index.php/ijresm/article/view/1556”, 2 Dec 2021 [Online] | Journal Article | I have decide not to make use of this source due to its poor grammar, too short to include much detail and most of it can be found elsewhere. | No |
| Dwiti Pandya, Khushboo Ram Narayan, Sneha Thakkar, Tanvi Madhekar, B.S. Thakare, “https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=b861e8de6f3fa5e7aba25d06daa5fa7d45f54f93”, Dec 2015 [Online] | Journal Article | The International Journal of Computer Applications published this source, and their editor would have carried out checks on the content. | Yes |
| Tony M. Damico, “http://www.inquiriesjournal.com/articles/1698/a-brief-history-of-cryptography”, 2009 [Online] | Journal Article | This article was published on the Inquiries Journal website. However, this site has a particular focus on the social sciences, arts, and humanities, so its articles on encryption may be less useful/accurate. | Yes |
| Section 2 – Quantum Mechanics and Quantum Computing | | | |
| Brian Clegg, The God Effect, 2006 | Book | Brian Clegg has studied Natural Science (specialising in experimental physics) at the University of Cambridge and has written a number of other science books, suggesting that he has expertise in his field. This makes this source more reliable. | Yes |
| John Gribbin, Computing with Quantum Cats, 2013 | Book | The author has a masters in Physics from the University of Sussex and has written several other books on quantum physics as well as many in the scientific field. This shows he has expertise in quantum computing and is more likely to be an accurate and trustworthy source. | Yes |
| George Johnson, A Shortcut Through Time – The Path To The Quantum Computer, 2003 | Book | The author, George Johnson is a Science author who writes for the New York Times and has written several other science based books, suggesting that he is experienced in this field and is a trustworthy source. | Yes |
| Eleanor Rieffel, Wolfgang Polak, “https://dl.acm.org/doi/pdf/10.1145/367701.367709”, 3 Sept 2000 [Online] | Journal Article | This article is aimed at helping non-physicists understand how quantum computing differs from conventional computing. It may be simplified slightly to help it do this. However, I am also intending to simply my section on quantum computing for the same reasons, so this should not be a problem. | Yes |
| Ajit Narayanan, “https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=c5a58aa3662b027a1d5ae38f460ddc0edf16e2d0”, 1999 [Online] | Journal Article | This article was accepted by the University of Exeter, a Russell Group university so it must be to a reasonably high standard and be accurate. | Yes |
| Donald Krambeck, “https://www.allaboutcircuits.com/technical-articles/fundamentals-of-quantum-computing”, 6 Aug 2015 [Online] | Website article | All about circuits is a publication and forum for electrical engineers. The writer is also an electrical engineer and so it is likely he would have an above average understanding of the subject matter. | Yes |
| Carolyn Mathas,  “https://www.edn.com/the-basics-of-quantum-computing-a-tutorial/”, 13 Aug 2019 [Online] | Website article | This website is run by EDN (electronic design news), an engineering group. Therefore it is likely they will have some understanding of the topic. However, they and the author do not appear to have any specific knowledge of quantum computing which may make it less accurate. | Yes |
| Yoshito Kanamori, Seong-Moo Yoo, “https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1410&context=jitim”, 2020 [Online] | Journal Article | This article is from the Journal of International Technology and Information Management. Quantum computing would fall inside their expertise and the article would have been reviewed to ensure it is of appropriate quality, making the source more reliable. | Yes |
| Jeff Desjardins, “https://www.visualcapitalist.com/three-types-quantum-computers/”, 14 Mar 2016 [Online] | Website article | Visual capitalist is a site that helps discover new business and investment opportunities. However, this could mean it makes quantum computing look more powerful and advanced than it really is and may be simplified to help people without a scientific background understand the subject. | No |
| Charles H. Bennett, Ethan Bernstein, Gilles Brassard, Umesh Vazirani, “https://arxiv.org/pdf/quant-ph/9701001.pdf”, 12 Dec 1996 [Online] | Journal Article | This article appeared in the Society for Industrial and Applied Maths Journal on Computing. They would have expertise in the field of quantum computing, making this source more likely to be accurate and trustworthy. | Yes |
