A research Paper for Symmetric and Asymmetric Cryptography

Akshay Kekunnaya[1], Rajeshwari Gundla[2], Siddharth Nanda[3]
[1]U.G. Student, SOE, ADYPU, Lohegaon, Pune, Maharashtra, India
[2]Senior Faculty-IT, iNurture, Bangalore, India
[3]Faculty-IT, iNurture, Bangalore, India

Abstract- The word data is very crucial in today's world related to personal and business term as it contains the personal or business information of a personal or group. Also, this data maybe theft by third party members if it is not secured by using the term cryptography. Cryptography helps us to maintain the encryption of data and also helps us to authenticate the user. When cryptography word comes then confidentiality, integrity,and availability are very crucial. This paper gives us that what is symmetric and asymmetric cryptography and what are the benefits of using that and how can we safeguard he data by the third party/Hacker.

Keywords- Data/Information's, Cryptography, Confidentiality, Integrity, and Availability

I. INTRODUCTION

Today's generation we all know that data is very crucial in one's personal or business life as this data can change there future and this data cannot be stored in any open way in file or computer. So, this data can be converted using the means of cryptographic algorithm using many types of keys which will help to hide the data or information. By chance if any other third party comes in line to steel the data or information, he needs to first decrypt the data which will be difficult as he needs to use different keys which is very tough foran individual. The difficulty is not based on how we encrypt the data, but it is based on the secret key used to encrypt the data or information. As and when the term cryptography strikes the CIA is very crucial in all the terms. CIA stands for Confidentiality, Integrity, and Availability

II. CRYPTOGRAPHY

Cryptography is basically an art of writing. This art was introduced in the era of 19th century in "The Gold-Bug" a novel by Edgar Allan Poe. Before, cryptography was used in war to communicate between the base and battle field. This text is first converted to cipher text using the means of encryption and for reading that cipher text first we needed to covert back to plain text by using the means of decryption. To hide any data two techniques are mainly used one is Cryptography other is Steganography.

Also, there are some laws of cryptography which was stated in 1980's, but many countries follow different type of laws. Some countries do not allow to use software's of cryptography and some does not allow the free version of cryptography software's and there are various laws in different part of the world.

III. CRYPTOGRAPHY GOALS

Confidentiality: - Confidentiality in basic term states that, the data or information should be only available for the authorized people and no data is leaked or accessed by unauthorized people or hackers. This confidentiality is obtained by encrypting the data by using the means of cryptographic algorithms.

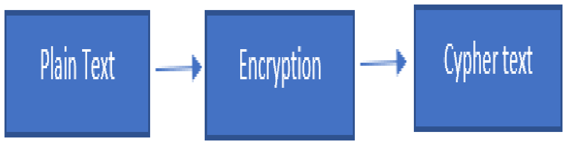
Integrity: -Integrity is the term where it ensures that no data or information is modified or changed by any of the third-party members. Also, we know that the data is accurate only if it is correctly stored in database.For example, if you were sending an online money transfer for 1000Rs, but the information was tampered in such a way that you actually sent 10,000Rs, it could prove to be very costly for you.

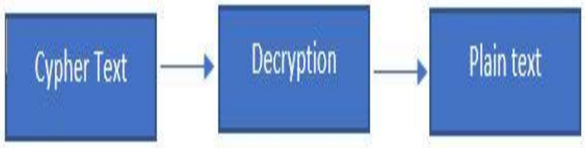
Availability: - Availability, simply defines that the available of data of information for the authorized people 24/7. Information only has value if the right people can access it at the correct time when needed.

Also, there are few terms which can be related to cryptography. They are: -

- **Authentication: -** In this, the term Authentication refers to proving's one's identity so that the person can access the information properly and securely.
- **Non-repudiation: -** Non-repudiationmeans to verify that the data in received by the receiver or not.

Data Encryption and Data Decryption



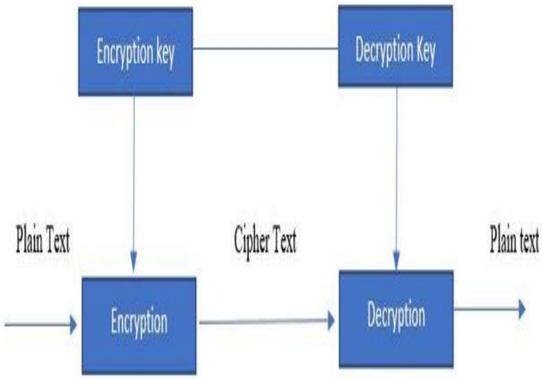


Data encryption is the process of converting the plain text into a text which is not read by humanswithout using a key called cipherkey. This key can be of any type depending on the way of doing encryption. This key can contain any character (foreign or non-foreign) according to the way of encryption Let's take an example, one person has to send a message “Hello” to the person, when he sends the message, the message “Hello” will be encrypted using a key called cipher and this message will be send to that person .After transmitting, the cipher text should be converted back to plain text , this is done by method of decryption using the same key or different key and then the message “Hello” will be read by the person.

