Cryptography

Rahul Laxmikant Gajre
Research Student

Abstract -

With the internet having reached a level that merges with our lives, growing explosively during the last several decades, data security has become a main concern for anyone connected to the web. Data security ensures that our data is only accessible by the intended receiver and prevents any modification or alteration of data. Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

INTRODUCTION -

Cryptography is a technique to achieve confidentiality of messages. The term has a specific meaning in Greek: “secret writing”. Nowadays, however, the privacy of individuals and organizations is provided through cryptography at a high level, making sure that information sent is secure in a way that the authorized receiver can access this information. With historical roots, cryptography can be considered an old technique that is still being developed. Examples reach back to when the ancient Egyptians used “secret” hieroglyphics, as well as other evidence in the form of secret writings in ancient Greece or the famous Caesar cipher of ancient Rome.

Billions of people around the globe use cryptography on a daily basis to protect data and information, although most do not know that they are using it. In addition to being extremely useful, it is also considered highly brittle, as cryptographic systems can become compromised due to a single programming or specification error

The importance of information and communication systems for society and the global economy is intensifying with the increasing value and quantity of data that is transmitted and stored on those systems. At the same time those systems and data are also increasingly vulnerable to a variety of threats, such as unauthorized access and use, misappropriation, alteration, and destruction.

The hiding of information is called encryption, and when the information is unhidden, it is called decryption. A cipher is used to accomplish the encryption and decryption. Merriam-Webster’s Collegiate Dictionary defines cipher as ―a method of transforming a text in order to conceal its meaning. The information that is being hidden is called plaintext; once it has been encrypted, it is called cipher text. To hide any data one technique mainly used is Cryptography.

Cryptography is the science of protecting data, which provides methods of converting data into unreadable form, so that Valid User can access Information at the Destination. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography is the transformation of readable and understandable data into a form which cannot be understood in order to secure data. cryptography refers exactly to the methodology of concealing the content of messages, the word cryptography comes from the Greek word "Kryptos", that means hidden, and "graphikos" which means writing.

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. It includes techniques such as microdots, merging words with images and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers. The information that we need to hide, is called plaintext , It’s the original text, It could be in a form of characters, numerical data, executable programs, pictures, or any other kind of information, The plaintext for example is the sending of a message in the sender before encryption, or it is the text at the receiver after decryption.

The data that will be transmitted is called cipher text , it's a term refers to the string of "meaningless" data, or unclear text that nobody must understand, except the recipients. it is the data that will be transmitted Exactly through network, Many algorithms are used to transform plaintext into cipher text. Cipher is the algorithm that is used to transform plaintext to cipher text, This method is called encryption, in other words, it's a mechanism of converting readable and understandable data into "meaningless" data.

The Key is an input to the encryption algorithm, and this value must be independent of the plaintext, This input is used to transform the plaintext into cipher text, so different keys will yield different cipher text, In the decipher side, the inverse of the key will be used inside the algorithm instead of the key.

The two fundamental techniques for encrypting data are “symmetric cryptography,” which entails the usage of the same key to encrypt/ decode information; and “asymmetric cryptography,” which makes use of public and private keys to encrypt/ decode information. Examples of symmetric algorithms are Data Encryption Standard (DES), Triple-DES (3DES), Blowfish, and Advanced Encryption Standard (AES). The most well-known asymmetric algorithms are RSA and ELGAMAL Schema.

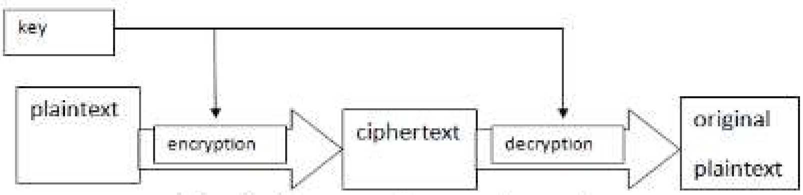

Fig. 1. Symmetric cryptosystem

In symmetric key cryptography is also known as private-key cryptography, a secret key may be held by one person or exchanged between the sender and the receiver of a message. If private key cryptography is used to send secret messages between two parties, both the sender and receiver must have a copy of the secret key.

