Research article Available online www.ijsrr.org ISSN: 2279–0543

International Journal of Scientific Research and Reviews

A Review on Cryptography In Information Security

Sahiba Mehndiratta

M.tech Scholar, [1]Department of CSE, Rawal Institute of Engineering and Technology, Faridabad, Haryana, India, Email: sahibamehandiratta@gmail.com

ABSTRACT

Cryptography in information security is the study and practice of techniques for secure communications, which is performed in the presence of third party. Cryptography is a secret sharing scheme and secret sharing of information. In this paper we proposed a cryptography which can be used to hide the original information from the unwanted user. The information can be in any standard format. The information is sent to the destination through network and then information is decrypted. We have to use symmetric-key cryptography and asymmetric-key cryptography. With the enhancement of communication technology and a need of secure information also arises which is fulfilled by different encryption techniques like: Cryptography, Steganography, Digital Signature etc. Cryptography is an encryption technique used for network security when different networks are interconnected and become venerable to attacks and intrusion. The resulting scheme maintains the perfect security of original information. Cryptography in information security is very important task for securing the information from unauthorized user. This paper also discusses the study of attacks that show how to protect the information oven in secure medium and from the external attackers.

KEYWORDS— Cryptography, Steganography, Goals of Cryptography, Types of Cryptography, Attacks

***Corresponding author:**

Sahiba Mehndiratta

M.tech Scholar,

Department of CSE,

Rawal Institute of Engineering and Technology,

Faridabad, Haryana, India

Email: sahibamehandiratta@gmail.com

INTRODUCTION

Cryptography is defined by the Greek word that is “krypto’s” which means “Hidden Secrets” and “Graphein” which means writing respectively. Cryptography referred as the encryption that defined the process of converting the information from plaintext to ciphertext. Decryption is opposite to the encryption process because ciphertext information back to plaintext information. A cipher is a pair that performed encryption and decryption. A cipher process is controlled by algorithm and by the key. The key is kept secret which is used for communication and it is necessary for decrypt the cipher text.

Cryptography is the process of hiding the information. It is the practice of techniques that converting the flat able data into the inflatable data and again converted into original format which provides Confidentiality, Integrity, Availability and Authentication.

Cryptography is a process of securing the information and communication by using codes and those who are intended can read and process it. In computer science, cryptography refers to protect the information and communication techniques based on mathematical concepts and set of rule based calculation called algorithms. These algorithms are used for key generation and digital signing and verification to protect the data privacy and confidential information like credit card transactions and email.

STEGANOGRAPHY

Steganography is the process that hides the messages with in the object, text, audio or picture in such a way that only sender and receiver can believe the presence of message. Steganography is similar to Cryptography. Steganography protects the content of the message and communication parties where cryptography protects only the contents of message. It is possible to combine both cryptography and Steganography together. The basic advantage of this combination is that higher level security is achieved that hides the meaning as well as the physical message. Steganography includes concealment of information in computer files.

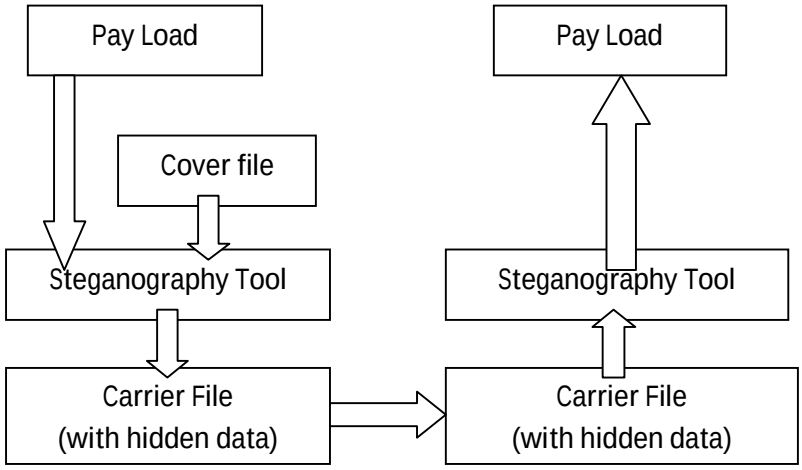

Figure2.1: STEGANOGRAPHY

Terms Used In Steganography

Carrier File: Carrier File is the file that hides the knowledge in Steganography.

Payload: It is the kind of knowledge that is to be hidden in Steganography.

Steganalysis: It is the type of method that concealing the knowledge from a carrier file.

Redundant-Bits: It is the type of knowledge within the file which may be altered without damaging the file.

