International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 6 Issue: 7 12 - 16

A Review on Various Methods of Cryptography for Cyber Security

Dr. Ekta Agrawal
Assistant Professor,
Department of Computer Science
Shri Vaishnav Institute of Management, Indore, M.P., India
e-mail:ektaagrawal4jan@gmail.com

Dr. Jitendra Jain
Assistant Professor,
Department of Computer Science
Shri Vaishnav Institute of Management, Indore, M.P., India
e-mail: jitendra1974@gmail.com

Abstract: In the today's world of digital communication networks, the privacy and security of the transmitted data has become a basic necessity for communication. Data Security is the science and study of techniques of securing data in computer and communication systems from unknown users, disclosures and modifications. Cyber security issues plays a vital role in moving towards digital information age. Therefore, the encryption and decryption systems have been implemented for protecting information. The internet users are rapidly increasing day by day which causes a lot of cyber-criminals. The security of not only the single system but the entire systems will be ensured by the task of network security and controlled by network administrator. In this paper, an attempt has been made to review the various methods of Cryptography and how these methods will help to secure data from unauthenticated users. This paper has primarily focused on Cyber Security and Cryptographic concepts. This paper has also discusses the various attacks and cryptographic algorithms that are used in various applications of cyber security.

Keywords: *Cryptography, Encryption, Decryption and Cyber Security*

*****

I. INTRODUCTION

Cryptography is a technique of transforming and transmitting private data in an encoded way so that only authorized and intended users can obtain or work on it. The word *cryptography* [1] is derived from the Greek words *Κρυπτο* which means hidden or secret. The art of converting the simple text message into unreadable message is termed as cryptography. Cryptography provides the method of sending information between communicators such that intruders are unable to read the message. The unknown users want to break the non readable text which is not an easy task. The non readable message will be converted into readable form by the authorized person.

Information security aspects such as confidentiality, data integrity, entity authentication, and data authentication are provided by cryptography. [2,3]

II. COMPONENTS OF CRYPTOGRAPHIC SYSTEM

The basic components for cryptographic systems are as follows:

A. Plain Text

The Plain Text is used to describe the plain language message or information and the resulting encrypted. It is a message in a form that is easily readable by humans. In cryptography, plaintext is ordinary readable text before being encrypted into cipher text or after being decrypted. For example, Paul is a person wishes to send "Cryptography and cyber security are related to each other" message to the person Justin. Here "Cryptography and cyber security are related to each other" is a plain text message.

B. Cipher Text

The unreadable output of the encryption algorithm is known as cipher text. In cryptography, cipher text (ciphertext) is data that has been encrypted. For example, "Ajd672#@91uk l8 *^ 5% uh Bhywu29" is a Cipher Text produced.

C. Encryption

Encryption is a process of converting information or data into coded format and especially prevents form unauthorized users. Cryptography uses the encryption technique to send confidential messages. An encryption algorithm and a key are the part of process of encryption. The sender follows the encryption process. [7,8]

D. Decryption

Decryption is used to describe a method of un-encrypting the data manually using the proper codes or keys. Cryptography uses the decryption technique at the receiver side to obtain the original message from unreadable message (Cipher Text). A Decryption algorithm and a key are the part of process of decryption. Generally the encryption and decryption algorithm are same. [2,3]

E. Key

The key is a parameter or piece of information that determines the output of cryptographic algorithm.. It acts as private and provides secure communication.. For example, if the sender uses a key of +3 (Encryption Key) to encrypt the Plain Text "Cryptography" then Cipher Text produced will be "Fuswrjudskb". Similarly when the receiver uses a key of -3 (Decryption Key) to decrypt the Cipher Text "Fuswrjudskb" then Plain Text obtained will be "Cryptography". [5]

