International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

A Review Paper on Network Security and Cryptography

Preeti Dewangan

Assistant Professor CSE, Rungta College of Science & Technology, Durg (C.G.), India

Abstract: ***Cryptography is the science of information security. The word is derived from the Greek kryptos, meaning concealed. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide in order in storage or transit. Modern cryptography intersect the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords. Cryptology prior to the modern age was almost one and the same with Encryption, the translation of information from a understandable state to apparent nonsense. The sender retained the ability to decrypt the information and therefore avoid redundant persons being able to read it.***

Keywords: Security, Cryptography, Encryption.

1. Introduction

Human being from ages had two inherent needs − (a) to converse and share information and (b) to commune selectively. These two requirements gave rise to the art of coding the communication in such a way that only the deliberate people could have access to the information. unlawful people could not extract any information, even if the scrambled communication fell in their hand. The art and science of concealing the messages to introduce silence in information security is predictable as cryptography. The word 'cryptography' was coined by combining two Greek words, 'Krypto' significance hidden and 'graphene' meaning writing.

1.1 History of Cryptography

The art of cryptography is measured to be born along with the art of writing. As civilizations evolved, human beings got prearranged in tribes, groups, and kingdoms. This led to the appearance of ideas such as power, battles, primacy, and politics. These ideas further fueled the natural want of people to communicate secretly with careful recipient which in turn ensured the continuous growth of cryptography as well.

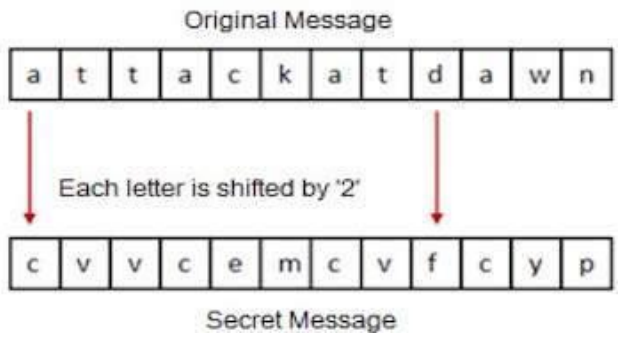
The roots of cryptography are start in Roman and Egyptian civilizations.

Hieroglyph − The Oldest Cryptographic Technique

The first identified evidence of cryptography can be traced to the use of 'hieroglyph'. Some 4000 years ago, the Egyptians used to correspond by messages written in hieroglyph. This regulations was the secret known only to the scribes who used to transmit messages on behalf of the kings. One such primitive writing is shown below.

Later, the scholars irritated on to using simple mono-alphabetic substitution ciphers during 500 to 600 BC. This involved replacing alphabets of message with other alphabets with some covert rule. This rule become a key to retrieve the note back from the garbled message.

The earlier Roman technique of cryptography, usually recognized as the Caesar Shift Cipher, relies on broken up the letters of a sense by an agreed figure (three was a common choice), the recipient of this message would then shift the letters back by the same number and get the original message.



Modern cryptography is the keystone of computer and communications security. Its base is based on various concepts of mathematics such as number theory, computational-complexity theory, and probability theory.

1.2 Characteristics of Modern Cryptography

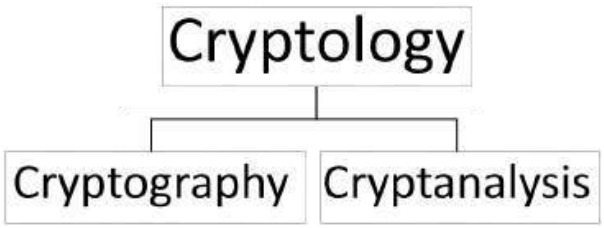
There are three main characteristics that divide modern cryptography from the classical approach.