Steganography is the approach of sending the hidden knowledge in such a way that no one is aware of that the secret key message was sent. There are not any ciphers or other alternative encryption like it is in cryptography. It is conjointly referred to as cover writing. Steganography is an attempt to achieve secure and undetectable communication. Steganography provides only secure and undetectable communication. The protection of the Steganography depends on the secrecy of the information encoding system.

GOALS OF CRYPTOGRAPHY

To protect IT information it is required to classy problems & create a security goal which are being attacked is Confidentiality, Integrity and Availability.

Confidentiality

Confidentiality is a matter of great concern to information security that Organization information should be confidential. Information should be stored under safe custody so that it cannot be accessed by unauthorized people and confidentiality should be maintained while it is being transferred to other entity for its uses. Under Network computing Environment only authorized system administrators are allowed to handle stored Data on server & only authorized user those are permitted to access data from server under strict watch and monitoring process.

Integrity

Integrity of information means that information would be required to change as and when required by the authorized entities with an authorized systematic established process where information Integrity can be checked and ensured. Under Network computing environment Data is being shared on servers and modification keeps happening as per need by authorized entities those can be tracked in case of any failure of information.

Availability

The beauty of information it should be available as per need to the authorized entities and should not be available to unauthorized one. Information need to be modified and stored at right place by the authorized entities, the entire process need to be strongly monitored under "Network" computing environment.

Authentication

Authentication provides the identification of the conceiver. It confirms to the receiver that the information received has been sent only by a known association and verified sender. Authentication service has two variants –

Message authentication identifies the conceiver of the message with none of the regard router or system that has sent the message.

Entity authentication is assurance that the knowledge has been received from a particular entity, say a selected website.

TYPES OF CRYPTOGRAPHY

Fundamentally, there are two styles of cryptosystems supported the way during which encryption-decryption is carried out in the system −

- Symmetric Key Encryption
- Asymmetric Key Encryption

The main distinction between these cryptosystems is that the relationship between the encryption and the decryption key. Logically, in any cryptosystem, each the keys are closely associated. It is much not possible to decrypt the ciphertext with the key that's unrelated to the encryption key.

Symmetric Key Encryption

The encryption method is the process wherever same keys are used for encrypting and decrypting the knowledge is thought as Symmetric Key Encryption.

The study of symmetric cryptosystems is termed as symmetric cryptography. Symmetric cryptosystems are generally remarked as secret key cryptosystems. A widely known examples of symmetric key encryption methods are − Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

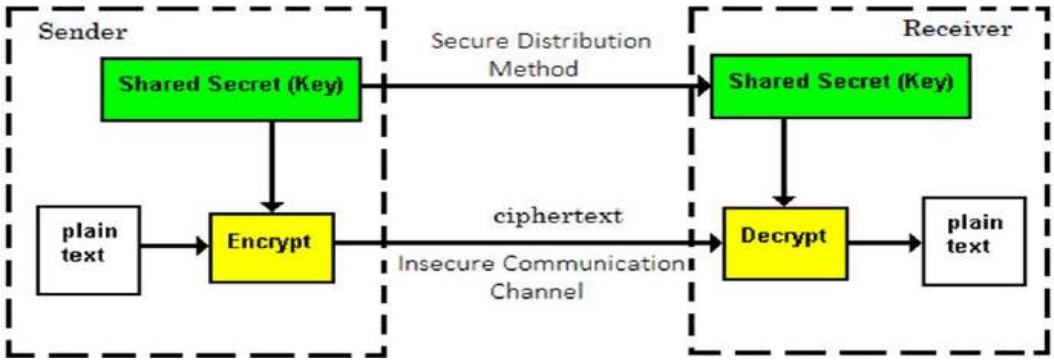

Figure4.1: SYMMETRIC KEY ENCRYPTION

The features of cryptosystem that supported the symmetric key encryption are −

- Persons using symmetric key encryption should share a typical key before to exchange of data.
- Keys are recommended to be modifying frequently to prevent any attack on the system.

ASYMMETRIC KEY ENCRYPTION

The encryption method wherever totally different keys are used for encrypting and decrypting the knowledge is thought as Asymmetric Key Encryption. Although the keys are totally different, they're mathematically connected and therefore, retrieving the plaintext by decrypting ciphertext is possible. The method is depicted within the following illustration –