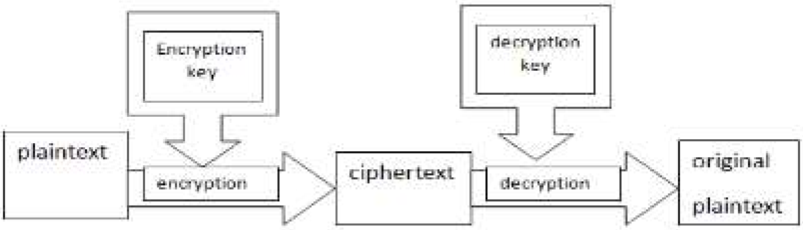

Fig. 2: Asymmetric cryptosystem

In the two-key system is also known as the public key system, one key encrypts the information and another, mathematically related key decrypts it. The computer sending an encrypted message uses a chosen private key that is never shared and so is known only to the sender. If a sending computer first encrypts the message with the intended receiver's public key and again with the sender's secret, private key, then the receiving computer may decrypt the message, first using its secret key and then the sender's public key. Using this public-key cryptographic method, the sender and receiver are able to authenticate one another as well as protect the secrecy of the message.

Common Terms Used in Cryptography

□ Plaintext: The original and understandable text. As an instance, 'Y' needs to transmit a "Computer" message to 'Z'. Here, "Computer" is the plain text or the original message.

□ Ciphertext: The text that cannot be understood by way of anybody or a gibberish text, example "A@$&J9."

□ Encryption: A process of changing clear text into unclear text. The manner of encipherment needs an encipherment algorithm and a key. Encipherment occurs on the sender side.

□ Decryption: A reverse method of encode. It is a manner of converting ciphertext into plaintext.

□ Key: A key is character, number, or a special character. It is used at the time of encipherment on the original text and at the time of decode on the ciphertext.

The basic concept of a cryptographic system is to cipher information or data in order to achieve confidentiality of the information in a way that an unauthorized person would be unable to derive its meaning. Two of the most common uses of cryptography would be using it to transmit data through an insecure channel, such as the internet, or ensuring that unauthorized people do not understand what they are looking at in a scenario in which they have accessed the information.

In cryptography, the concealed information is usually termed “plaintext”, and the process of disguising the plaintext is defined as “encryption”; the encrypted plaintext is known as “ciphertext”. This process is achieved by a number of rules known as “encryption algorithms”. Usually, the encryption process relies on an “encryption key”, which is then give to the encryption algorithm as input along with the information. Using a “decryption algorithm”, the receiving side can retrieve the information using the appropriate “decryption key”

Cryptography Goals

By using cryptography many goals can be achieved, These goals can be either all achieved at the same time in one application, or only one of them.
These goals are:

□ Confidentiality: it is the most important goal, that ensures that nobody can understand the received message except the one who has the decipher key.

□ Authentication: it is the process of proving the identity, that assures the communicating entity is the one that it claimed to be. This means that the user or the system can prove their own identities to other parties who don’t have
personal knowledge of their identities.

□ Data Integrity: its ensures that the received message has not been changed in any way from its original form. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user. This can be achieved by using hashing at both sides the sender and the recipient in order to create a unique message digest and compare it with the one that received.

□ Non-Repudiation: it is mechanism used to prove that the sender really sent this message, and the message was received by the specified party, so the recipient cannot claim that the message was not sent. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

□ Access Control: it is the process of preventing an unauthorized use of resources. This goal controls who can have access to the resources, If one can access, under which restrictions and conditions the access can be occurred, and what is the permission level of a given access.

Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems and not discussing sensitive procedures with outsiders.

Cryptographic Algorithms

Cryptosystems use a set of procedures known as cryptographic algorithms,
or ciphers, to encrypt and decrypt messages to secure communications among computer systems, devices and applications.

A cipher suite uses one algorithm for encryption, another algorithm for message authentication and another for key exchange. This process, embedded in protocols and written in software that runs on operating systems (OSes) and networked computer systems, involves:

- public and private key generation for data encryption/decryption
- digital signing and verification for message authentication
- key exchange.

SUMMARY

Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one that has the decipher key, and "data cannot be changed" means the original information would not be changed or modified. Cryptography plays a vital and critical role in achieving the primary aims of security goals, such as authentication, integrity, confidentiality, and no-repudiation. Cryptographic algorithms are developed in order to achieve these goals. Cryptography has the important purpose of providing reliable, strong, and robust network and data security. Cryptography will continue to emerge with IT and business plans in regard to protecting personal, financial, medical, and ecommerce data and providing a respectable level of privacy.

REFERENCES

1] https://en.wikipedia.org/wiki/Cryptography
2] https://searchsecurity.techtarget.com/definition/cryptography
3] https://www.kaspersky.com/resource-center/definitions/what-is-cryptography
4] https://www.ijrte.org/wp-content/uploads/papers/v8i2S3/B10690782S319.pdf
5] https://www.techopedia.com/definition/1773/decryption
6] https://www.tutorialspoint.com/cryptography/cryptography_tutorial.pdf