# A RESEARCH PAPER ON CRYPTOGRAPHY

Gurdeep Singh[1], Prateek Kumar[2], Nishant Taneja[3], Indu[4]

***Abstract: Data is any type of stored digital information. Security is about the protection of assets. Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, personal databases and websites. Cryptography is evergreen and developments. Cryptography protects users by providing functionality for the encryption of data and authentication of other users. Compression is the process of reducing the number of bits or bytes needed to represent a given set of data. It allows saving more data. Cryptography is a popular ways of sending vital information in a secret way. There are many cryptographic techniques available and among them AES is one of the most powerful techniques. The scenario of present day of information security system includes confidentiality, authenticity, integrity, non- repudiation. The security of communication is a crucial issue on World Wide Web. It is about confidentiality, integrity, authentication during access or editing of confidential internaldocuments.***

***Keywords :Data Encryption and decryption, Compression, Cryptography Concept, Security, Integrity.***

## I. INTRODUCTION

To secure the data, compression is used because it use less disk space (saves money), more data can be transfer via internet. It increase speed of data transfer from disk to memory. Security goals for data security are Confidential, Authentication, Integrity, and Non-repudiation. Data security delivers data protection across enterprise. Information security is a growing issue among IT organizations of all sizes. To tackle this growing concern, more and more IT firms are moving towards cryptography to protect their valuable information. In addition to above concerns over securing stored data, IT organizations are also facing challenges with everincreasing costs of storage required to make sure that there is enough storage capacity to meet the organization's current and future demands. Data compression is known for reducing storage and communication costs. It involves transforming data of a given format, called source message to data of a smaller sized format called code word. Data encryption is known for protecting information from eavesdropping. It transforms data of a given format, called plaintext, to another format, called cipher text, using an encryption key. Currently compression and encryption methods are done separately. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardnessassumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use andexport.

## II. CRYPTOGRAPHY

The art of cryptography is considered to be born along with the art of writing. As civilizations evolved, human beings got organized in tribes, groups, and kingdoms. This led to the emergence of ideas such as power, battles, supremacy, and politics. These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well. The roots of cryptography are found in Roman and Egyptiancivilizations.

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 ciphertext.

To hide any data two techniques are mainly used one is Cryptography other is Steganography. In this paper we use 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.

Basic Terminology of Cryptography

Computers are used by millions of people for many purposes. such as banking, shopping, military, student records, etc.. Privacy is a critical issue in many of these applications, how are we need to make sure that an unauthorized parties cannot read or modifymessages.

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.

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.
Computer security it's a generic term for a collection of tools designed to protect any data from hackers, theft, corruption, or natural disaster while allowing these data to be available to the users at the same time. The example of these tools is the antivirus program.

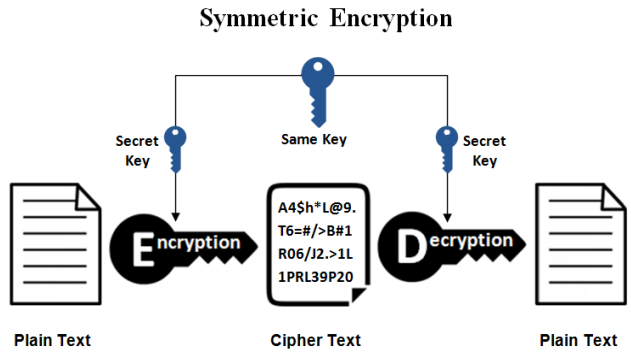
Network security refers to any activity designed to protect the usability, integrity, reliability, and safety of data during their transmission on a network, Network security deals with hardware and software. The activity can be one of the following anti-virus and anti-spyware, firewall, Intrusion prevention systems, and Virtual PrivateNetworks.
Internet Security is measures and procedures used to protect data during their transmission over a collection of interconnected networks, while information security is about how to prevent attacks, and to detect attacks on information-based systems.
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 theiridentities.
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 thatreceived.
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 thistransaction.
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 givenaccess.
Data Encryption
A data encryption is a random string of bits created explicitly for scrambling and unscrambling data. Data encryption is designed with algorithms intended to ensure that every key is unpredictable and unique.
Cryptography uses two types of keys: symmetric and asymmetric. Symmetric keys have been around the longest; they utilize a single key for both the encryption and decryption of the ciphertext. This type of key is called a secret key. Secret-key ciphers generally fall into one of two categories: stream ciphers or block ciphers. A block cipher applies a private key and algorithm to a block of data simultaneously, whereas a stream cipher applies the key and algorithm one bit at a time.
Most cryptographic processes use symmetric encryption to encrypt data transmissions but use asymmetric encryption to encrypt and exchange the secret key. Symmetric encryption, also known as private key encryption, uses the same private key for both encryption and decryption. The risk in this system is that if either party loses the key or the key is intercepted, the system is broken and messages cannot be exchanged securely.

Data Decryption
One of the foremost reasons for implementing an encryption-decryption system is privacy. As information travels over the World Wide Web, it becomes subject to access from unauthorized individuals or organizations. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (ciphertext). Decryption is the process of converting ciphertext back to plaintext.

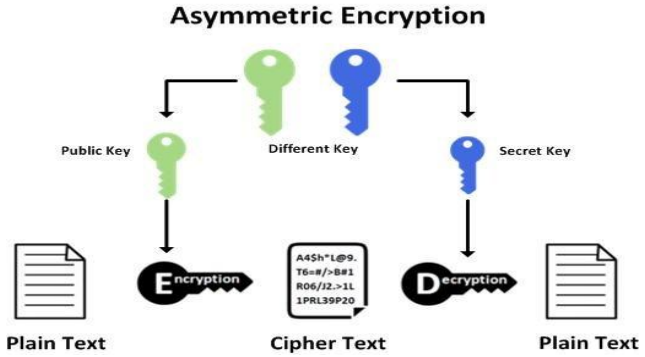
Symmetric Key Cryptography
In symmetric key cryptography is also known as private-key cryptography, a secret key may be held by one person or exchanged between the sender and the receiver of a message. If private key cryptography is used to send secret messages between two parties, both the sender and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




Asymmetric KeyCryptography

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 themessage.




COMPRESSION

Data compression offers an attractive approach for reducing communication costs by using available bandwidth effectively. Compression algorithms reduce the redundancy in data representation to decrease the storage required for that data. Over the last decade there has been an unprecedented explosion in the amount of digital data transmitted via the Internet, representing text, images, video, sound, computer programs etc

Data compression implies sending or storing a smaller number of bits. Compression is the reduction in size of data in order to save space or transmission time. Many methods are used for this purpose, in general these methods can be divided into two broad categories: Lossy and Lossless methods. Lossy Compression generally used for compress an images. In this original data is not identical to compressed data that means there is some loss e.g. Block Truncation Coding, Transform Coding, etc... Lossless Compression used for compress any textual data.

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 ormodified.

REFERENCES

[1] https://www.techopedia.com/definition/1773/decryption
[2] www.computerhope.com/jargon/d/decrypti.htm
[3] https://en.wikipedia.org/wiki/Cryptography
[4] https://www.techopedia.com/definition/25403/encryption-key
[5] http://searchsecurity.techtarget.com/definition/private-key
[6] https://www.tutorialspoint.com/cryptography/cryptography_tutorial.pdf