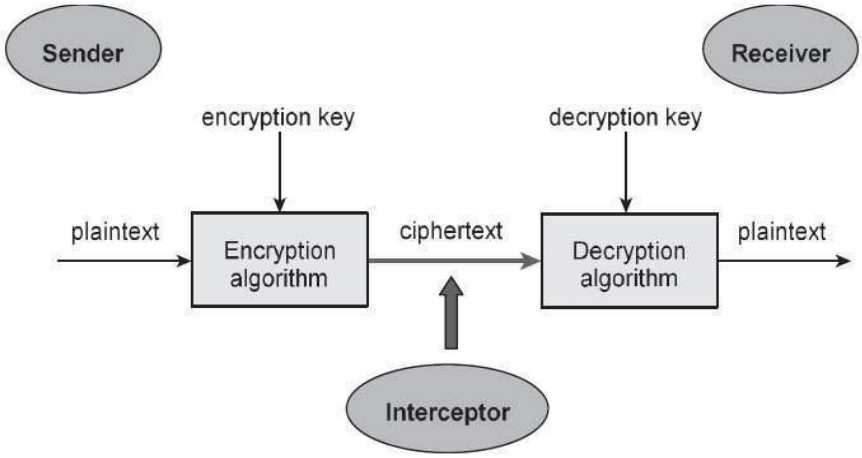

Fig. 1 Components of Cryptographic System

III. DATA SECURITY FACTORS

The important factors which are used for data security are shown with the help of Figure 2. They are as follows:

A. Confidentiality

The Sender and receiver should have right to access the contents of a data is specified as confidentiality. [9]

B. Authentication

Authentication is used to establish proof of identities. The origin of the data is correctly identified is ensured by this authentication process [9].

C. Integrity

The contents of the data remain the same when it reaches to the receiver is ensured by the integrity factor [9].

D. Non- repudiation

The person who cannot deny something is termed as Non-repudiation [9]

E. Access Control

This factor helps to specify who can access the data. [9]

F. Availability

Availability states that resources should be available to authorized users only. [9]

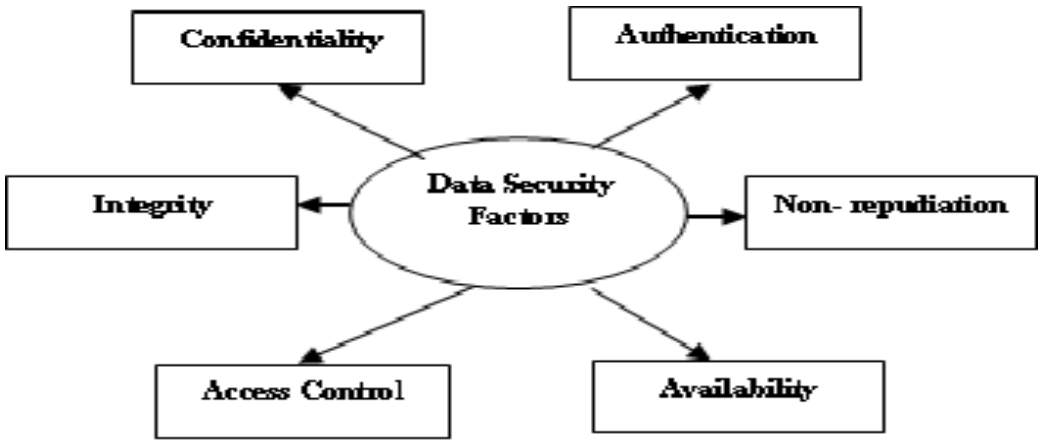

Fig. 2 Data Security Factors

IV. TYPES OF ENCRYPTION TECHNIQUES

There are two types of encryption techniques, known as symmetric cryptography which is also known as shared secret encryption and second is called public key encryption which is also known as asymmetric cryptography.

A. Private Key Cryptography or Symmetric Cryptography

This form of encryption uses a secret key, called the shared secret, to scramble the data into unintelligible gibberish. The person on the other end needs the shared secret (key) to unlock the data the encryption algorithm. User can change the key and change the results of the encryption. It is called symmetric cryptography because the same key is used on both ends for both encryption and decryption. The encryption and decryption process used by the sender and receiver in symmetric key cryptography is shown in Figure 3. [7,8,9]

