Cryptography: Encryption, Cipher And Security

Sreenivas.R[1], Dr. Uma Maheswari.B [2]

[1]Dept of Computer Application

[2]Asst.Prof.Dept of Computer Application

[1, 2]PSG College of Arts and Science Coimbatore, India.

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. In order to achieve this level of security, various algorithms and methods have been developed. Cryptography can be defined as techniques that cipher data, depending on specific algorithms that make the data unreadable to the human eye unless decrypted by algorithms that are predefined by the sender.*

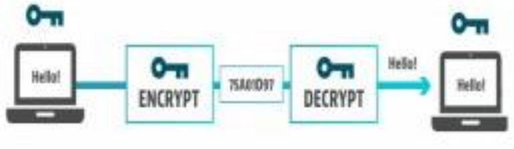
Keywords- Cryptography, Data encryption and decryption, Compression, Security, Cipher.

I. INTRODUCTION

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 hardness assumptions, making such algorithms hard to break in practice by any adversary. 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. 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. 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.

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 fuelled 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 Egyptian civilizations. 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 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.



A. 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 party cannot read or modify messages.

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.

B. 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:

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

2. *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.

3. *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.

4. *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.

5. *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.

III. DATA ENCRYPTION AND DECRYPTION

A. Data Encryption

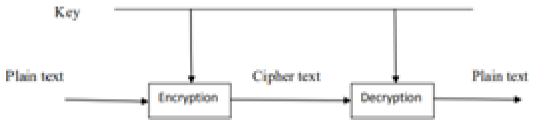
A data encryption is a random string of bits created explicitly for scrambling and unscrambling data. Data encryption is designed with algorithms intended to ensure that every key is unpredictable and unique. Cryptography uses two types of keys: symmetric and asymmetric. Symmetric keys have been around the longest; they utilize a single key for both the encryption and decryption of the cipher text. 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.

B. 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 (cipher text). Decryption is the process of converting cipher text back to plaintext.

C. 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.



Symmetric Cryptosystem

D. Asymmetric Key Cryptography

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.

IV. 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: Loss and Lossless methods. Loss 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.

V. SECURITY

A. Computer security

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.

B. Network security

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 Private Networks.

C. Internet Security

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.

VI. CIPHER

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.

A. Caesar Cipher

This is one of the oldest and earliest examples of cryptography, invented by Julius Caesar, the emperor of Rome, during the Gallic Wars. In this type of algorithm, the letters A Through We are encrypted by being represented with the letters that come three places ahead of each letter in the alphabet, while the remaining letters A, B, and C are represented by X, Y, and Z. This means that a "shift" of 3 is used, although by using any of the numbers between 1 and 25 we could obtain a similar effect on the encrypted text. Therefore, nowadays, a shift is often regarded as a Caesar Cipher. As the Caesar cipher is one of the simplest examples of cryptography, it is simple to break. In order for the cipher text to be decrypted, the letters that were shifted get shifted three letters back to their previous positions. Despite this weakness, it might have been strong enough in historical times when Julius Caesar used it during his wars. Although, as the shifted letter in the Caesar Cipher is always three, anyone trying to decrypt the cipher text has only to shift the letters to decrypt it

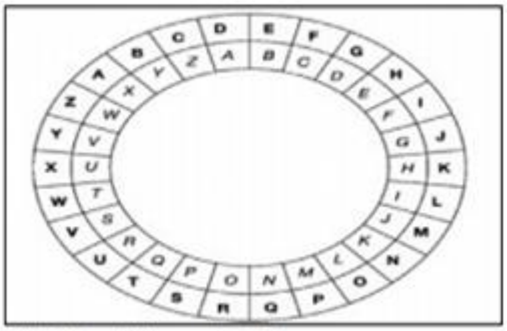
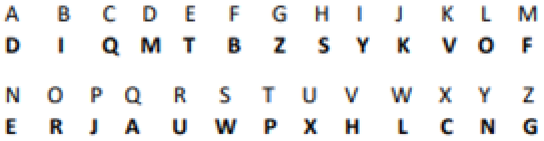

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

Fig. 2. Caesar Cipher encryption wheel

B. Simple Substitution Ciphers

Take the Simple Substitutions Cipher, also known as Monoalphabetic Cipher, as an example. In a Simple Substitution Cipher, we take the alphabet letters and place them in random order under the alphabet written correctly, as seen here:

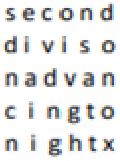


A	B	C	D	E	F	G	H	I	J	K	L	M
D	**I**	**Q**	**M**	**T**	**B**	**Z**	**S**	**Y**	**K**	**V**	**O**	**F**
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	**R**	**J**	**A**	**U**	**W**	**P**	**X**	**H**	**L**	**C**	**N**	**G**

In the encryption and decryption, the same key is used. The rule of encryption here is that “each letter gets replaced by the letter beneath it”, and the rule of decryption would be the opposite. For instance, the corresponding cipher text for the plaintext CAN is QDN

C. Transposition Ciphers

Other cipher families work by ordering the letters of the plaintext to transform it to cipher text using a key and particular rule. Transposition can be defined as the alteration of the letters in the plaintext through rules and a specific key. A columnar transposition cipher can be considered as one of the simplest types of transposition cipher and has two forms: the first is called “complete columnar transposition”, while the second is “incomplete columnar”. Regardless of which form is used, a rectangle shape is utilized to represent the written plaintext horizontally, and its width should correspond to the length of the key being used. There can be as many rows as necessary to write the message. When complete columnar transposition is used, the plaintext is written, and all empty columns are filled with null so that each column has the same length. For example:



second
diviso
nadvan
cingto
nightx

The cipher text is then derived from the columns depending on the key. In this example, if we used the key “321654”, the cipher text is going to be: cvdng eiaii sdncn donox nsatt oivgh However, when it comes to an incomplete columnar transposition cipher, the columns are not required to be completed, so the null characters are left out. This results in columns of different lengths, which can cause the cipher text to be more difficult to decipher without the key.

VII. CONCLUSION

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. 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.

I. REFERENCE

[1] B. Preneel, Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer, 2010.

[2] J. Katz and Y. Lindell, lntroduct:ion t:o Modern Cryptography, London: Taylor & Francis Group, LLC , 2008.

[3] S. J. Lincke and A. Hollan, "Network Security: Focus on Security, Skills, and Stability," in 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee, 2007.

[4] O. O. Khalifa, M. R. Islam, S. Khan and M. S. Shebani, "Communications cryptography," in RF and Microwave Conference, 2004. RFM 2004. Proceedings, Selangor, 2004.

[5] N. Jirwan, A. Singh and S. Vijay , "Review and Analysis of Cryptography Techniques," International Journal of Scientific & Engineering Research, vol. 3, no. 4, pp. 1-6, 2013 .

[6] S. Tayal, N. Gupta, P. Gupta, D. Goyal and M. Goyal, "A Review paper on Network Security and Cryptography," Advances in Computational Sciences and Technology , vol. 10, no. 5, pp. 763770, 2017.

[7] www.computerhope.com/jargon/d/decrypti.htm

[8] https://en.wikipedia.org/wiki/Cryptography

[9] https://www.techopedia.com/definition/25403/encryption-key

[10] http://searchsecurity.techtarget.com/definition/pr ivate-key

[11] https://www.tutorialspoint.com/cryptography/ryptography_tutorial.pdf