ISSN No:-2456-2165

Research Paper on Cyber Security & Cryptography

Divya Chanana
Assistant Professor (SGTBIM&IT)
Department of Mathematics
GGSIPU

Abstract:- Cyber attacks are increasing day by day . So network security (to prevent the data from getting theft) is a must. There are various ways to prevent the data from getting stolen and Cryptography is one of them.Cryptography is a way of storing and transmitting the data in a particular form so that only those for whom it is intended can read it and process it.In this paper we will learn about Cryptography, its goals , how it helps in preventing cyber attacks .

I. INTRODUCTION

Cyber Security refers to the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation. Cryptography is about Mathematical functions and can be applied to technical solutions for increasing cyber security. Transforming the confidential data in a coding form and then transmitting it so that only authorized users can work on it is known as Cryptography. Cryptography is originated from Greek word "crypto" means hidden and "graphy" means writing, so cryptography means hidden or secret writing.

II. COMPONENTS OF CRYPTOGRAPHIC SYSTEM

Components of Cryptographic system are as follows:

A. Plain Text: The confidential data that should be secured while transmission is referred as plain text.
B. Cipher Text: The transformed plain texts that cannot be understand without applying encryption algorithm and encryption key over the plain text.
C. Encryption Algorithm: It is a mathematical process which is used to convert plain text into cipher text using some encryption key.
D. Decryption Algorithm: This is the reverse process of encryption algorithm. To produce the original text we use cipher text and encryption algorithm.
E. Encryption key: The value which is applied within encryption algorithm to get the cipher text from the plain text is called the encryption key. To make the cryptographic system successful safeguarding of encryption key is important. The value of encryption key is known to both sender and receiver or only to the sender
F. Decryption key: To get the plain text back from the ciphertext decryption key is applied within the decryption algorithm. The value of decryption key is known only to the receiver.

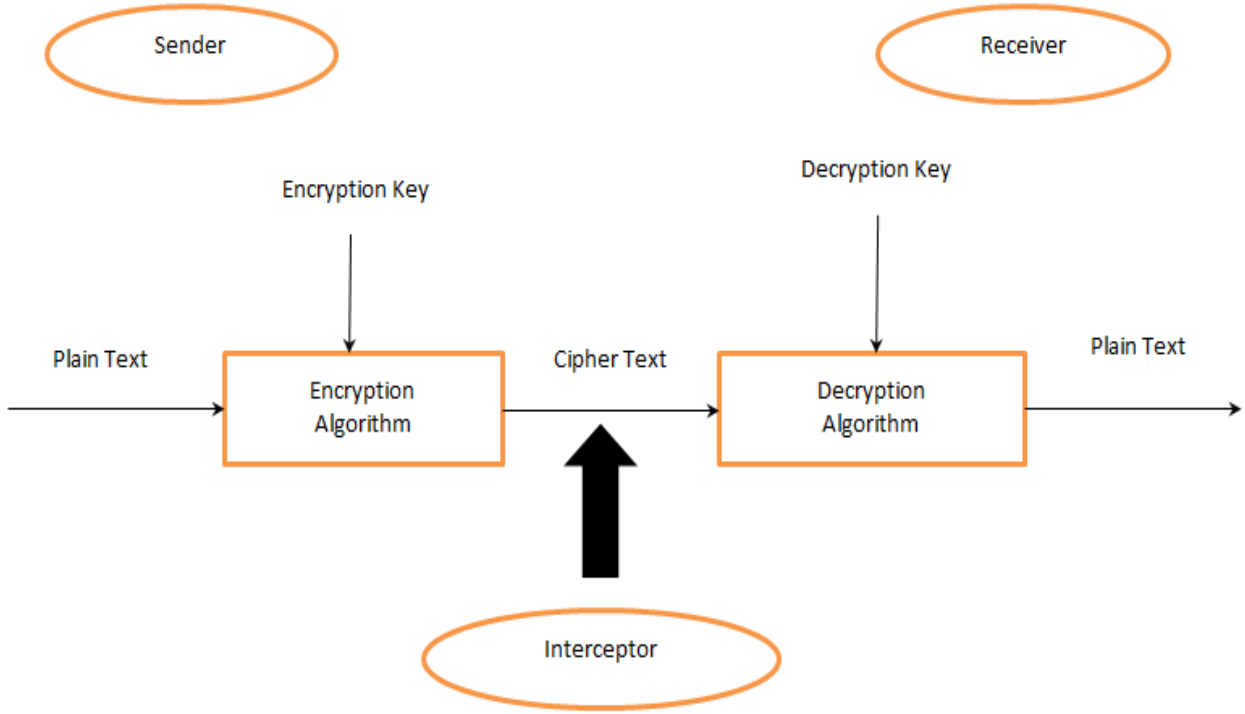

Fig 1: Cryptographic System

ISSN No:-2456-2165

III. HOW CRYPTOGRAPHY WORKS

Cryptography requires two steps: encryption and decryption. The encryption process uses a cipher in order to encrypt plain text and turn it into cipher text. On the other hand, Decryption uses the same cipher to convert the cipher text back into plain text.

