A REVIEW ON CRYPTOGRAPHY, ATTACKS AND CYBER SECURITY

Nidhi Mathur[1], Gaurav Mitawa[2], Prashant Mathur[3]

[1] *PG Scholar, Computer Science & Engineering, Sobhasaria Group of Institutions,* Sikar**,** *Raj., India*
[2] *Asst. Professor, Computer Science & Engineering, Sobhasaria Group of Institutions,* Sikar**,** *Raj., India*
[3] *UG Scholar, Computer Science, Arya College of Engineering and IT, Jaipur, Raj., India*

ABSTRACT

A big part of the population of the world relies on the internet to communication in their social, marketing and commercial purposes. Actually on serious note internet is the powerful tool for the communication technology. On the internet communication happen in the form of data (text message, files or any kind of electronic mail). Data confidentiality becomes very challenging as the communication technology is expanded day by day. The risk of the data loose or stolen simultaneously increases by the cyber criminals (hacker or attacker). Hackers attack on the communication systems, become the communication medium insecure and after that stolen the confidential information for their financial purposes and misuse data in the illegal activity. Attacks are typically classified based on the action performed by the attacker; an attack thus can be the active or passive. In active attack the information is modified in an unauthorized manner where as the main target of the passive attack is that to obtain unauthorized access to the information. Encrypt data is the best way to secure the data from unauthorized users or aggressor. Cryptography is the technique to encrypt the confidential data using the various mathematical operations and algorithms. Cryptography is one such way to make sure that confidentiality, authentication, integrity, availability and identification of user data can be maintained as well as security and privacy of data can be provided to the user.

Keyword: *Cryptography, Cryptanalysis, Cryptology, Active Attack, Passive Attack, Cyber Security,*

1. INTRODUCTION

The combined study of the cryptography as well as the cryptanalysis is known as the cryptology. Two branches of the cryptology are

- Cryptography
- Cryptanalysis

Cryptography is consists of Greek Word Kryptos and Gráphein, literally meaning is “hidden/secret writing”. It is the exercise of art and science of secret writing used to share secret information or data over public networks, where contents of the novel message are mutated into unreadable or unidentified form, to be retrieved only by the deliberate person. It is the technique to provide secure communication in the presence of adversaries to maintain information security such as CIA (Confidentiality, Integrity and Availability) Triads and non-repudiation.

Cryptanalysis associates with the study and analysis of cryptographic algorithms in a practical way to understand their encrypted information and find out the vulnerabilities to crack them. It is also known as code-breaking as well as cracking the code.

Aim of this paper is to review about basis and overview of cryptography and the types of attacks act on the crypto system.

1.1 Basis Model of the Cryptography

Figure 1 shows the basis model of cryptography. The aim of this model is that whenever the confidential information is shared between the sender and receiver through a communication medium. Confidential information is in the form of plain text sender encrypted the plain text using an encryption algorithm and convert in the cipher text (meaning less form) and lock that with the help of encryption key. The lock of cipher text is opened by the intended receiver only when have the decryption key. After open the lock receiver access the original confidential message. There is always an uncertainty that attacker breach the system, if he success in it there is chance to read the message but in this case message is now cipher text without decryption key cant able to understand that. So confidentiality and integrity of the message is maintained.

