{tag} {/tag}International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 131
-
Number 9

Year of Publication: 2015

Authors:

Dwiti Pandya, Khushboo Ram Narayan, Sneha Thakkar, Tanvi Madhekar, B.S. Thakare

10.5120/ijca2015907390
{bibtex}2015907390.bib{/bibtex}

Abstract

Secure communication has been required since thousands of years. This led to the invention of cryptography. In ancient world, primitive methods were adopted for passing messages secretly. But with the invention of internet and world wide web, which is used for communicating via mail, messages, online shopping, online banking, etc., increased the need of information security. Thus a proper understanding of various methods of cryptography and its implementation can fulfill the requirements of securing valuable and sensitive information. This paper takes us through the various methods of cryptography adopted in the ancient period, medieval period and the modern era.

References

1. “History of cryptography.” Wikipedia: The Free Encyclopedia. Wikimedia Foundation, Inc. 5th November 2015. Web. 10th November 2015.

2. “Cryptography.” Wikipedia: The Free Encyclopedia. Wikimedia Foundation, Inc. 27th November 2015. Web. 29thNovember2015.
3. The Evolution of Cryptography. (n.d.). Retrieved November12,2015,fromhttp://www.sherpasoftware.com/blog/the-evolution-of-cryptography/
4. Bellare, M., Rogaway, P., 2005. Introduction to modern cryptography.
5. J. Daemen and V. Rijmen. The Design of Rijndael. Springer, 2001.
6. M. Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. SIAM J. Comput, Vol. 17, No. 2, April 1988.

Index Terms

Computer Science Security

Keywords

AES, DES, MD4, RC4, SHA, SIGABA