Classic Cryptography	Modern Cryptography
It manipulates fixed characters, i.e., letters and digits directly.	It operates on binary bit sequences.
It is mainly based on 'security through obscurity'. The techniques working for coding were kept secret and only the parties involved in communication knew about them.	It relies on openly known arithmetical algorithms for coding the information. confidentiality is obtained through a secrete key which is used as the seed for the algorithms. The computational difficulty of algorithms, nonattendance of secret key, etc., make it not possible for an attacker to obtain the original information even if he knows the algorithm used for coding.
It requires the entire cryptosystem for communicating in secret.	Modern cryptography require parties paying attention in secure message to have the secret key only.

1.3 Context of Cryptography

Cryptology, the study of cryptosystems, can be subdivided into two branches −

- Cryptography
- Cryptanalysis



What is Cryptography?

Cryptography is the art and science of making a cryptosystem that is able of providing information safety.

Cryptography deal with the actual secure of digital information. It refers to the design of device based on arithmetical algorithms that provide basic information security services. You can think of cryptography as the organization of a large toolkit contain different techniques in safety application.

What is Cryptanalysis?

The art and science of contravention the cipher text is recognized as cryptanalysis.

Cryptanalysis is the sister bough of cryptography and they together co-exist. The cryptographic procedure consequences in the cipher text for broadcast or storage. It involve the learn of cryptographic mechanism with the meaning to break them. Cryptanalysis is also used during the design of the fresh cryptographic technique to test their security strength.

V Security Services of Cryptography

The primary purpose of using cryptography is to give the following four basic information security services. Let us now see the likely goals intended to be satisfied by cryptography.

Confidentiality

Confidentiality is the basic security service provided by cryptography. It is a safety service that keeps the in order from an unauthorized person. It is from time to time referred to as privacy or secrecy. Confidentiality can be achieve through many means starting from physical secure to the use of arithmetical algorithms for information encryption.

Data Integrity

It is safety service that deals with identify any alteration to the data. The information may get modified by an illegal entity intentionally or accidently. Integrity service confirm that whether data is whole or not since it was last created, transmitted, or stored by an authorized user. Data integrity cannot prevent the change of data, but provides a means for detect whether data has been manipulate in an illegal manner.

Authentication

Authentication provides the recognition of the originator. It confirm to the receiver that the data established has been sent only by an recognized and established sender.
Authentication service has two variants −

- Message authentication identifies the creator of the message with no any regard router or scheme that has sent the message.
- Entity authentication is pledge that data has been received from a specific entity, say a exacting website.
- Apart from the originator, authentication may also provide declaration about other parameter related to data such as the date and time of formation/transmission.

Non-repudiation

It is a security repair that ensures that an entity cannot refuse the possession of a previous commitment or an action. It is an guarantee that the original creator of the data cannot deny the formation or transmission of the said data to a recipient or third party.

Non-repudiation is a property that is most attractive in situations where there are probability of a argument over the exchange of data. For example, once an arrange is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation repair was enable in this transaction.

1.4 Cryptography Primitives

Cryptography primitives are not anything but the gear and technique in Cryptography that can be selectively used to give a set of desired safety services −

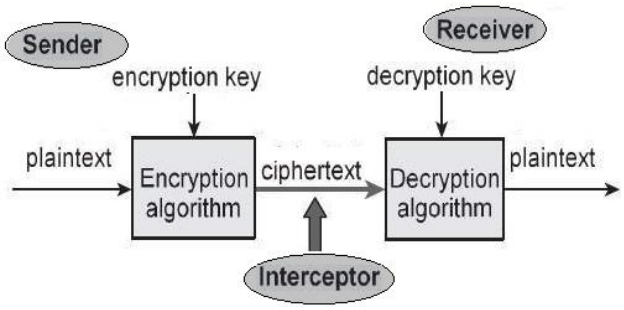
- Encryption
- Hash functions
- Message Authentication codes (MAC)
- Digital Signatures

The following table shows the primitives that can attain a particular safety repair on their possess.