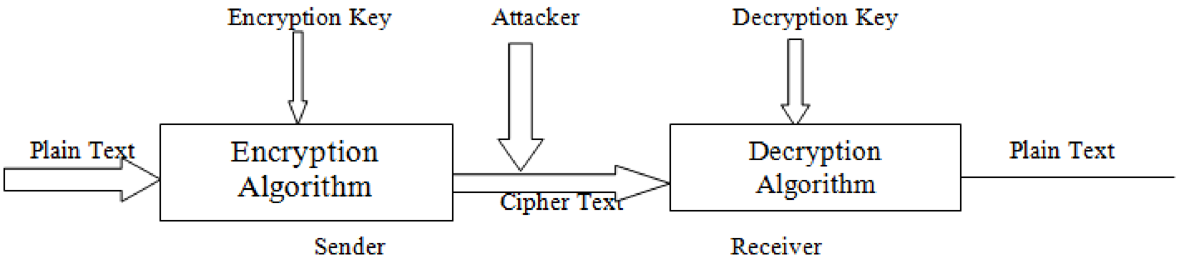

Figure 1: Basis Model of Cryptography

1.2 Different Elements of the Cryptography

- **Plain text**
  It is confidential information that we need to hide that is encrypted and sent over the network. Generally speaking, it's the first content; it could be in a type of characters, number-crunching information, executable projects, pictures, or some other sort of data.
- **Cipher text**
  It is the sort of calculation that is utilized to move meaningful or plain content into unintelligible content or encoded structure known as cipher text. It is the good for nothing information or misty content that no one must comprehend, aside from the beneficiaries. The information will be transmitted precisely through the system; numerous calculations are utilized to change plaintext into cipher text.
- **Encryption Algorithm**
  It is a mix of complex scientific capacities that are utilized to encode private data.
- **Decryption Algorithm**
  It is additionally an amalgamation of composite scientific capacities that are utilized to decode the mystery data. More often than not, an unscrambling calculation is an in spite of the encryption calculation
- **Encryption Key**
  It is a secret values that the sender utilizes as one of the inputs to the encryption algorithm in union with plain text or understandable format to generate a cipher text or non understandable.
- **Decryption Key**
  It is a secret value that the receiver employs as one of the inputs to the decryption algorithm in synchronicity with cipher text to get plain text.
- **An Attacker**
  It is an entity who always tries to listen to the communication channel to interrupts the cipher text and further tries to convert the cipher text to plain text.

2. Types of Attacks the Cryptosystem

The techniques utilizes by an adversary for the reason of breaching secured systems and make system insecure are known as cryptographic attacks. These attacks can be classified in two major categories.

- Passive attacks
- Active attacks

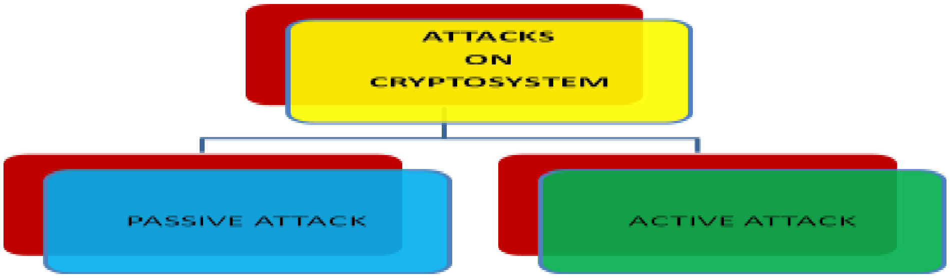

Figure-2 Types of Attacks on Cryptosystem

2.1 Passive Attack

In Passive attacks, intruder or hackers tries to eavesdrop to the network connection to gain some information or data and attempts to break the system which is based upon the data packets transfers between sender and receiver. Determining known plain texts is one of the illustrations of passive attack where an adversary is analyze the unencrypted traffic and looks for sensitive piece of information like usernames or passwords that have been pooled between communicating parties. Snooping and Traffic Analysis are two types of the passive attack.

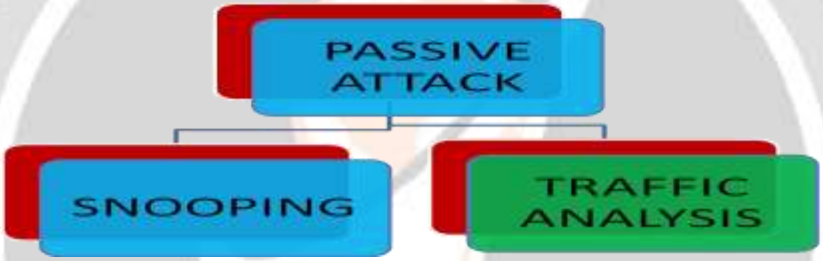

Figure-2.1 Types of Attacks on Cryptosystem

Snooping is a method to access top secret information of a person or some organization or association by the means of unauthorized access. Snooping consist of an attacker scrutinize the emails sent or received by a particular person or by watching somebody typing on his system in the real time based by using purposely designed software to gain remote access. Cybercriminals are generally used as spyware tool which is known as keyloggers. They use keyloggers to take by and by recognizable data, login qualifications and delicate venture information. It is a kind of reconnaissance innovation used to screen and follow every keystroke composed on an unambiguous PC's console. Once in a while keyloggers knew as a keystroke lumberjack or framework screen. Keyloogers software is also accessible for use on smart phones. They store each key stroke that has been pressed on the keyboard and the beauty of these key loggers is their property to work in invisible mode, where the prey is unaware of security breach.

