Cryptography in Network Security

Narendra Jangid [1], Anil Dhankar[2], Saroj Hiranwal[3],Harshita Kaushik[4]
[1]Dept of MCA
[2] Professor, Dept of MCA
[3] Assoc. Professor, Dept of MCA
[4]Asstt. Professor, Dept of MCA
[1, 2, 3, 4] RIET Jaipur

Abstract- *the main aim of this paper to provide the information of cryptography and we all so describe uses of cryptography and define the major point of network security basically cryptography use for protecting over network and data connection and we also describe about unauthorised and illegal access. In present over data and security is more sensible just because of highly uses of computer and data network. Network security and cryptography is the subject which provide basic and advance information and solution to protect over data in digital from and also we learn about that which type of security attack and office security services we have to avoid. We see that cryptography and network security is use in many application like banking, government agencies, military and secret services huge level organization. in cryptography we use various types of technique and algorithm to protect over network and data.in this paper we disuse about various types of encryption and decryption technique in cryptography and also talk about cryptography model, algorithm and crypto system types*

Keywords- cryptography encryption, decryption, network security and network attacks.

I. INTRODUCTION

The present over whole world is depending on web and its application for there all work of life. Network security insure as to over data and system resources are safe it is responsible for all the security of our information which is passed through the internet from one compute to other system the term of cryptology is taken from freak word "KRYPTOSLOGOS" which mins "HIDDEN WORD " cryptography is the method of securing information and protective data in cryptography we use combination of algorithm and mathematics to encrypt and decrypt data cryptography is one of the rising innovation for securing securing information. In network security we setup some specific thing using date, the authorised person can access the data. There are for types of security issues that is anon-repudiation, mystery, classification and validation cryptography use to store sensitive information or covert it to unreadable from.

Security Attack

Passive Attack

In passive attack the attacker obtain the information that is passed on network.

Top four more passive attack

1. SPOOFING
2. UNAUTHORIZED ACCESS
3. UNAUTHENTICATED ACCESS
4. MALICIOUS SHOFTWARE

Active attack.

In active attack the attacker get the information which is passed on network and modified date information.

Top three more Active attack

1. Modification
2. Repudiation
3. Sniffing

Cryptography process

In cryptography we have four stage after completing each step we finished the cryptography.

The stages are

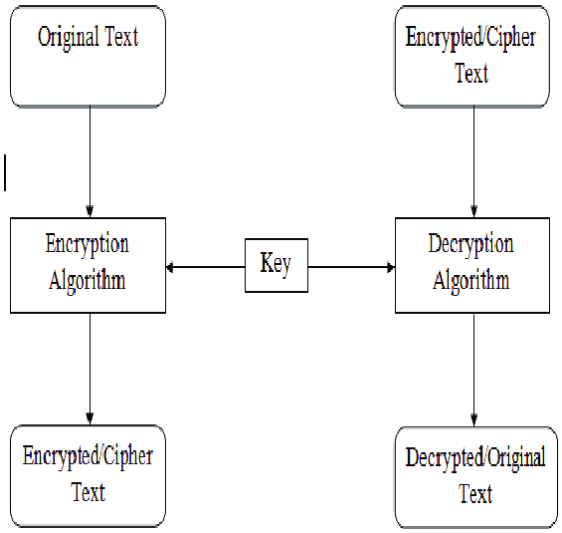
1. Plan text
The original massage which is encoded in none as plan text.

2. Encryption
The process of converting plan text to cipher text is known as encryption.

3. Cipher text
The unreadable from of plan text is known as cipher text.

4. Decryption

The procedure of reconverting the cipher text to plan text is none as decryption.