Services \ Primitives	Encryption	Hash Function	MAC	Digital Signature
Confidentiality	Yes	No	No	No
Integrity	No	Sometimes	Yes	Yes
Authentication	No	No	Yes	Yes
Non Reputation	No	No	Sometimes	Yes

A cryptosystem is an execution of cryptographic technique and their associated transportation to provide in sequence security services. A cryptosystem is also referred to as a cipher scheme.

Let us discuss a simple model of a cryptosystem that provides privacy to the information being transmit. This essential model is depict in the picture below –



The design shows a sender who needs to transfer some responsive data to a recipient in such a means that any party intercept on the communication channel cannot extract the data.

The purpose of this easy cryptosystem is that at the ending of the procedure, only the sender and the receiver will be familiar with the plaintext.

1.5 Components of a Cryptosystem

The various mechanism of a basic cryptosystem are as follow −

- **Plaintext.** It is the data to be protected during communication.
- **Encryption Algorithm.** It is a arithmetical process that create a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that take plaintext and an encryption key as input and produce a ciphertext.
- **Ciphertext.** It is the twisted version of the plaintext produced by the encryption algorithm using a precise the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromise by anyone who has access to the communication channel.
- **Decryption Algorithm,** It is a numerical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that take a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm basically reverse the encryption algorithm and is thus closely connected to it.
- **Encryption Key.** It is a cost that is recognized to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in arrange to calculate the ciphertext.
- **Decryption Key.** It is a worth that is known to the receiver. The decryption key is connected to the encryption key, but is not for all time identical to it. The receiver inputs the decryption key into the decryption algorithm all along with the ciphertext in order to compute the plaintext.

For a given cryptosystem, a set of all likely decryption keys is called a **key space**.

An **interceptor** (an attacker) is an illegal entity who attempts to determine the plaintext.Can see the ciphertext and may know the decryption algorithm. He, however, must never know the decryption key.

Types of Cryptosystems

Basically, there are two type of cryptosystems base on the way in which encryption-decryption is carried out in the system −

- Symmetric Key Encryption
- Asymmetric Key Encryption

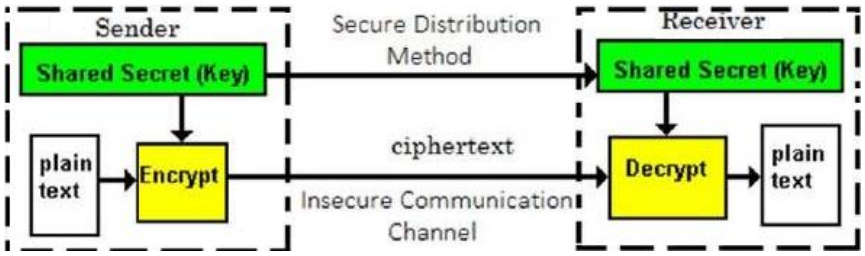
The main difference between these cryptosystems is the association between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely linked. It is practically not possible to decrypt the ciphertext with the key that is not related to the encryption key.

Symmetric Key Encryption

The encryption process where **same keys are used for encrypting and decrypting** the in order is known as Symmetric Key Encryption.

The learn of symmetric cryptosystems is referred to as **symmetric cryptography**. Symmetric cryptosystems are too now and then referred to as **secret key cryptosystems**.

A few famous examples of symmetric key encryption method are − Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.