Traffic Analysis is a method of capture and extracting meaningful information from the traffic packets that are being transmitted via network between sender and receiver. Users engaged in the communication are unconscious about the reality that their communication lines are being tapped or hacked by an attacker. It can also be executed when the messages that are being transmitted are encrypted and used to find out some momentous patterns in communication. Moreover, traffic analysis can also reveal confidential information like Internet Protocol addresses (IP addresses) with Media Access Control addresses (MAC addresses) of the sender and receiver. These addresses are further utilized to make public their geological location.

2.2 Active Attack

In active attacks, a intruder tries to influence or manipulate the data being transmitted through a network or within a system for the intention of infecting a computer using Virus, Trojan horses or worms. Active attacks can be easily acknowledged but are complicated to prevent because legitimate or genuine user have no control over their own system while under attack. Four categories of active attacks are Masquerade, Replay, Modification, and Denial of Service.

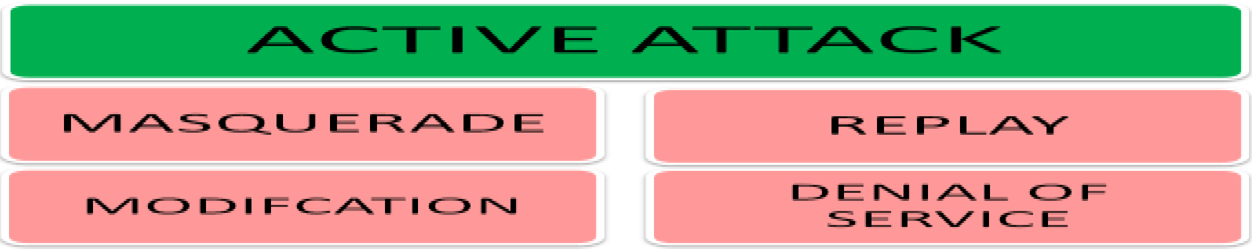

Figure-2.2 Types of Attacks on Cryptosystem

Masquerade is type of an active attack where an intruder makes believe to be the legitimate or genuine user in order to achieve unauthorized access or higher privileges. Masquerade might work with guesstimate of usernames and passwords or by finding security loop holes in a system. This attack forced or manipulated in such a way that the banks and various other online shopping or trading websites to alert their users after a specific period of time for the point of changing or altering their passwords.

Replay is also type of an active attack where the hacker intercepts a message and stores it locally on its own system, then resend the same message again to the intended receiver. Let easily understood with an illustration where a person sends request to his bank to transfer some amount to one of his friend and an attacker intercepts or hacked that message and after some time sends it again to the bank friend and an attacker intercepts that message and after some time sends it again to the bank.

Modification

In this attacker alters or modify the actual contents of an original message for the intention of gaining personal benefit may be in term of fame or money. Modified message can also be used synchronously with replay attack. Furthermore, intruder or imposter can also manipulate the message headers to reroute the same message but some other destination in such a way that harm the original sender. Suppose if a spy intercepts a message sent by a chief officer from the war area requesting to send reinforcements is transformed to something else and changes the course of war to absolutely reverse side.

Denial of Service

It is that type of the active attack that has the potential to momentarily or totally shut down an entire service provided by a dedicated server. Attacker can launch avalanche (sudden large amount) of service requests to overload a web server which ultimately leads to crash. At a higher level of superiority, an attacker can reroute the packets or bundles from already infected machines to bamboozle the automatic systems employed to identify Denial of Service attacks.

3. Ultimate Goal of the Computer Security

The ultimate goal of computer security is to protect our communication devices to the unauthorized malicious attackers. There are so many concepts all together works and reach the goal of cyber security such as CIA (Confidentiality, Integrity and Availability) Traid, Authentication, Non repudiation and Access control. **CIA TRAID** is the amalgam of the three concept namely, confidentiality, Integrity and availability.

