Analysis of Cryptography and It's Importance in Security System

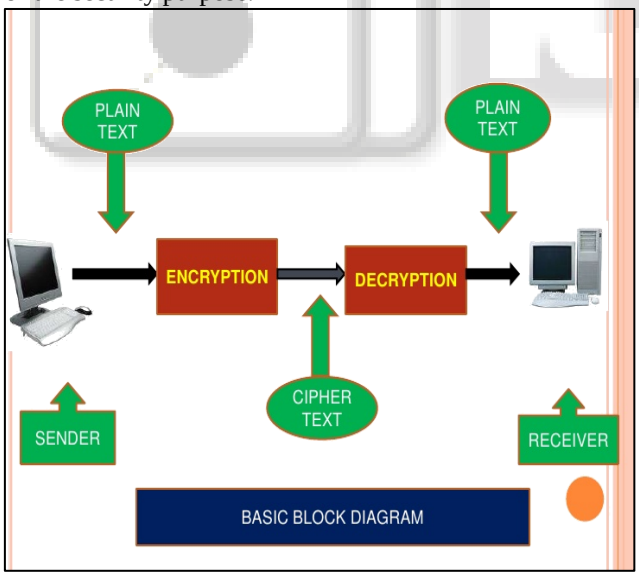
Nikhil Rawat[1] Mohd. Bilal Ansari[2] Divyani Jigyasu[3]
[1,2]Student [3]Associate Professor
[1,2,3]Department of Computer Science and Engineering
[1,2,3]Arya Institute of Engineering & Technology, Jaipur, Rajasthan, India

Abstract— As we know that data is very much important for the users. Data is any type of storing digital information. Data security refers to the technique to secure the data from the unauthorized users to computers and websites. Cryptography is an evergreen technique of it. Cryptography protect users by providing functionality of encryption for the data. cryptography is a popular way of sending the vital information in a secret way by using some techniques. There are many types of cryptography techniques are used but among them AES (advanced encryption system) is one of the powerful technique. The scenario of today's information security system includes confidentiality, integrity and authenticity.

Keywords: AES (advanced encryption system), Cryptography

I. Introduction

Security goals for data security are confidentiality, integrity, authenticity and non-repudiation. Data security delivers the data in a protected manner across enterprise. More and more IT firms are move towards the cryptography technique to secure their valuable data and information. Cryptography convert the plain text (user data) into cipher text(coded data) for the security purpose.



II. Cryptography

A. What is Cryptography?

Cryptography is a method of storing and transmitting the data in a particular form so that only that person can process it for whom it is intended. Cryptography includes many techniques such as microdots, merging text with image to hide information in storage. In today's computer world this technique is often used for securing the data. Many IT firms or organizations are moving towards this technique to secure their valuable data.

Cryptography converts plain text(ordinary text, sometimes referred to as clear text) into cipher text(a process called encryption) and back cipher text to plain text(called decryption). Cryptography used encryption and decryption process to transmit the data.

To hide any data two techniques are generally used one is cryptography and another is stenography. In this paper we used cryptography. Cryptography is the art of protecting data, which provides method of converting plain data into unreadable form, so that only the valid user can access that information at their destination.

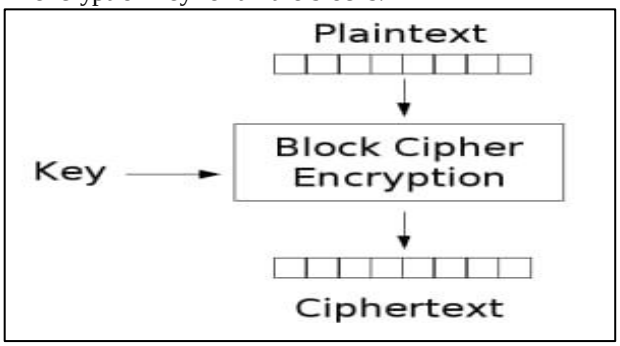
B. Cryptography Objectives

There are four objectives namely:

1) Confidentiality: it is the most important goal, that ensures that nobody can understand the message except the one for whom it was intended and who got the permission to read it or has the decipher key.
2) Integrity: it ensures that the received message has not been changed to its original sending message. The information cannot be altered in transit between the sender and receiver.
3) Authentication: in this, the sender and receiver can confirm their identity and the origin/destination of the information before transmitting any data or message.
4) Non-repudiation: it is a mechanism that proves that the sender really sent this message, and the message is received by the recipient, so the receiver cannot claim that the message was not sent.

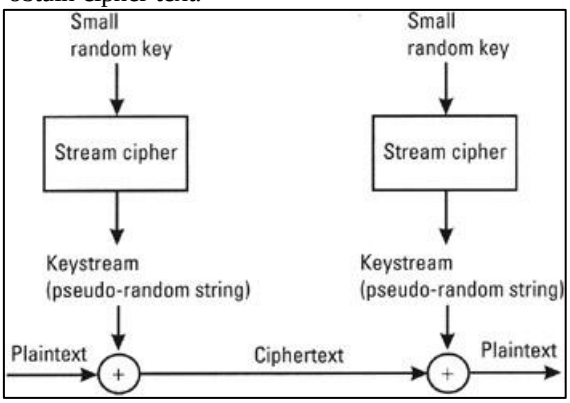
There are two more encryption algorithm are used in modern cryptography technique they are block cipher and stream cipher:

– Block Cipher: The block cipher uses a deterministic algorithm that performs operations on fixed length data or fixed groups of bits. The basic idea behind block cipher is that it divides the text into relatively large block, typically of 64 bits or 128 bits long and encode each block separately. In this the same key is used as a encryption key for all the blocks.