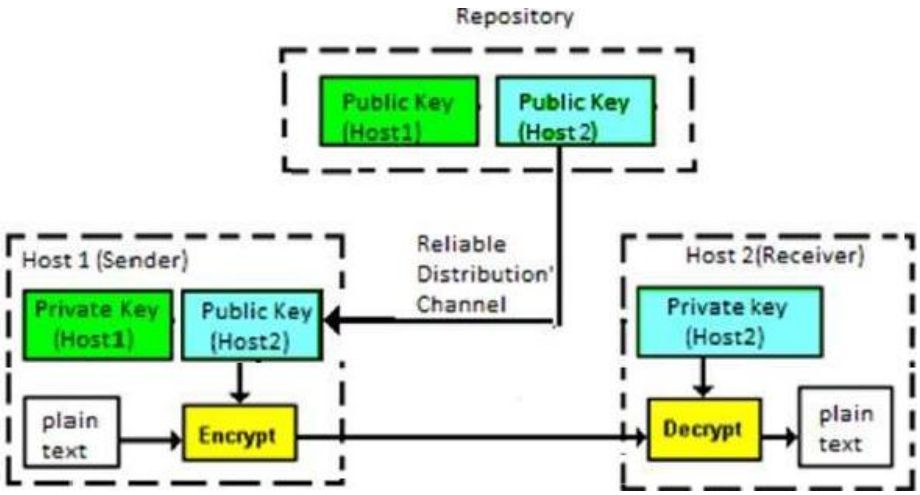
Preceding to 1970, all cryptosystems in a job symmetric key encryption. Even today, its significance is very high and it is being used lengthily in many cryptosystems. It is very unlikely that this encryption will fade away, as it has certain reward over asymmetric key encryption.

The most important features of cryptosystem base on symmetric key encryption are −

- Persons by symmetric key encryption must share a ordinary key prior to exchange of information.
- Keys are optional to be changed regularly to prevent any attack on the system.
- A robust mechanism desires to exist to swap the key between the communicating parties. As keys are necessary to be changed regularly, this mechanism becomes expensive and cumbersome.
- In a group of **n** people, to allow two-party communiqué between any two persons, the number of keys required for group is **n × (n – 1)/2**.
- Length of Key (number of bits) in this encryption is lesser and hence, process of encryption-decryption is earlier than asymmetric key encryption.
- Processing control of computer system necessary to run symmetric algorithm is less.

Asymmetric Key Encryption

The encryption process where **unlike keys are used for encrypting and decrypting the information** is known as Asymmetric Key Encryption. Though the keys are different, they are exactly related and hence, retrieve the plaintext by decrypting ciphertext is possible. The process is depict in the following picture −



Asymmetric Key Encryption was made-up in the 20th century to come over the require of pre-shared secret key between communicate persons. The most important features of this encryption scheme are as follows −

- Every user in this scheme needs to have a pair of unlike keys, **private key** and **public key**. These keys are exactly related − when one key is used for encryption, the other can decrypt the ciphertext back to the original plaintext.
- It require to put the public key in public repository and the private key as a well-guarded covert. Hence, this technique of encryption is also called **Public Key Encryption**.
- Though public and private keys of the user are related, it is computationally not possible to discover one from another. This is a power of this scheme.
- When *Host1* needs to send data to *Host2*, he obtains the public key of *Host2* from storehouse, encrypts the data, and transmit.
- *Host2* uses his private key to take out the plaintext.
- Length of Keys (number of bits) in this encryption is great and hence, the procedure of encryption-decryption is slower than symmetric key encryption.
- Processing power of computer system necessary to run asymmetric algorithm is superior.

Symmetric cryptosystems are a natural concept. In contrast, public-key cryptosystems are quite hard to comprehend.

Relation between Encryption Schemes

A précis of basic key property of two type of cryptosystems is known below:

	Symmetric Cryptosystems	Public Key Cryptosystems
Relation between Keys	Same	Different, but mathematically related
Encryption Key	Symmetric	Public
Decryption Key	Symmetric	Private

Payable to the advantages and disadvantage of together the systems, symmetric key and public-key cryptosystems are often use together in the sensible information security system.

2. Conclusion

Network security is a vital factor that many organization consider. An attack or threat may reason substantive loss of in order or data to an organization. It may also destroy critical infrastructure. It is, therefore, the best decision to develop a reliable security policy for the firm's network. The above network security policies can play a significant role in mitigating the risks that the firm may experience in its operational environment. All the security policies should ensure that the information and data are confidential without affecting its availability or integrity.