Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

A Review on Cryptography, Attacks and Cyber Security

Anu and Divya Shree
Assistant professor(Resource Person)
Department of Computer Science (UIET)
Maharshi Dayanand University
Rohtak, Haryana

Seema Ahlawat
Student
Department of Computer Science (UIET)
Maharshi Dayanand University
Rohtak, Haryana

Abstract: If we look at the world today then we will see that Internet has reached to each and every aspect of our day-to-day life. It is used for vital purposes and one of them is for communication, whether it is normal, business or confidential interactions. With enhancement of communication technology a need for secure communication also arises which is fulfilled by different encryption techniques like cryptography, digital signatures, watermarking, steganography etc. Cryptography is an encryption technique used for network security when different networks are interconnected and become venerable to attacks and intrusions.
In this paper we will review cryptography with its goals, types and algorithms used for it. Also types of attack used for intrusion and cyber security technology.

Keywords: Cryptography, cryptanalysis, cyber attacks, cipher text, key, terms, Cyber security, attacks.

INTRODUCTION

Cryptography is a technique of transforming and transmitting confidential data in an encoded way so that only authorized and intended users can obtain or work on it. It is a Greek origin word in which “crypto” means hidden and “graphy” means writing [4], so cryptography means hidden or secret writing. It introduces triads like confidentiality, non-repudiation, integrity and authenticity within ongoing data communication.

Cryptanalysis is process of defeating the work of cryptography. This word is also originated from Greece where kryptós stands for "hidden" and analýein means "to loosen" or "to untie" [8]. It is used to intrude or breach the cryptographic system with or without knowing the secret key of the process.

Cryptology is the study of cryptography and cryptanalysis together. Cryptography is sometimes also referred as Cipher-system. A basic illustration of cryptosystem is given in below figure (Fig1) where sender transforms plain text into cipher text using some encryption algorithm and secret key, then transmits it over the channel. At receiver’s side plain text is extracted from cipher text using decryption algorithm and decryption key.

(i) Components of Cryptographic system: -
Basic components of any cryptographic system are as follow:-
(a) Plain Text:- It is the secret or confidential data to be secured while transmission.
(b) Cipher Text: - It is the transformed and changed plain text which is not understandable while merely looking at it. It is obtained after applying encryption algorithm and encryption key over the plain text. It may or may not be safe guarded. If it’s not safe guarded then any intruder can access it easily from the public channel using which it is being transmitted. But decoding it without knowing the secret key is a tough task.
(c) Encryption Algorithm: - It is a mathematical step-by-step process used for converting plain text into cipher text based on some encryption key. Different examples of such algorithm are AES, DES, blowfish and serpent etc. It is used at sender’s side.
(d) Decryption Algorithm: - It is exactly the reverse mathematical process of used encryption algorithm. It takes cipher text and decryption key to produce original plain text. It is used at receiver’s side.
(f) Encryption Key: - This key is a value that is the lead aspect of the cryptographic system which is either known only to sender or to both sender and receiver. Safe guarding of this key is of great importance for making cryptographic system successful. This key is applied within encryption algorithm to generate cipher text out of plain text.
(g) Decryption Key: - This key is the value known to receiver and it may or may not be identical to encryption key. It is applied within decryption algorithm to generate the plain text back from received cipher text. A collection that contains all possible decryption keys is known as Key Space.

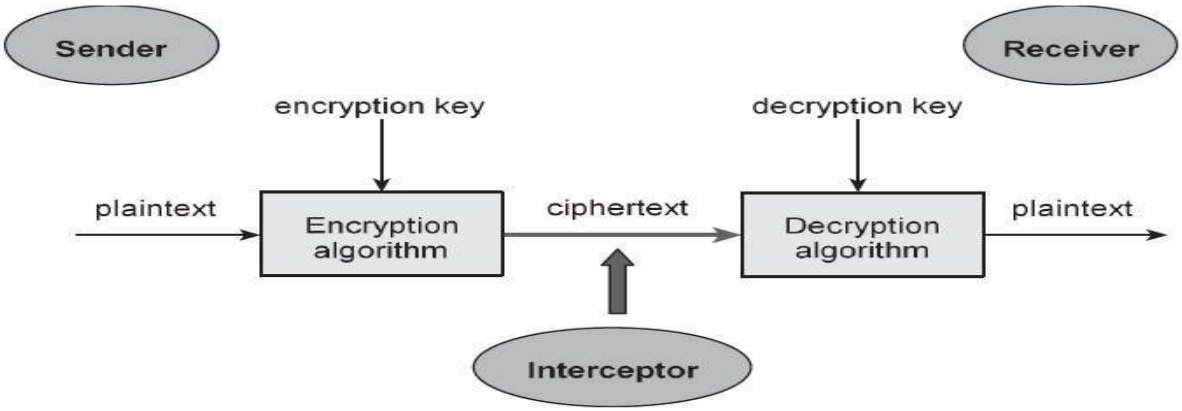

Fig1:- Cryptographic system

(ii) Goals of Cryptographic System: -

Every encryption system must ensure some features that contribute to secrecy of transmission; these features are referred as goals of cryptographic system. A bundle of such goals are focused but they can be categorized into main five such goals which are listed ahead: -

- Privacy or Confidentiality:- It is a feature that ensures that no one except the intended user can read the secret message.
- Authentication: - It is the process of verifying the identity of sender and receiver before interacting with the cryptographic system.
- Non-repudiation: - It is the feature used to ensure that sender is the one who has sent the message and feedback is being provided by the receiver only. Neither sender nor receiver could deny about message being sent by them.

