Survey on Various Most Common Encryption Techniques

Vikram Singh, Jaspal Ramola
B.Tech, Dept. Of Computer Science Engineering,
Dronacharya College Of Engineering, Gurgaon, India

Abstract- **This paper will present a perspective on the current field of encryption algorithms, in particular on private key block ciphers which are widely used for bulk data and link encryption. We have initially survey some of the more popular and interesting algorithms currently in use. This paper focuses mainly on the different kinds of encryption techniques that are existing, and comparative study all the techniques together as a literature survey. Aim an extensive experimental study of implementations of various available encryption techniques. Also focuses on encryption techniques, information encryption techniques. This study extends to the performance parameters used in encryption processes and analyzing on their security issues.**

I. INTRODUCTION

The high growth in the networking technology leads a common culture for interchanging of the data very drastically. Hence it is more vulnerable of duplicating of data and re-distributed by hackers. Therefore the information has to be protected while transmitting it, Sensitive information like credit cards, banking transactions and social security numbers need to be protected. For this many encryption techniques are existing which are used to avoid the information theft. In recent days of wireless communication, the encryption of data plays a major role in securing the data in online transmission focuses mainly on its security across the wireless. Different encryption techniques are used to protect the confidential data from unauthorized use. Encryption is a very common technique for promoting the information security. The evolution of encryption is moving towards a future of endless possibilities. Everyday new methods of encryption techniques are discovered. This paper holds some of those recent existing encryption techniques and their security issues.

II. BASIC TERMS USED IN CRYPTOGRAPHY

Plain Text

The original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. For example, Alice is a person wishes to send "Hello Friend
how are you" message to the person Bob. Here "Hello Friend how are you" is a plain text message.

Cipher Text

The message that cannot be understood by any one or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message. For example, "Ajd672#@91ukl8*^5%" is a Cipher Text produced for "Hello Friend how are you".

Encryption

A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The
process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes
place at the sender side.

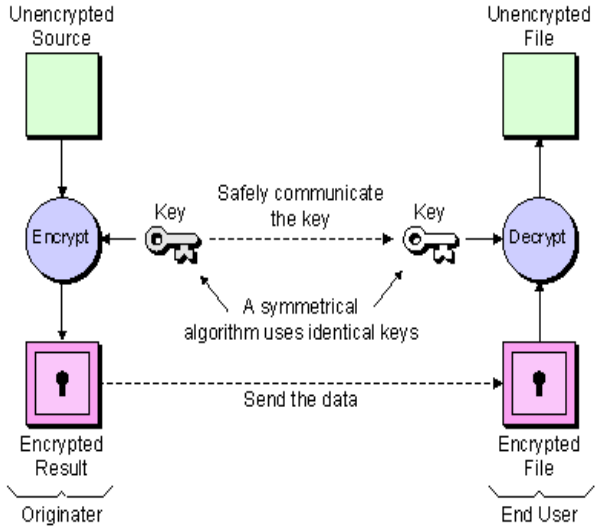
Decryption

A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption

algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.

Key

A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. For example, if the Alice uses a key of 3 to encrypt the Plain Text "President" then Cipher Text produced will be "Suhvlghqw"



Encryption Technique

III. PURPOSE OF CRYPTOGRAPHY

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and soon. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

Confidentiality

Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

Authentication

The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

Integrity

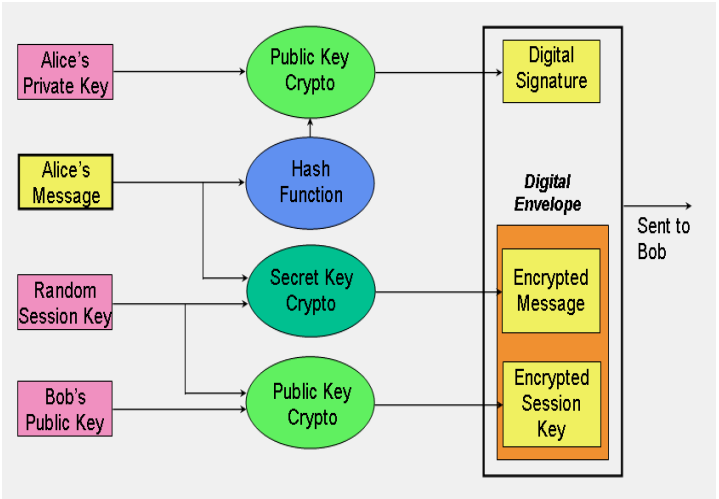
Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

Non Repudiation

Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

Access Control

Only the authorized parties are able to access the given information.



Encryption technique

IV. CLASSIFICATION OF CRYPTOGRAPHY

Encryption algorithms can be classified into two broad categories- Symmetric and Asymmetric key encryption.

Symmetric Methods

Symmetric cryptography, also called private-key cryptography, is one of the oldest and most secure encryption methods. The term "private key" comes from the fact that the key used to encrypt and decrypt data must remain secure because anyone with access to it can read the coded messages. A sender encodes a message into cipher text using a key, and the receiver uses the same key to decode it.

People can use this encryption method as either a "stream" cipher or a "block" cipher, depending on the amount of data being encrypted or decrypted at a time. A stream cipher encrypts data one character at a time as it is sent or received, while a block cipher processes fixed chunks of data. Common symmetric encryption algorithms include Encryption Standard(DES), Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA).

Asymmetric Forms

Asymmetric or public key, cryptography is, potentially, more secure than symmetric methods of encryption. This type of cryptography uses two keys, a "private" key and a "public key," to perform encryption and decryption. The use of two keys overcomes a major weakness in symmetric key cryptography, since a single key does not need to be securely managed among multiple users.

In asymmetric cryptography, a public key is freely available to everyone and used to encrypt messages before sending them. A different, private key remains with the receiver of cipher text messages, who uses it to decrypt them. Algorithms that use public key encryption methods include RSA and Diffie-Hellman.

V. CONCLUSION

In this wireless world nowadays, the security for the data has become highly important since the communication by transmitting of digital products over the open network occur very frequently. In this paper, it has been surveyed that the existing works on the encryption techniques. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. To sum up, all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security.

REFERENCES

[1] William Stallings " Network Security Essentials (Applications and Standards)", Pearson Education, 2004.