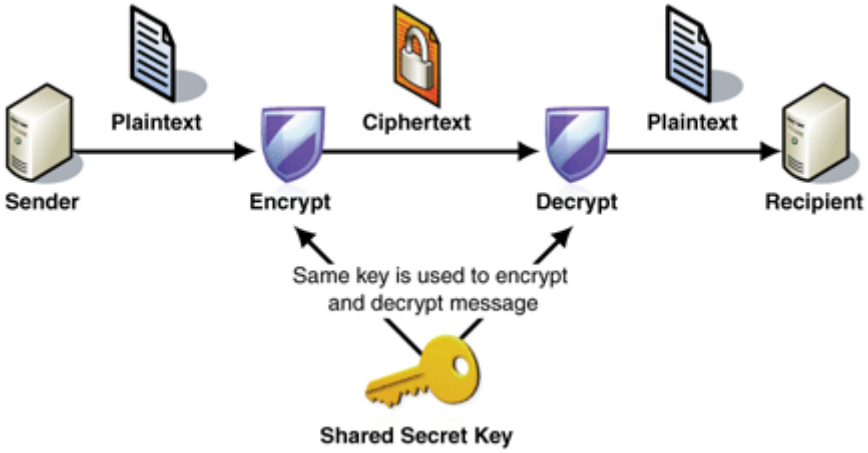

Fig. 3 Symmetric Key Cryptography

B. Public Key Encryption (PKE) or Asymmetric Cryptography

Asymmetric Cryptography uses encryption technique that divides the key into two different keys. The first key acts as public where as second key acts as private. The text is encrypted by user with the use of the recipient's public key. The receiver is decrypted by their private key. Figure 4 shows the working of Asymmetric Key Cryptography.[4,9]

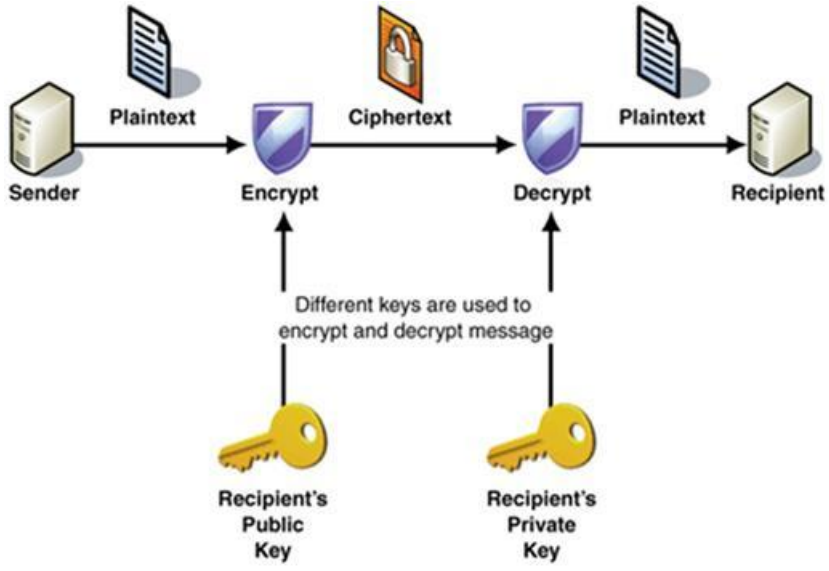

Fig. 4 Asymmetric Key Cryptography

V. MAJOR TYPES OF ATTACKS

Within a network, there are many attacks which are possible over any communication. The major types of attacks are as follows [3,6]:

A. Security Threats

Security threats are attacks where the system of the user is delayed in some manner that leads to loss of confidential data. This includes activities like service denying, attacking with viruses, malwares, spywares and Trojan horses. It also includes like intruding database or accessing Internet without permission.

B. Data capturing and cryptanalysis

This attack is performed while data is travelling in communication channels. The confidential data is captured or stolen from the channels and cryptanalysis is performed on it to extract the original data.

C. Unauthorized Installing of Applications

Virus intrusion and security breaching is achieved when unauthorized or uncertified applications within the system has been installed. To avoid it only certified applications must be allowed and unwanted applications such as audios, videos, games or other Internet applications must be avoided.

D. Unauthorized Access

Intrusion of any unauthorized person within the network resources leads to loss of confidential information. Hence proper authentication techniques for user's identity must be used and only resources must be monitored and checked from time-to-time.

E. Virus Infection

When network or resources are attacked with viruses, malware, Trojan horses or spywares leads to loss or manipulation of confidential data. It may sometimes destroy different resources and components of the network by effecting their source codes or hardware.