(iii) Types of Cryptographic Systems: -

Cryptographic systems are usually divided into two basic types [5]: -

Symmetric Key Encryption: - It is that type of encryption where both sender and receiver share identical key. It is also called secret-key encryption. It could be implemented either using block cipher technique or stream cipher technique.Block Cipher performs encryption block-by-block of plain text whereas stream cipher performs encoding character-by- character.

Some examples of symmetric key encryption are AES (Advanced Encryption Standard) and DES (Data Encryption Standard).

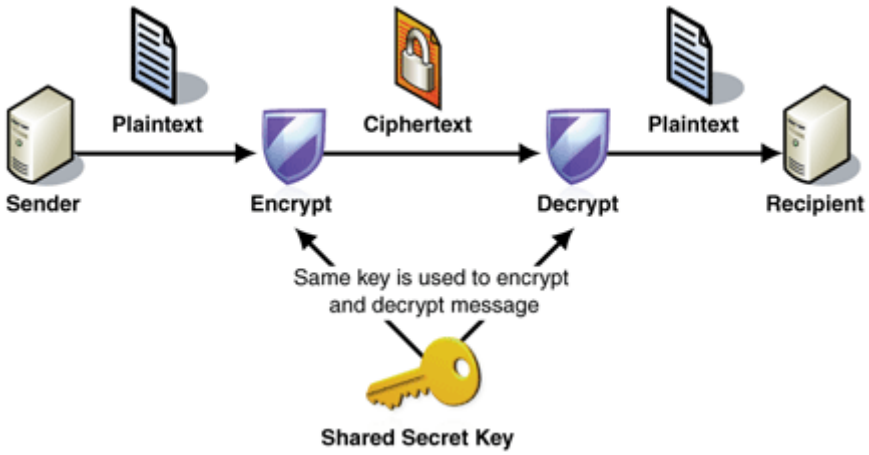

Fig2: - Symmetric Key Encryption

Asymmetric Key Encryption: - In symmetric key, the key has to be communicated safely to all receivers and sender without being breached which seemed tough task. To overcome the disadvantage of symmetric key type, asymmetric key encryption was developed. Here, two keys are used for cryptography process. Public key is used for encryption which is known to everyone and private key is used for decryption which is known only to user. This eliminates the need for sharing keys. It is also known as public-key encryption.

Some examples of asymmetric key encryption are Deffie-Hellman, DSA (Digital Signature Algorithm) and ElGamal etc.

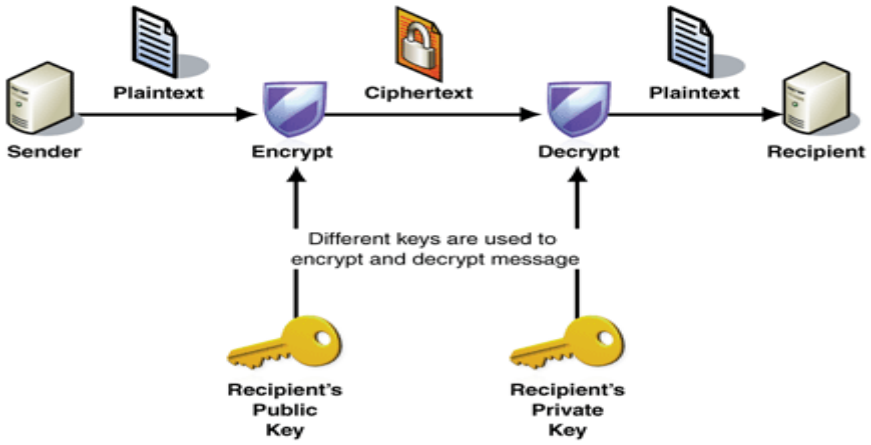

Fig3: - Asymmetric Key Encryption

MAJOR TYPES OF ATTACKS

Many attacks are possible over any ongoing communication within a network. Some major types of attacks are explained below [1]: -

(a) Security Threats: - Security threats are attacks where the system of the user is hampered in some manner that leads to loss of confidential data. This includes activities like service denying, attacking with viruses, malwares, spywares and Trojan horses. Also activities 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: - Installing unauthorized or uncertified applications within the system leads to virus intrusion and security breaching. 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 or in data records 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.

CYBER SECURITY TECHNIQUES

To overcome or undo the attacks on networks different technologies are used these days. Some of the major techniques are given below [1]:-

(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.

CONCLUSION

In this paper we reviewed how cryptography works and ensures that data is not breached or manipulated during any transmission. We also discussed about its types and goals. Data security can be maintained using different techniques like Cryptography, watermarking, digital signatures, firewalls, access controls and steganography etc. The importance of secure communication has lead to popularity of cryptographic systems so we can conclude that cryptography has emerged as an essential technique to safeguard our confidential information.

REFERENCES

[1].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).

[2]. 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.

[3]. 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.

[4]. 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.

[5]. 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).

[6]. 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).

[7]. Swati Kashyap and Er. Neeraj Madan, "A Review on: Network Security and Cryptographic Algorithm", International Journal of Advanced Research in
(January 2014).

Computer Science and Software Engineering, Volume 5, Issue 4, April 2015 ISSN: 2277 128X.

[8]. "https://en.wikipedia.org/wiki/Cryptanalysis", Online.

[9]. Ritu Pahal, Vikas Kumar,"Efficient implementation of AES", International journal of advanced research in computer science and software engineering, volume3, issue 7 (july2013).

[10].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