International Journal of Engineering, Applied and Management Sciences Paradigms, Vol. 01, Issue 01, February 2013
ISSN (Online): 2320-6608
www.ijeam.com

Cryptography: The Need for Today's Networks and its other Aspects

Martin Dev

Research Scholar, Abu Dhabi, United Arab Emirates

Abstract

There are so many branches of computer science but cryptography has its own importance. Any researcher should be aware of this technology so that the possibility of stolen of data can be reduced. The researcher should study this topic in very detail so that the all aspect of this branch can be used to make data more secure. Also cryptography is very interesting thing to learn and to be expert in this technique. This paper is about the different aspects of this technique.

Keywords: *Cryptography, Ciphers, Symmetric and Non-symmetric Cryptography.*

Introduction

Cryptography is taken from Greek word and the meaning is hidden or secret. The meaning is that there is secure communication between two persons or machines even in the presence of third party. And for third party the happening things are unknown. In this topic, sometimes it has to face legal issues. I am explaining an example of USA where at one time the supreme court of USA said that the criminals can use this technology for their wrong things. So there should be some steps so that government should control on the criminals to do wrong things. Today this the need of networks to make them more secure and apply this technology for making privacy of data records which are very important for everyone.

Types of Cryptography

Symmetric Key Cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976. This is just like a lock which is open and closed by the same key and same mechanism.

Public Key Cryptography

This is the cryptography where sender and receiver having different keys to encrypt and decrypt. One pair of keys is used to encrypt the data and another pair of data is there to decrypt the data.

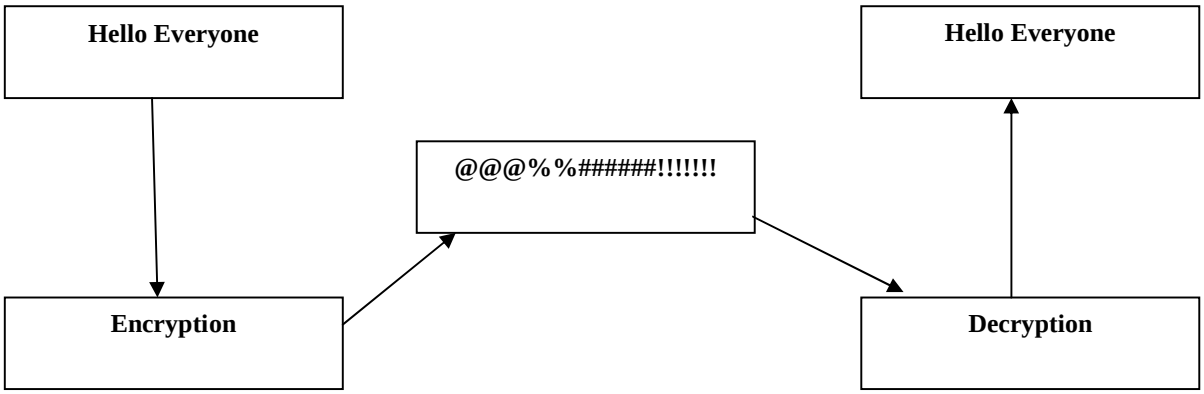

Figure 1: The Cryptography Magic

Aim of New Methodologies

To find weak points in the cryptographic schemes and make these more and more strong so they cannot be broken by intruder.

Cryptanalysis of symmetric-key ciphers typically involves looking for attacks against the block ciphers or stream ciphers that are more efficient than any attack that could be against a perfect cipher.

The Government Issues

There may be restrictions from government side assuming that the secret information may be used by criminals and such type of other peoples by communication between them.

The control of the government may be in some algorithm, they want there should be a central agency which will also having information regarding the secure communications.

The government want there should be digital right management and they should give digital signature so that in future they can trace the person doing some wrong things.

The government influence in the techniques can be understood by example of NSA involvement in USA. In USA it is passed that there should be involvement of security agencies in the development of new ciphers and also the fundamentals regarding those and at least NSA should know that method so that in future the criminal mind persons can be traced by finding their encrypted informations.

Conclusion

Finally we conclude that cryptography is very important for everyone. Everyone should learn it and uses its technique for securing their data. Also should learn the deep knowledge of the cryptography so that

this may a strong oppose to the intruders. The different aspects of this technique useful in the different fields and can be used for secure systems. So we can also conclude that while using this technology for people, the government issues are also very important.

References

[1] R. Rivest, A. Shamir, L. Adleman A Method for Obtaining Digital Signatures and Public-Key Cryptosystems Communications of the ACM, Vol. 21 (2), pp120–126 (1978). Previously released as an MIT "Technical Memo" in April 1977, and published in Martin Gardner's Scientific American Mathematical recreations column

[2] "British Document Outlines Early Encryption Discovery". New York Times Retrieved 2012-03-27.

[3] Clifford Cocks. A Note on 'Non-Secret Encryption', CESG Research Report, 20 November 1973.

[4] Singh, Simon (1999). The Code Book Doubleday pp 279–292

[5] "Shannon": Claude Shannon and Warren Weaver, the Mathematical Theory of Communication, University of Illinois Press, 1963, ISBN 0-252-72548-4

[6] Pascal Junod, "On the Complexity of Matsui's Attack", SAC 2001

[7] Dawn Song, David Wagner, and Xuqing Tian, "Timing Analysis of Keystrokes and Timing Attacks on SSH", In Tenth USENIX Security Symposium, 2001.