Confidentiality
CIA TRAID
Integrity
Availablity

Figure-3 CIA Traid

Confidentiality is equivalent to privacy and refers to the protection of secret information from unauthorized users or attackers by employing encryption techniques and also to make confident that legitimate users can in fact access that information. Two other concepts works behind this namely Data Confidentiality and Privacy

- **Data confidentiality** gives affirmation that private or secret information isn't made open or unveiled to some other unapproved people.
- **Privacy g**uarantees that people control or impact what data identified with them might be gathered and put away and by whom and to whom that data might be unveiled in any capacity not share it.

Integrity

It is the second concept of CIA triad which is also important as confidentiality. It ensures that during the data transfer from one device to another device there is no modification or leaked of the data by the unauthorized person. Only the authorized person can able to modification and rectifies the information or any data. This term covers two related ideas namely Data Integrity and System Integrity

- **Data integrity**

It guarantees about the data and projects are changed just in an exact and definitive way and just by the approved individual.

- **System integrity**

It gives affirmation that a framework plays out its well-proposed work in a healthy way, free from the conscious or accidental unapproved control of the framework.

Availability whenever genuine users needs the whatever information wants easy available for them which ensures the availability legitimate users. Every bit of information has a specific value, only when authorized users access it at right times. It requires modification and maintenance of hardware immediately upon any problem. Security mechanism function is like that its affording auto detection of malicious requests and advanced hardware.

Authentication simply means of authentication is identification or detection. It is a mechanism that is used to find out in such a manner whether someone is real that person what he has affirmed to be. The assets of being real and being are capable to be checked and reliable; trust in the legitimacy of a transmission, a message, or message maker. This implies confirming that clients are who they articulate they are and that information gotten at the framework drew closer from a confided in area and source.

Non Repudiation is the concept behind non repudiation is that if the parties whenever neither involves in an online transaction to did not refuse receiving a successful transaction nor can they deny having commenced the transaction. It is the ability to prove that an operation has taken place at a scrupulous time. It can cause messy situation whenever lacking in non-repudiation comes. Visualize a circumstance where the beneficiary in a bank transaction informs that he has not received the desired amount of money and sender in not capable of providing the confirmation of successful completion of the transaction. Security system for non-repudiation includes the use of digital signatures. Digital signatures validate that the message has been sent by the intended user because they utilize sender’s private key to digitally sign a document.

Access control is the method is accountable to providing privileges to different types of legitimate or genuine users act in an organization or on particular system. This mechanism can provide or alter permissions related to read, write and delete a particular file according to the designation of a person. Sometimes Access control is also referred as selective limitation of access to resources and can be provided with the help of usernames and biometric devices

4. CONCLUSIONS

There is no doubt that the future is the era of Information technology and it is also fact as like the technology growth simultaneously there is always probability of the cyber criminal attacks the system. It just like that everything is some advantages and some disadvantages also. There is only one way to secure that always update the system, aware the new technology in the IT sector, always visit trusted sites and most important whenever share something internet always use encryption techniques .

5. REFERENCES

[1]. Michael Nieles ,Kelley Dempsey and Victoria Yan Pillitteri, Computer Security Division Information Technology Laboratory of US department of Commerce, NIST Special Publication 800-12 Revision 1 “An Introduction to Information Security” June 2011

[2]. William Stallings, “Cryptography and Network Security: Principles and Practice”, Pearson Education/Prentice Hall, 5th Edition.

[3]. Atul Khate,” Cryptography and Network Security” 3rd Edition

[4]. Anu, Divya Shree and Seema Ahlawat, “A Review on Cryptography, Attacks and Cyber Security “ International Journal of Advanced Research in Computer Volume 8, No. 5, May-June 2017

[5]. Swati Kashyap and Er. Neeraj Madan, “A Review on: Network Security and Cryptographic Algorithm”, Int. Journal of Advanced Research in Computer Science and Software Engineering, , April 2015

[6]. Jangala. Sasi Kiran M.Anusha, A.Vijaykumar, M.Kavya, “Cryptography: The Science of Secure Communication” IJCSNS, April 2016