VI. AREAS OF CYBER SECURITY

The major areas which are included in cyber securities are as follows:

A. Application Security

Any software the user can use to run their business needs to be protected, whether the IT staff builds it or whether the user can buy it. Any application may contain holes, or vulnerabilities, those attackers can use to infiltrate user's application. [10]

B. Information Security

Information security is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. [10]

C. Email Security

The personal information is used by attackers to build phishing attacks to deceive recipients and send them to sites serving up malware. Incoming messages are blocked by an email security and controls outbound messages to prevent the loss of confidential information. [6.10]

D. Mobile Device security

Mobile devices and applications are targeted by cyber criminals. The user will also need to configure their mobile devices to keep network traffic secure. [10]

E. Web Security

Web security deals with websites' security, web applications and web services. Website security is the act of protecting websites from unauthorized access, use, modification, destruction or disruption. [10]

F. Wireless Security

Wireless security is the prevention of unauthorized access or damage to systems using wireless networks. The subset of network security that adds protection for a wireless computer network is termed as Wireless network security and also known as wireless security.

VII. CYBER SECURITY TECHNIQUES

Different techniques are used to overcome or prevent from these attacks on networks. Some of the major techniques are described here [3]:

A. Authentication

All data and documents received must be authenticated if they are sent by trusted sender or not. They must also be checked for unwanted breaching or alterations within data.

B. Antivirus

Antivirus software must be installed and updated on regular time intervals. Also network and systems checks must be conducted regularly.

C. Firewalls

This software keeps track of inward and outward traffic of any system. It also inform user about unpermitted access and usage.

D. Access Control

Each user must have their particulars like username and passwords so that only intended users may log in.

E. Cryptography

It is the technique of encoding plain text into cipher text before transmitting it over channel for avoiding stealing of confidential data.

VIII. CONCLUSION

In this paper the working of cryptography has been reviewed and ensures that data is not breached or manipulated during any communication. It has been also discussed about the various components of cryptographic algorithm, factors affecting security of data and types of encryption techniques. Data security can be maintained using different techniques like Cryptography, digital signatures, firewalls, access controls etc. Various attacks have been observed which has been protected through techniques of cyber security. The importance of secure communication has lead to popularity of cryptographic systems so it can be concluded that cryptography has emerged as an essential technique to safeguard our confidential information.

IX. REFERENCES

[1]. A. Kahate, "Cryptography and Network Security", 2nd Edition, Tata Mc-Grew – Hill Publisher ltd, 2011.

[2]. Anjula Gupta and Navpreet Kaur Walia, " Cryptography Algorithms: A Review", International Journal of Engineering Development and Research, ISSN: 2321-9939, Volume 2, Issue 2, pg.no-1667-1672.

[3]. Divya Sukhija, "A Review Paper on AES and DES Cryptographic Algorithms", International Journal of Electronics and Computer Science Engineering, ISSN: 2277-1956, V3 N4-354-359.

[4]. Gunjan Gupta nad Rama Chawla, "Review on Encryption Ciphers of Cryptography in Network Security", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 7 (July 2012).

[5]. Pranab Garg and Jaswinder Singh Dilawari, "A Review Paper on Cryptography and Significance of Key Length", International Journal of Computer Science and Communication Engineering, IJCSCE Special issue on "Emerging Trends in Engineering" ICETIE 2012.

[6]. Rajesh R Mane, "A Review on Cryptography Algorithms, Attacks and Encryption Tools", International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2320-9801, Vol. 3, Issue 9 (September 2015).

[7]. Swati Kashyap and Er. Neeraj Madan, "A Review on: Network Security and Cryptographic Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, April 2015 ISSN: 2277 128X.

[8]. Vikas agarwal et al., "Analysis and Review of Encryption and Decryption for Secure Communication", International Journal of Scientific Engineering and Research IJSER), ISSN (Online): 2347-3878, Volume 2, Issue 2 (February 2014).

[9]. Ekta Agrawal & Dr. Parashu Ram Pal, "A More Effective Approach Securing Text Data Based on Private Key Cryptography" in International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC) ISSN: 2321-8169, Volume: 5 Issue: 3, March 2017.

[10]. Jitendra Jain & Dr. Parashu Ram Pal, "A Recent Study over Cyber Security and its elements" in International Journal of Advanced Research in Computer Science (IJARCS) ISSN: 0976-5697, Volume: 8 Issue: 3, April 2017.