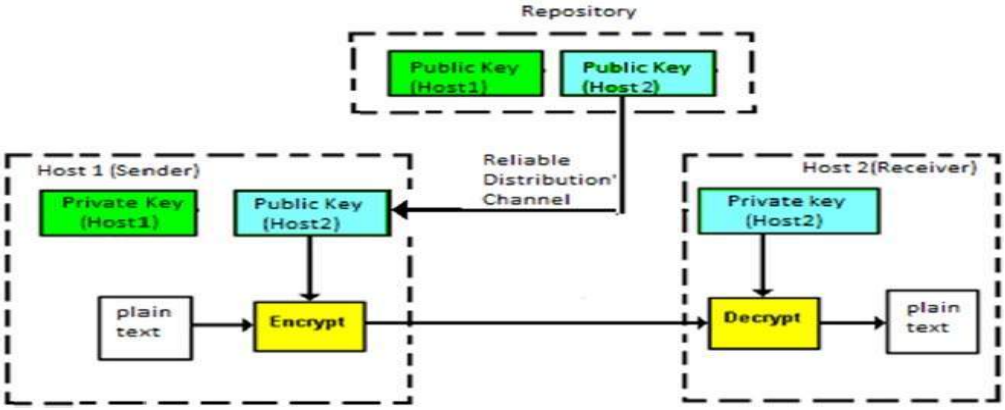

Figure4.2: ASYMMETRIC KEY ENCRYPTION

Features of this encryption method are as follows −

- Each user within the asymmetric system must have a pair of dissimilar keys, non-public key and public key. These keys are mathematically connected − once one secret key is used for encoding and the other is used for decoding the ciphertext back to the first plaintext.

- It needs to put the general public key in public repository and also the non-public key as a well-guarded secret. Hence, this method of encryption is additionally referred as Public Key Encryption.

ATTACKS

Side Channel Attack

Side Channel Attack contains the extra data based on physical implementation of a cryptography formula together with hardware that is employed to encrypt the information and rewrite (decrypt) the data. The cryptography attack techniques access to plaintext or ciphertext and generally contains both the text and possibly the cryptography algorithm: A side channel attack sometimes contains the extra information like time taken to performing the calculation, voltage used and so on. Some side channel attacks are discovered. One of the aspects of side channel attack is network based attack versus Open SSL.

Open SSL used only two styles of multiplication: one is for equal sized words that are called as Karatsuba and other alternative multiplication is unequal sized words. The Karatsuba is quicker than the unequal sized words and completely different in speed may be detected by networking using the SSL TCP/IP connection. Another example of side channel attack is timing attack.

Timing Attack

Timing attack is one the instance of side channel attack. The time period of program is taken into account as a constraint, some parameter should be reduced by the coder. The time period of cryptography device may represent the knowledge channel and provide the attacker with priceless information once secret parameters connected in it. This is the idea that outlined by the timing attack. The context is that of associate RSA signature, and therefore the goal of the attacker is to recover the secret key exponent d. A standard method to perform a standard modular exponentiation is that the square and multiply algorithm. The formula is especially a sequence of standard multiplications and squares (which we are going to regard easy multiplication of a price by itself) once implemented in a scholar way, modular multiplications are time-consuming operations. Montgomery proposed an ingenious thanks to speed-up these operations, by transferring them to a modulus that is best suited to the machine's internal structure.

Algorithm 2 Sq. and multiply

$x = m$

For $i = w - 2$ down to zero do

$x = x^2 \bmod n$

If d_i == one then

$x = x \cdot m \bmod n$

End if

End for

Return x

The attack is a associative iterative divide and conquers attack: we are going to begin by attacking the first unknown bit dw−2, and, at every step of the attack, assume we all know bits dw−1 . . . di+1 and recover bit d_i.

Here, d_{w-1} denotes the foremost important significant bit of d (which we tend to assume to be equal to 1) and d_0 denotes the lsb.

Brute Force Attack

A brute force attack is a methodology used to acquire private user data like usernames, passwords, passphrases, or Personal Identification Numbers (PINs). These attacks are typically carried out using a script or larva to 'guess' the specified data till one thing is confirmed. Brute force attacks will be enforced by criminals to undertake to access encrypted data/information. Whereas you would possibly assume a password keeps your data/information safe, analysis has shown that any eight-character password will be cracked in less than six hours.

A Brute Force Attack is the simplest methodology to realize access to a website or server (or something that's password protected). It tries different combinations of usernames and passwords once more again and again until it gets in. This repetitive action is like a military attacking a fort.

Brute force attacks are usually mentioned as brute force cracking. Indeed, brute force — during this case computational power — is employed to undertake to crack a code. Instead of employing a complicated algorithm rule, a brute force attack uses a script or larva to submit guesses till it hits on a mix that works.

There are many of tools simply available to assist hackers launch brute force attempts. However even writing a script from scratch wouldn't be an excessive amount of a stretch for somebody comfortable with code. Whereas these attacks are simple to execute, depending on the length and nature of the password and therefore computational power used, they may take days, weeks, or may be years to achieve success.

Before we glance at a way to spot and stop against brute force attacks, we should always note some another terms associated with this topic.

