

Math 311w-01 Lab 3: Information

<http://www.libraries.psu.edu/psul/researchguides/phycimath/math.html>

How can you trust information you find on the Internet? Where can you find an answer that is detailed enough to be useful, but not too complex for you to understand? Since anyone can publish information instantly on the World Wide Web distinguishing quality information can be very difficult. Before the coming of the information age, there were only a few options for research – books, magazines, and scholarly journals.

Scholarly journals (also called academic, peer-reviewed, or refereed journals) are the traditional method of communicating new scientific discoveries. Authors generally submit their articles to several other scientists for review and comment, and these reviewers must approve the article before it is published. Since the audience is other scientists, the language used is highly technical and specific to the field. Scholarly journals are one type of primary source for research.

Primary sources are newly created or recorded knowledge by a scientist or researcher. These can be scholarly journal articles, scientific reports or even an in-person presentation. Secondary sources review, discuss, or analyze primary sources and are written later. Some examples of secondary sources are encyclopedia articles, science news reports, and most books.

Both types of information sources may have citations, references to earlier research. Citations in a primary source are an acknowledgement of previous research and give a link between earlier knowledge and the current study. Citations in a secondary source indicate where the author got the information they used to write their review of the topic.

For this lab, work in groups of two at each computer. Take notes on what you find on the back.

1. Visit the Wikipedia article for RSA Cryptography (<http://en.wikipedia.org/wiki/RSA>) and go to the Notes, References and External links. Since this article is a secondary source, these are the many information sources used to create it. Identify the type of information source (scholarly journal article, book, etc) for each of the five references on the back of this worksheet.
2. For each of the five, evaluate it on the following criteria:
 - a. Authority – who is the author and what is their level of expertise
 - b. Audience – who is the article written for and at what level is the article written
 - c. Currency – how recent is the article and does that matter
 - d. Content – could you understand and use the article for a paper in this class
3. Now go to Lionsearch (<http://psu.summon.serialsolutions.com>) and find a scholarly article on RSA Cryptography that you think has high quality in those four criteria and cite it below.

NOTES

1. Rivest, R., A. Shamir, L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"

2. SIAM News, Volume 36, Number 5, June 2003

7. Don Coppersmith, "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities", Journal of Cryptology, v. 10, n. 4, Dec. 1997

References

Menezes, Alfred; Paul C. van Oorschot; Scott A. Vanstone (October 1996). Handbook of Applied Cryptography.

External Links

Rivest; Ronald L. (Belmont, MA), Shamir; Adi (Cambridge, MA), Adleman; Leonard M. (Arlington, MA), December 14, 1977, U.S. Patent 4,405,829