EasyChair Preprint

№ 7952

A Review- Paper on Cryptography and Network Security

Esha Rawat, Anuska Singh, Alap Mahar and Amit Agarwal

May 15, 2022

A Review Paper on Cryptography and Network security

Esha Rawat[1], Anuska Singh[2], Alap Mahar[3], Prof. Amit Agarwal[4]

[1]esharawat935@gmail.com, [2]singhanuska906@gmail.com, [3]alapmahar@gmail.com, [4]director.ittanakpur@gmail.com

(Department of Computer Science and Engineering, Dr. APJ Kalam Institute of Technology, Tanakpur DISTRICT- Champawat, Uttarakhand)

ABSTRACT:

With the emergence of new media age and growing needs of people to shift their offline schedule online, there has been a drastic growth in the exchange of information worldwide. Now a days sharing data and information through internet leads to the occurrence of e-crime or cyberterrorism. Hence, it becomes necessary to secure our information from the cyberattacks. In this paper we provide an overview of cryptography and network security. Cryptography is a technique that encrypts our information into unreadable codes so that the cryptanalysts does not get access to our information.

KEYWORDS:

Cyber-attacks, Cryptography, Network security, Crypt analyst, Encrypt

INTRODUCTION:

We are living in the new media age, here information has become most necessary aspect of our life. And as we know necessary things needs to be preserved and so is with information, we do need to secure information from unauthorized access. With an expansion of cyberspace and information technology many illicit users strike and demolish the network by using fraudulent means (i.e., mails, websites, etc.)

With this we felt the need to secure our information/ data which is promoted by cryptography and network security. Hence, Cryptography was initiated by Claude E. Shannon.

Cryptography was originated from Greek word “Krypto’s” which implies “hidden” or “secret” and “Graphikos” which means “to study or to write”. So basically, it is the study or writing of secret codes.

In the review of “Network Security and Cryptography”, Dr. Sandeep Tayal et al. [1] mentioned that cryptography is the science of writing codes. Establishment of social network community and e-commerce applications has led to daily production of huge amounts of data by various clients all over the network. It has enhanced infosec for data transfer with guarantee. As lots of people are accessing internet, this issue further views the importance of cryptography techniques.

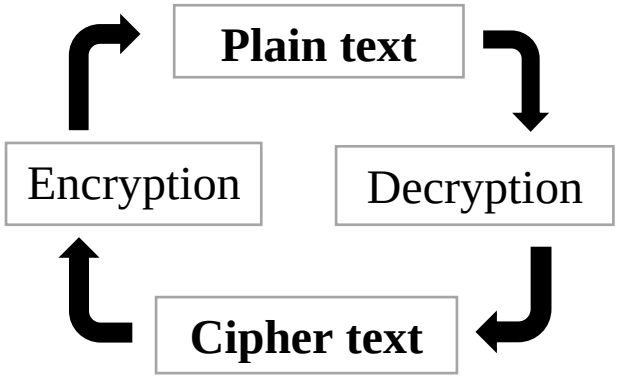

***Fig. 1** Procedure of cryptography*

LITERATURE SURVEY

TERMINOLOGY:

Cryptography

Cryptography is a technique of guarding our communication which involves usage of codes, so that concern person can read and process it.

It is that kind of transformation which is associated with conversion of unencrypted text into decrypted text and vice versa.

Plain text

The first disguised information or message that an entity would wish to convey to any other entity, is depicted as plain text. It is readable information or message that is sent by sender's end to receiver. Information under plain text can be of any form i.e., a message, documents, files etc. Plain text is safeguarded from any sort of formatting.

Key

A key in cryptography is a string of numbers or characters that are stored in a file. With cryptographic algorithm it can convert ASCII text into coded message.

Cipher text

Cipher (code) is an algorithm which is put into plain text to get cipher text. [2] Basically, the text which cannot be understand by anyone or gibberish text, example "A@$&J9". It is the unreadable or encoded information of the message that was conveyed by the sender. It is upshot of encryption performed on plain text using an algorithm.

Encryption

The procedure of transforming unencrypted text (plain text) into encrypted text (cipher text) mainly to prevent unauthorized access or to secure digital data using one or more mathematical techniques. With an encrypted message an authorized user can access the original information.

[3] A data encryption is a random string of bits created explicitly for scrambling data. Data encryption is designed with algorithms intended to ensure that every key is unpredictable and unique.

Decryption

It is the process of converting encoded text into decoded text. It is accessible to authorized users only because decryption requires a secret key or passwords. It basically converts cipher text to plain text.

Crypt analyst (hackers)

Crypt analyst are generally code breakers. Those individuals who associates with the study of secret code system in order to obtain secret information are identified as crypt analyst. Hackers can access the secret messages or information by their coding system and their technical knowledge in the field of cryptographic techniques.