Hybrid Brute Force Attacks

A brute force attack uses a systematic approach to idea that doesn't use outside logic. Similar attacks include a **dictionary attack**, which could use an inventory of words from the dictionary to

crack the code. Another alternative attacks would possibly begin with ordinarily used passwords. These are typically described as brute force attacks. However, according to the result they used some logic to decide that iterations is also the foremost doubtless first, they are a lot of accurately mentioned as hybrid brute force attacks.

Reverse Brute Force Attack

A reverse brute force attack involves employing a common cluster of password or group of passwords against multiple double usernames. This doesn't target one user however might be used to try to gain access to a selected network.

The best protection against this type of attack is to use sturdy passwords, or from associative administrator's point of view, need that sturdy passwords are used.

Credential Stuffing

Credential stuffing may be a unique variety of brute force attack that uses broken username and password pairs. If a username/password pairing is understood, an associative attacker will use it to realize access to gain multiple sites. Once during a user's account, they need full management over that account and access to any of the small details it holds.

Precautions like two-factor authentication and security queries can help to prevent damage by these forms of attacks. However, the best simplest protection is for users to never use the same password for multiple accounts.

THE GOAL OF A BRUTE FORCE ATTACK

Once a hacker makes a successful login try, what's next? The solution may be a whole vary of things can be carried out. Here are some of the main ones:

- Stealing or exposing users' personal data found within online accounts
- Harvesting sets of credentials purchasable to third parties
- Posing as account house owners to spread fake content or phishing links
- Stealing system resources to be used in alternatives activities
- Defacement of an internet site through gaining access to admin credentials
- Spreading malware or spam content or redirecting domains to malicious content

CONCLUSION

We use different kinds of algorithms to determine security services in several service mechanisms. We have tendency use either personal key cryptography or public key cryptography per demand. If we would like to send message quickly we have a tendency to use private key algorithm and if we want to send messages secretly we use public key algorithm. As we have tendency to

toward a society wherever automated information resources are inflated and cryptography can still increase in importance as a security mechanism.

Electronic networks for banking, shopping, internal control, benefit and service delivery, information/data storage and retrieval, distributed process and government applications can want improved strategies for access control management and data/knowledge security. The information/data security can be easily achieved by using Cryptography technique.

Cryptography will avoid extortion in electronic trade and guarantee the legitimacy of financial exchanges. It will demonstrate your identity or guaranteed your obscurity. It keeps vandals from modifying webpage and keeps fashionable contenders from perusing secret records. Furthermore, later on, as business and communication keep on moving to PC systems, cryptography will get to be more crucial.

The essential requirements for security incorporate confidentiality, validation, integrity and non-renouncement to represent such security administrations, most frameworks uses two noteworthy categories of cryptographic algorithm to be specific symmetric-key and public-key algorithms. In symmetric-key same secret key is utilized for both encryption and decoding. Public-key algorithms are in light of the thought of differentiating the key used to disorganise a message from the one used to rewrite it. Symmetric algorithms are speedier than asymmetric yet have a number disadvantages like absence of scalability, troublesome key administration and provides simply privacy. The selection of cryptosystem depends on the matter and therefore the form of the task wherever to be applied. If speed is required in a secure network group symmetric ciphers are used however if communication in an unsecured network group then asymmetric ciphers are used and wherever security is much important then the speed then hybrid systems are the best simplest selection.

FUTURE SCOPE

The future scope of cryptography is to victimization of the various styles of attacks to raising the network security by performing the protection on the network that increase the user needs. To transmit the information over the web will maintain security by having setup like anti-virus, regular updates, observance spreading awareness and education. We will additional use alternative cryptography so per the user demand better higher results can be found out. All the techniques have their own blessings. Thus we will realize effective and efficient results. We have tendency to use different types of algorithms to determine security services in several service mechanisms. We have tendency to use either personal key cryptography or public key cryptography according per demand. If we would like to send message quickly we have a tendency to use personal key algorithm and if we want to send messages secretly we use public key algorithm.

REFERENCES

1. Zhang hong" Chaos Theory and its Application in Modern Cryptography", 978-1-4244-7237-6/10/$26.00 ©201O IEEE
2. Sourabh Chandra Sk Safikul Alam" A comparative survey of symmetric and asymmetric key cryptography", 978-1-4799-5748-4/14/$31.00 © 2014 IEEE
3. Rajnikant Pandey"Cryptography & Security implementation in Network Computing Environments ",978-9-3805-4421-2/16/$31.00_c 2016 IEEE
4. Shehnaz T. Patel" Lightweight Cryptography in WSN", 978-I-S090-00S 1-7I 1S/$3 1.00©20 IS IEEE