IV. SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY

As mentioned, all the above cryptographic term is most important for understanding symmetric and asymmetric cryptography. Now let us study in detail about this topic.

Symmetric Cryptography: -



According to Sarita Kumari[3]and also Sarita Kumari[4]Research PaperSymmetric Cryptography is a way of encrypting a data using akey called cipher. In this, both the people will have the same key to encrypt or decrypt the data. In this if one of the users misplaces the key, that user won't be able to encrypt or decrypt the data. There are two types of symmetric key cryptography, they are: -

- Stream ciphers
- Block ciphers.

Stream Cipher: - In this, stream cipher encrypts a single digit or a letter of the message send by the sender to the receiver.

So, let's take an example of Vigenere Cipher.

Let's take a plaintext “ATTACKATNINESHARP”

The person who is sending the message takes a key and repeats it till it matches the length of plaintext. So, let's take a key
“SPEED”
then,
“SPEEDSPEEDSPEEDSP”
will be the key of the same size, now we will write the plain text and the key one below the other for making a cipher text

ATTACKATNINESHARP

SPEEDSPEEDSPEEDSP

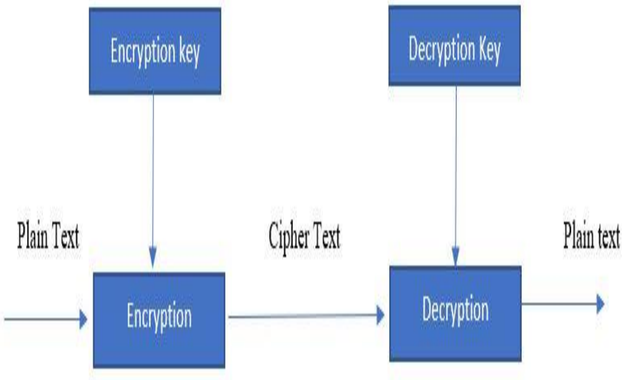
After this we get a cipher text called “SIXEFCPXRLFTWLDJE”

This cipher text should be converted to plain text by the receiver to know the plaintextwhich is done the same way the sender did by using the key and the logic, if the receiver dose not decrypt the message properly, the message won't be clear and can lead to n number of misunderstandings. Also, if the third party looks into this cipher text, he also needs the same key to decrypt and for finding the key it will be difficult for third party because the key will be only with sender and receiver (in certain cases).

Basically, in today's world, all modern cryptographic systems still use symmetric-key algorithms to encrypt and decrypt the data.Encrypting the data doesn't guarantee that the message is completely changed or not. For this reason, an authentication code is attached to a cipher text ensuring that changes in this cipher text is noted by thereceiver. As of the term and research we cannot use non-repudiation in symmetric cipher.

Block ciphers: - This type of cipher works on a fixed-length of groups of bits called blocks. This block encrypts in 128-bit with a key with a predetermined length. Basically, this technique is used to remove the chance of encrypting identical blocks of text. In block cipher the size is not a multiple of block size, for example let's take a 140-bit plaintext. So, this plaintext will be blocked by 64-bits of two and 12 of the third block. Now this additional 12 bits need to have extra 52 redundant bits to complete its 64 bit and is equal to the rest two block divided.

Asymmetric Cryptography: -



The image represents that for this type of cryptography the key used by the people are different.

According to Harpreet Kaur[5] paperAsymmetric cryptography also known as public-key cryptography is a method, of using two key one is private key and another public key to encrypt and decrypt the data which is sent by sender and received by the receiver.Asymmetric cryptography is very different from symmetric cryptography.A public key is available to everyone for them who are sending the message but a private key is a secret key which is known by a single person who is sending the message. Any message which is encrypted using public key should/can be only decrypted using the same type of key.

Table of Compression: -

Sl No	**Types**	**Difference**
1	Symmetric Cryptography	• Symmetric uses a single key for encryption and decryption of the message. • Symmetric encryption is a very old type of practice. • Symmetric is timing saving
2	Asymmetric Cryptograph	• asymmetric uses two keys for encryption and decryption. • Asymmetric cryptography is a modern way to encrypt and decrypt the data. • Asymmetric is time consuming

V. CONCLUSION

In this, we have seen what is the use of cryptography and where and when to use cryptography. We have learned the type of cryptography that is symmetric and asymmetric cryptography. Cryptography is used to ensure that the message sent by the people is secured or not.

VI. REFERENCES

[1]. Harshala B. Pethe, Dr. Subhash. R. Pande, "Implementation Of Data Encryption Standard Algorithm" International Journal Of Computer & Mathematical Sciences Ijcms Volume 4, Issue 9 September 2015.

[3]. https://en.wikipedia.org/wiki/Cryptography#Symmetric-key_cryptography accessed on 8th April 2019

[4]. Sarita Kumari a Research Scholar: A research Paper on Cryptography Encryption and Compression Techniques

[5]. Sonia Rani: Technical Review on Symmetric and Asymmetric Cryptography Algorithms

[6]. Harpreet Kaur: Technical Review on Symmetric and Asymmetric Cryptography Algorithms