| Matt Swayne, “https://thequantuminsider.com/2023/03/24/quantum-computing-challenges/”, 24 Mar 2023 [Online] | Website Article | The Quantum Insider is a site dedicated to provided news and articles on quantum computing. As this is the sites only subject, it is likely that they are accurate and relatively reliable. | Yes |
| Section 3 – The Threat Quantum Computers Pose and How It Can Be Mitigated | | | |
| Roger A. Grimes, Cryptography Apocalypse – Preparing For The Day When Quantum Computing Breaks Today’s Crypto, 2020 | Book | The author of the book is a computer security expert who has written multiple other hacking/security related books. | Yes |
| Marco A. Barreno, “https://digitalcommons.dartmouth.edu/cgi/viewcontent.cgi?article=1022&context=senior\_theses”, 21 Jul 2002 [Online] | Thesis | This source was a thesis at Dartmouth College. However, as it is only a thesis, rather than being written by an established scientist or author, it may be less reliable or accurate. | Yes |
| Paul Bikram, **“**http://gyan.iitg.ac.in/handle/123456789/2258”, 2023 [Online] | Thesis | This was a thesis at the Indian Institute of Technology. Since the institute would focus on technology, their theses in this field would likely be more reliable and accurate than average, making this a somewhat trustworthy source. However, it has not been written by someone with experience, making it less useful. | Yes |
| Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Jøsang, “https://arxiv.org/pdf/1804.00200.pdf”, 2018 [Online] | Journal Article | This article was published in the International Journal of Advanced Computer Science and Applications, so it is likely that it would have been reviewed for errors and that it is a high quality and accurate piece of writing. | Yes |
| William Buchanan, Alan Woodward, “https://www.tandfonline.com/doi/pdf/10.1080/23742917.2016.1226650”, 20 Sep 2016 [Online] | Journal Article | The Journal of Cyber Security Technology published this source, suggesting that it is accurate and reliable. | Yes |
| Tohfa Niraula, Aditi Pokharel, Ashmita Phuyal, Pratistha Palikhel, Manish Pokharel, “https://www.mecs-press.org/ijwmt/ijwmt-v12-n5/IJWMT-V12-N5-2.pdf”, 2022 [Online] | Journal Article | This source is from the Modern Education and Computer Science Press which suggests it has been reviewed and edited, making it a more reliable source. | Yes |
| Zach Kirsch, “https://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf”, 15 Dec 2015 [Online] | University Article | This article was accepted by Tufts university so it must be to a reasonably high standard and be accurate. | Yes |
| Anne Broadbent, S´ebastien Lord, “https://arxiv.org/pdf/1903.00130.pdf”, 8 Oct 2019 [Online] | University Article | This article was accepted University of Ottawa, so it is to a university standard and has been researched thoroughly, suggesting it is a good source. | Yes |
| Douglas Stebila, Michele Mosca, “https://link.springer.com/chapter/10.1007/978-3-319-69453-5\_2”, 20 Oct 2017 [Online] | Conference paper | This is part of the series Lecture Notes in Computer Science a medium for the publication of new developments in computer science and information technology research, teaching, and education which has existed since 1973 and so must be of high quality and useful. | Yes |
| Daniel J. Bernstein, Tanja Lange, “https://eprint.iacr.org/2017/314.pdf”, 2017 [Online] | University Article | This article was accepted by 2 universities so it must be high quality and accurate, making it a trustworthy source. | Yes |
| William Barker, William Polk, Murugiah Souppa, “https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf”, 28 April 2021 [Online] | NIST Cybersecurity White Paper | This source was produced by NIST the (American) National Institute of Standards and Technology. They would be an authority on the subject of standard quantum proof encryption and this makes the source more credible and trustworthy. | Yes |
| Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Duˇsek, Norbert L¨utkenhaus, Momtchil Peev, “https://arxiv.org/pdf/0802.4155.pdf”, 30 Sept 2009 [Online] | Scholarly Article | Most of the authors come from physics departments at universities, several from quantum technologies departments. This makes it likely that they are experts in the field and their work is reliable and accurate. | Yes |