Cryptographer

A cryptographer is a person who encrypts(code) the messages to ensure cyber aegis and network security. Basically, cryptographers are the code maker and considered as a cyber security professional with an expertise in cryptography.

Block cipher

It is the technique of encoding data into blocks to achieve coded text via cryptographic key and algorithm.[4] Block ciphers have been widely used since 1976 in many encryption standards. Block ciphers provide the backbone to encryption technique behind the most modern era ciphers.

Non – Repudiation

[5] Non repudiation ensures that no party can deny that it sent or receive the message via encryption, digital signatures or approved some information. It also cannot deny the authenticity of its signature on a document. It is also widely used in computing, information security and communications.

HISTORICAL SIGNIFICANCE

The technique of cryptography is recognized to be inherited with the technique of writing. It is a science that gives us the knowledge of writing codes and ciphers. It allows us to transmit all the information securely via internet.

The origin of cryptography is found in Roman and Egyptian civilization. One of the basic forms of cryptography is symbol replacement, it uses Egyptian (1900 BCE) and Mesopotamia symbols (1500 BCE) to replace message.

In Sparta, spartan scytale was used. In this technique message was written on a banner and then was wrapped on cylinder of similar size.

Hieroglyph is one of the oldest cryptographic techniques used some 4000 years ago by the Egyptians to communicate.

Most advanced method was invented by roman empire which was Caesar cipher. In this technique letters of a message are shifted by certain places.

Thomas Jefferson brought a major break in history of cryptography (1795). Jefferson invented cipher wheel (also called Jefferson disk). This wheel consists of certain disk or wheel each containing 26 alphabets arranged around edge. The order of disk act as cipher keys and the receiver needs to decode the message.

A machine known as enigma cipher was used during World War II for encoding a message using rotating disk and it was virtually impossible to decode the message without another enigma machine.

Also, with the application of cryptography it was made possible to introduce cryptocurrency.

The Enigma Machine

[6] It is the machine where we can encode and decode the words and messages. This machine come into effect in the early to mid-20^{th} century to protect commercial, diplomatic, and military communication. It was employed extensively by Nazi Germany during second world war, in every branch of the German military. The Enigma machine was considered so secure that it was used to encipher the most top-secret messages.

The Enigma machine works on the mechanism of electromechanical rotor that consists 26 letters of alphabet.

Types of Encryptions

1. **Symmetric encryption**
   Besides symmetric encryption, it is well known as secret key cryptography. In this encryption same key is used at both sender as well as receiver's end which is identified as secret key. Therefore, it is also designated as symmetric key algorithm.

   PROS: It is fast and efficient for large amount of data.

   CONS: In this, data can be managed by crypt analyst or hacker. These are two following ways:

   1.1 Passive Attacks

   [7] Within passive attacks, hacker observes the system for exposure that permits them to interrupt information without altering it.

There are two common types of passive attacks:

a.) Traffic analysis
In traffic analysis, attackers monitor communication medium to collect at range of information including human and machines recognition, location etc.

b.) Footprinting

It is the technique in which the hacker collects the data about a specific targeted computer system. It gathers all information which includes network details, open ports, IP ranges etc.

1.2 Active attacks

It is the attack in which the crypt analyst (hackers) attempts to alter the data according to his/her convenience. It may control, change, or insert data into the already existing system. It includes following:

a.) Masquerade

b.) Modification of message

c.) Repudiation

d.) Deniel of service

Some examples of symmetric encryption

AES
It represents Advanced Encryption Standard. It originates from Rijndael algorithm. It was introduced in 2001 by US NSIT. It is the strongest algorithm among worldwide. It uses 128-bit block size in which data is split into 4 by 4 array comprising 16 bytes.

DES
It represents Data encryption standard. DES is a block cipher (symmetric key) which is inaugurated by an IBM in 1970 and endorsed by NIST (National institute of standard and technology). It encodes each data in block size of 64-bits(8-byte). The algorithm of DES is as follows:

- 8- byte of plain text enlists DES as an input.
- Then through DES algorithm it produces 8-byte of cipher text.

It is a symmetric key algorithm which indicates that the same key is used for encrypting or decrypting the data and information.

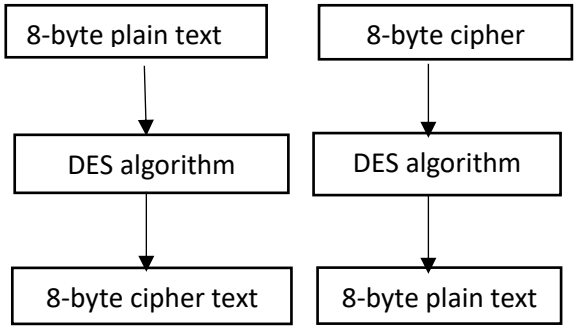

Fig. 2 *Encryption and Decryption using DES algorithm*

IDEA
[8] It implies international data encryption algorithm. It was enhanced by James L. Massey Xuejia Lai in 1990. IDEA uses 64-bit clear text with 8 rounds and a key length of 128-bit altered into 52 sub keys each of 128 -bits.