– Stream Cipher: In the stream cipher, it takes plain text in the form of characters or digits and combine them with a pseudo random key generator. The basic idea behind stream cipher is that it divides the text into small

blocks, typically of one bit or one byte long and encode each block depending on previous other blocks. In this the different key is used as a encryption key for each bit or byte, so the same bit or byte produces different cipher text. Some stream cipher use a random key generator which produce a random stream of bits. The cipher perform a exclusive OR operation between the bits in the key stream and the bits in the plain text to obtain cipher text.



III. DATA ENCRYPTION

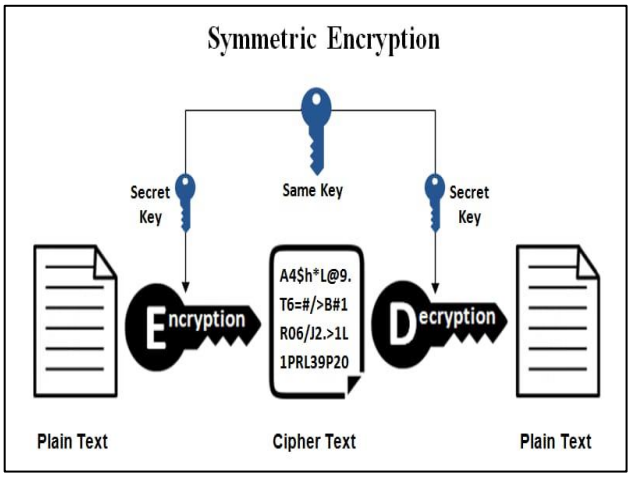
Data encryption is defined as the process of converting the plain text into cipher text by using an encrypted key, this process is called data encryption. Cryptography uses two types of keys one is symmetric and another is asymmetric. In symmetric, same type of key is used for both encryption and decryption process. Most cryptography processes uses the symmetric encryption for transmission, as it use only same type of key. Symmetric encryption is also known as private key encryption, uses the same private key for both encryption and decryption. The risk in this system is that if any of the party loses the private key then they didn't have the permission to access it and their system or message will be broken, hence the transmission is not possible.

IV. DATA DECRYPTION

As we know that the process encryption and decryption is used for system privacy or we can say, it is used for data privacy. As information travels over the world wide web, so sometimes it will create problems to the useful data. Decryption is the process of converting the cipher text or we can say encrypted data into plain text which can be easily understand by the system or the intended user.

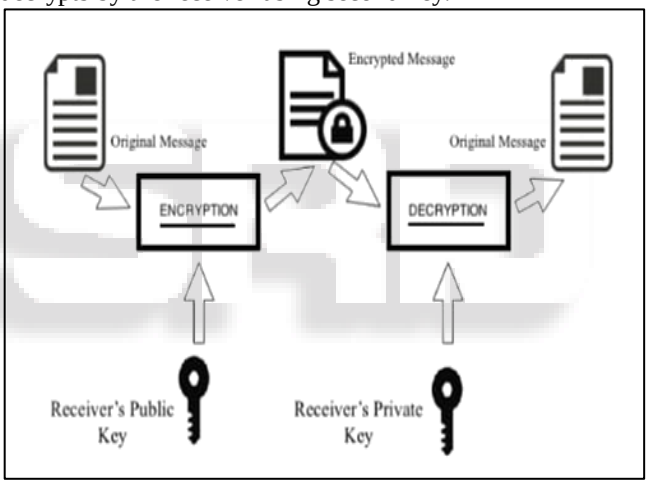
V. SYMMETRIC KEY CRYPTOGRAPHY

As we know that, symmetric key cryptography is also known as private key cryptography. In symmetric key cryptography same key is used for encrypting and decrypting the text. In this a secret key is shared between both the parties i.e. between both the sender and receiver. In this a sender have a secret key which is used for encrypting the text and the copy of same secret key is pass to the receiver for decrypting the text.



VI. ASYMMETRIC KEY CRYPTOGRAPHY

Asymmetric key cryptography is a two-key system which is also known as public key system. In this two keys are used one for encrypts the data and the another key decrypts the data. The computing sends the encrypt data uses a private key which is only known by sender and then that data is decrypts by the receiver using second key.



VII. CONCLUSION

The purpose of this section is to present that how cryptography is used to implement security in the web. From a technical point of view, cryptography is the solution to the many security challenges over the internet. As we towards a society where automated information are increased and the cryptography will continue to increase the security to the data. The information security can be achieved by using cryptography technique.

REFERENCES

[1] Mr.Vedprakash Sharma, Ms. Nabila Shaikh, Review paper on different cryptography algorithm for video.
[2] Neelima Saini, Sumita Mandal, Review paper on cryptography.
[3] Rajesh R Mane, Review paper on cryptography algorithm, attacks and encryption tools.
[4] Dr, Sandeep Tayal, Dr. Nipin Gupta, Dr. Pankaj Gupta, Deepak Goyal, Monika Goyal, A review paper on network security and cryptography.

[5] www.computerhope.com/cryptography
[6] www.techopedia.com/definition/25403/encryption-key
[7] www.tutorialspoint.com/cryptography/cryptography_tutorial.pdf

