

APPLIED CRYPTOGRAPHY FOR SECURE SYSTEM

SURAJ SINGH PANWAR

Department of Computer Science, H.N.B.Garhwal Central University,
Srinagar (Garhwal), Uttarakhand

ABSTRACT

Communication System has been one of the chief needs of the human social life. But it is noteworthy that if the communication is confidential than it becomes obvious to secure that against the illegal use or from hacker. With the changing physical and psychological scenarios, the methods of sending and securing messages have changed too. Cryptography is a technique which is being used for securing the messages from ancient time. Although it has gone through several changes as the centuries passed but even today it is the most trusted technique to secure the messages. By using different cryptographic method, we can provide our computer system or other communication system security. So illustration of cryptography and how does it comes into action, as well as the need of cryptography in modern scenario is necessary and essential for each user. This paper focuses on cryptography, OSI Security Architecture, model of cryptographic system, techniques for encryption from history to modern age and purpose for security requirements.

Keywords: Cryptography, History, OSI, Legal issues Computer crimes

REFERENCES

1. "Cryptography and Network Security" Principles and Practices by William Stallings.
2. "Data Communication and networking" by Behrouz A. Forouzan.
3. "Introduction to Modern Cryptography" by Jonathan Katz.
4. "Introduction to Modern Cryptography" by Mihir Bellare and Phillip Rogaway.
5. RSA Laboratories' Frequently Asked Questions About Today's Cryptography.
6. www.kremlinencrypt.com
7. www.cipherbyritter.com
8. www.cypher.com
9. www.searchsecurity.com
10. www.howstuffworks.com
11. www.cryptographyworld.com