1. Asymmetric encryption
In this algorithm, a secret key is divided into two keys. These are public key and a private key. As the denotation imply the public secret key is given to anyone authorized or not and private key must be secret. Public key encryption is the practice in which an entity can send an encrypted message using public secret key of the receiver, which

allows only receiver to decode the message using her/his own private secret key. In this only receiver can decode the message. This makes public key encryption a flawless method for conserving message. It covers identity assurance and non-repudiation. Some examples of it are Diffie-Hellman, ECC, DSA etc.

Two main types of asymmetric algorithm:

a.) RSA

It stands for Rivest, Shamir and Andelman. They are the inventors of this technique. It was first published in 1977. RSA is an algorithm in which the plain text and cipher text are the integers which lies between 0 and n-1 where n is the product of p and q (here p and q are two distinct prime numbers). In this algorithm public secret key is accompanies encoding and private secret key utilized for decoding of the information.

b.) ECC

It symbolizes elliptical curve cryptography which was came into force in 2004. ECC algorithm uses shorter keys which implies faster and secure. A 15360-bit RSA key is identical to 512-bit ECC key, which means denotes ECC can withstand more security than RSA.

c.) DSA

It stands for Digital Signature Algorithm. It is the scientific technology used to certify verity and legitimacy of message. It is the digital signature of original signature or stamped seal. This algorithm provides augmented inherent surveillance and aegis of the messages. Digital signatures are authenticated only when the owner signs a document electronically, the signature of the owner is composed by using signer's private security key which is incessantly kept unharmed by the signers/owner. It provides message authentication, integrity verification, non-repudiation.

d.) Hash function

[9] The term hash function has been used in computer science from quite some time. It specifies a mathematical function that constrict a string of arbitrary input to a string of fixed size.

Cryptographic hash functions have become one of the most crucial tools in the profession of cryptography and it is also used to accomplish a number of security goals like authenticity, digital steganography, digital time stamping etc.

Goals of network security

Network security is not only meant for surveillance of the computer at the time of conveying and receiving message, rather it aims to assure that the system is safe and secure. It guards the functionality, safety and security of the system. its primary goal is privacy, integrity and accessibility. The three columns of network security are represented as CIA triangle. "CIA triad" stands for confidentiality, integrity, and availability. It is sometimes referred as "AIC triad". Basically, this model is designed to counsel the management and guidelines for infosec and IT security within an organization.

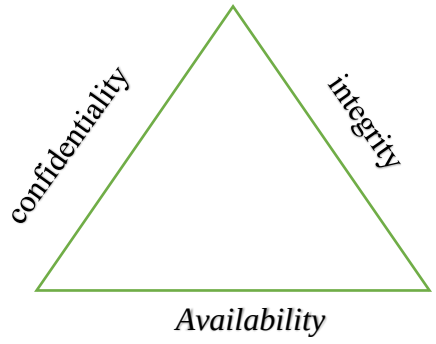

Fig. 3 *CIA Triads*

CONCLUSION:

Cryptography is a vital element for providing security for network-to-network data transmission. It plays a critical role in attaining the aim of security purpose such as authentication, non repudiation, etc. The main motive of cryptography is to provide reliable, well-built network and cybersecurity. In this review paper, we validated some of the researches that was formerly organized in the field of cryptography, network security and the purpose of various algorithms.

REFERENCES

[1] Sandeep Tayal N. Gupta, D Goyal and M Goyal *A review paper on "Network security and cryptography*" *Advances in computational science and technology, vol. 10, no. 5, pp.763-770, 2017.*

[2] Yahia Alemami, Mohommad A fendee Mohamed, Saleh Atiewi

[3] Sarita Kumari *Research scholar*

[4] Scott R. Ellis, *in computer and information security handbook (third edition), 2013*

[5] Rahul Awati *20 august 2021*

[6] Wikipedia.in

[7] Miller, A. R. *the cryptographic mathematics of enigma. Cryptologia, 19,1 (1995), 65 to 80*

[8] Sanjeev Kumar Mandal, A R Deepti

Research scholar, Department of master of computer application VTU, India

[9] Rajeev Sobti, G. Geetha *cryptography hash function: a review march 2012*

[10] Ch. Sandeep, V. Thirupathi, P. Pramod Kumar, S. Naresh Kumar *dept. of CSE, S R Engineering college, India*