Example, if you want to encrypt a simple message, "Hello".
So our plain text is "Hello".

We can now apply one of the simplest forms of encryption Known as shift cipher. With this cipher, we simply shift each letter with a shift of suppose three letters

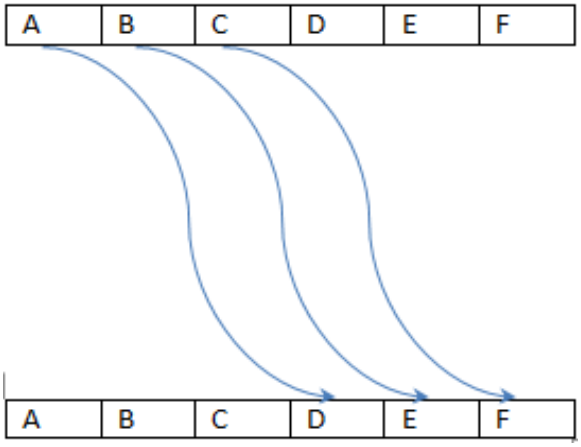

Fig 2

Meaning that:
A is shifted to D
B is shifted to E
C is shifted to F
D is shifted to G
E is shifted to H
F is shifted to I
G is shifted to J
H is shifted to K
And so on.

By applying this cipher, our plain text "Hello" gets converted into cipher text "Khoor"

Now, to the untrained eye "Khoor" means nothing like "hello". However one with the knowledge of Shift cipher could easily decrypt this message.

IV. GOALS OF CRYPTOGRAPHIC SYSTEM

Many attacks are possible over any ongoing communication within a network like Security threats, Unauthorized access, Data capturing, Virus infection etc. To prevent attacks(Security threats , unauthorized access,Virus infection)every encryption system must have some features that helps in secure transmission of any data. The main such goals are listed as follows:

A. Confidentiality: Cryptography ensures confidentiality through hiding a message and protects confidential data from unauthorized access.
B. Access control: Only authorized users can access to protect confidential data etc. Access would be possible for those individual that had access to the correct cryptographic keys.
C. Authentication: Before the interaction with the cryptographic system the process of verifying the sender and the receiver is termed as authentication.
D. Data Integrity: It ensures that the received message has not been changed from its original form in any way. The data may get modified by an unauthorized user intentionally or accidentally. Integrity makes sure that the data is intact or not since it was last created, transmitted or stored by an authorized user.
E. Non-Repudiation: It is a mechanism used to prove that sender really sent this message and the message was received by that specific party, so that the recipient cannot claim of not receiving the message.

V. TECHNIQUES OF CYBER SECURITY

The following technologies can be used to reduce network attacks:
A. Authentication: All the received data must be authenticated if it is sent by the trusted sender or not
B. Antivirus: On a regular period of time we should install and update antivirus software in our system.
C. Firewalls: The inward and outward traffic of any system can be tracked using this software. This software also helps in informing the user about any unpermitted access and usage.
D. Access Controls: Each user must have their particular username and password to avoid unauthorized access.
E. Cryptography: The technique of encoding the plain text into cipher text to avoid the confidential data from getting stolen before transmitting it over channel is cryptography.

VI. CONCLUSION

In this paper we have seen how cryptography make sure that the original data is not manipulated during any transmission. We also discussed about its goals. Network security can be prevented using various techniques like Cryptography, Firewalls, access controls and steganography etc. So to safeguard our confidential information we can say Cryptography is a must.

REFERENCES

[1]. Anu and Divya Shree, " A Review on Cryptography, Attacks and Cyber Security" , International Journal of Advanced Research in Computer Science.
[2]. Sarita Kumari, "A Research Paper on Cryptography Encryption and Compression Techniques, International Journal of Engineering and Computer Science.
[3]. https://thebestvpn.com