Block diagram of Cryptography process

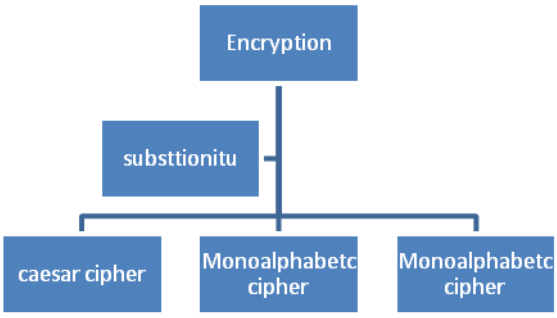
Encryption techniques

In cryptography the main classification of encryption types are:

- **SUBSTITUTION TECHNIQUES**
- **TRANSPOSITION TECHNIQUES**

SUBSTITUTION TECHNIQUES

In substitution techniques we replace the plan text letter to other letters or number.



The substitution techniques are

1. Caesar cipher
2. Monoalphabetc cipher
3. Play fair cipher
4. hill cipher

Caesar cipher

In Caesar cipher techniques we replace the latter of plan text to that alphabet which is standing on the third place of the latter.

Monoalphabetc cipher

In this cipher techniques we replace the plan text latter to any alphabet latter.

Play fair cipher

This cipher technique is work on matrix based latter constructed using a key word.

Hill cipher

In this cipher technique the encryption algorithm takes m successive plaintext letters and substituted for them m cipher text letters. The substitution is determined by m linear equations in which each character is assigned a numerical value (a=0, b=1….z=25).

Transposition techniques

In this technique a very different kind of mapping is achieved by performing sum short of permutation on the plan text latter.

Types of cryptography

Secret key cryptography

In secret key cryptography we use only a single key for both encryption and decryption process the key is known as secret or shared key .It is also known as symmetric cryptography.

Types of secret key algorithm

1. Aes Managed
2. DES Crypto service provide
3. HMACSHAL
4. RC2 Crypto service provider
5. Rijndael Managed
6. Triple DES Crypto service provider

Public key

In public key cryptography we use two unique key for encryption and decryption. This cryptography also known as asymmetric cryptography

Type of public key algorithm

1. DSA cryptography service provider
2. RSA crypto service provider
3. EC Diffie hell man
4. EC Diffie hell man cng public key
5. EC diffie hell man key derivation function
6. EC dsa cng

Hash Cryptography

Hash cryptography are one way transformation in this technique we convert the plan text into a fixed length number it is also used to enhance the public key process. A hash is design to act as a one-way function – you can put data into a hashing algorithm and get a unique string, but if you come upon a new hash, you cannot decipher the Input data it represents.

Type of hash cryptography key algorithm

1. HMACSHAL
2. MAC Triple DES
3. MD 5 crypto service provider
4. RIPEMD 160
5. SHAL Managed
6. SHA 256 Managed
7. SHA 384 Managed
8. SHA 512 Managed

II. CONCLUSION

At the end of this paper we see that the basic and useful information about cryptography in network security that how much cryptography is important for our data and network connection. Basically in future we have h huge scope in cryptography. As per our current growth in computer sci. we have to developnew algorithm and techniques for cryptography. The old method of cryptography Has low security level in present time so most of people are still researching for new techniques and algorithm for new type of data and most important high amount of data.

REFERENCES

[1] Zhijie Liu Xiaoyao Xie, Member , IEEE ,School of Mathematics and Computer Science and Zhen Wang, Key Laboratory of Information Computing Science of Guizhou Province , Guizhou Normal University Guiyang , China, The Research of Network Security Technologies

[2] Shyam Nandan Kumar, "Technique for Security of Multimedia using Neural Network," Paper id-IJRETM-2014-02-05-020, IJRETM, Vol: 02, Issue: 05, pp.1-7. Sep-2014

[3] N.Lalitha,P. Manimegalai, V.P.Muthu kumar, M. Santha,"Efficient data hiding by using AES and advance Hill cipher algorithm ", International journal of research in computer applications and Robotics, volume 2, issue 1 ,January 2014.

[4] Tayal, S., Gupta, N., Gupta, P., Goyal, D., & Goyal, M. (2017). A Review paper on Network Security and Cryptography. Advances in Computational Sciences and Technology, 10(5), 763-770.

[5] Kaur, S., Kaur, R., & Raina, C. K. (2017). Review on Network Security and Cryptography