Volume 9, Issue 2
April 2020

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X



# A comprehensive review on cryptographic techniques

**Anuj Kumar Gupta**

*Professor & Head, Chandigarh Group of Colleges, Mohali, Punjab*

Email: anuj21@hotmail.com

## ABSTRACT

Cryptography enables two persons to talk or communicate over a channel full of insecurities. The medium or the channel through which the information is being sent can be either a computer network or a telephone line. This is done in such a way that the other person cannot understand the communication between the two persons. In other words the information remains intact. This is the basic definition or the objective of cryptography. The "plaintext" is called the information which is to be sent by the sender. This information can contain any arbitrary data such as characters, numeric, alphabets or anything of that sorts. Now the sender has some predetermined key through which he can encrypt the data. The encrypted data is called the ciphertext. This ciphertext is sent by the sender over the channel to the receiver. Now any third person eavesdropping the information being sent from sender to receiver from the channel would not be able to understand the "plaintext" because it is already being encrypted by the sender. Only the receiver who has the access to the predetermined key can decrypt the data from ciphertext to "plaintext" and can reconstruct it.

Keywords: *Cryptography, Ciphertext, Encryption, Decryption.*

## 1. INTRODUCTION

Cryptography is the heart of security. If we need to maintain privacy, we need to encrypt our message (convert original message into the coded form) at the sender side and decrypt (convert coded form into original message) at the receiver side [1]. In other words cryptography is a science of writing secret code.

Meaning of Cryptography:

**kryptos (hidden) + graphein (to write) = secret writing**

According to Mathematician cryptography is defined as the study of mathematical techniques related to aspects of information security. Cryptography hides or protects the information from the persons who are unauthorized to its access as well as authenticates and do the correct verification of the message to the receiver. It form the basis to many security communication concern.

## 2. NEED OF CRYPTOGRAPHY

Cryptography provides Security to the data which is send over the transmission path. Nowadays there is almost no work possible without the use of computers and internet especially in the consumer field. So it is very important to consider the security of the information which is being sent through the internet without compromising with its speed and accuracy. Here cryptography comes into the picture [2]. The sensitive information contents that we want to secure from the third party includes.

1. Credit card Information
2. Bank account information
3. Social security Numbers
4. Private correspondence
5. Personal details
6. Sensitive company information

A significant portion of organizational budget is spent on managing information.

There are many types of information

- Both stored and processed within a computer
- And transferred between computers

There is a need to systematically define the requirements for security and identify means of satisfying these we need cryptography. Figure 1 shows the components of Cryptography. Original Message called plain text, when message is converted into coded form after applying Encryption method that called Cipher Text. And on the receiver side we can get original message by applying Decryption method [3].

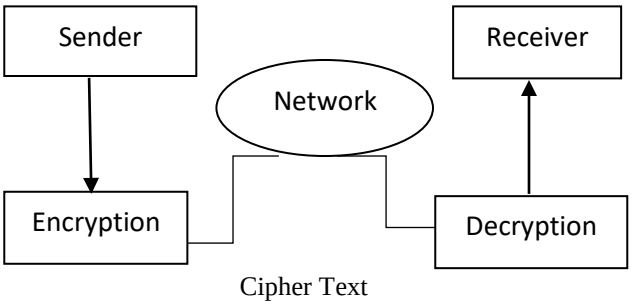



Figure 1. Components of Cryptography

Volume 9, Issue 2
April 2020

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X



## 3. ENCRYPTION AND DECRYPTION

The encryption and decryption algorithm are public, anyone can access them. The keys are secret, they need to be protected. Figure 2 describes the process of encryption and decryption. Plaintext is converted to ciphertext by applying Encryption Key by the sender and ciphertext is decrypted by applying Decryption Key to get the Plaintext by the receiver [7].

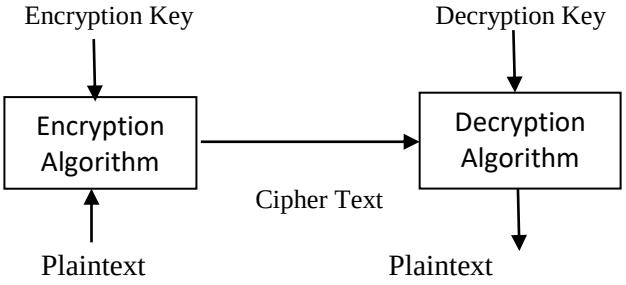



Figure 2. Encryption and Decryption Process

## 4. ENCRYPTION SYSTEMS

In the past times when no digital data was used, the cryptography was mainly used for the military purposes [4]. The data which is being coded is dependent on the machines or the computers. This is because the encrypted data which is based on the humans can be very easily cracked. Thus the science of cryptography is the main base for computer encryption.

There are main two categories of computer encryption which are as follows:

**1. Symmetric or conventional Method**: - In this method same key (the secret key) is used to encrypt or decrypt a message. The sender uses this key (secret key) to encrypt and decrypt a message and recover plaintext because a single key is used for both functions, so it is called Symmetric encryption [5].

Stream clippers and block clippers are two categories described under cryptography which are explained as follows.

1. The clippers which work on a single bit or a word at a time are the stream clippers. The same key is used to encrypt the plain text to the clipper text which is different.

2. A block clipper is so called because the scheme encrypts one block of data at a time using same key on each block. Same plain text block will always encrypts to same clipper text using same key.

**A. Types of Encryption/Decryption symmetric methods**

**Conventional methods**
There are two categories of conventional methods where the encryption and decryption keys are different.

1. Character-Level Encryption
2. Bit-Level Encryption

**Types of Character-Level Encryption:-**

a) Substitution
b) Transposition

a) **Substitution**: Substitutes the position of each character by a given key. Figure 3 shows the technique of this method.

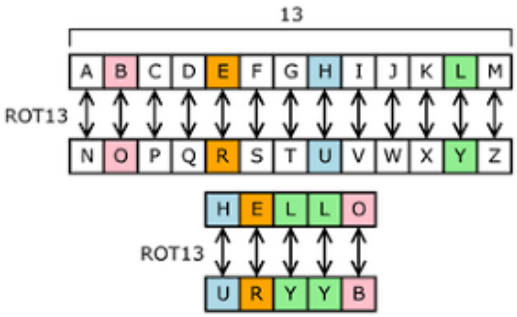



Figure 3. Substitution Cipher Method

b) **Transposition**: - An even more secure method is transposition encryption in which the character retain their plaintext form but change their positions to create the cipher text according to a given key. Figure 4 shows the method of transposition process [6].

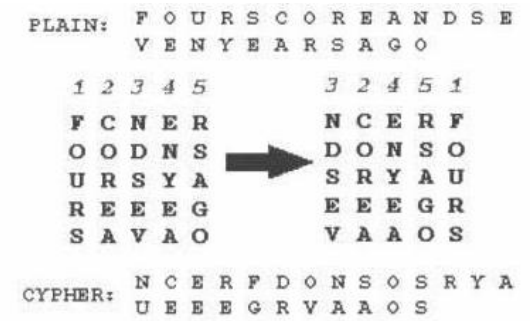



Figure 4: Transposition Cipher Method

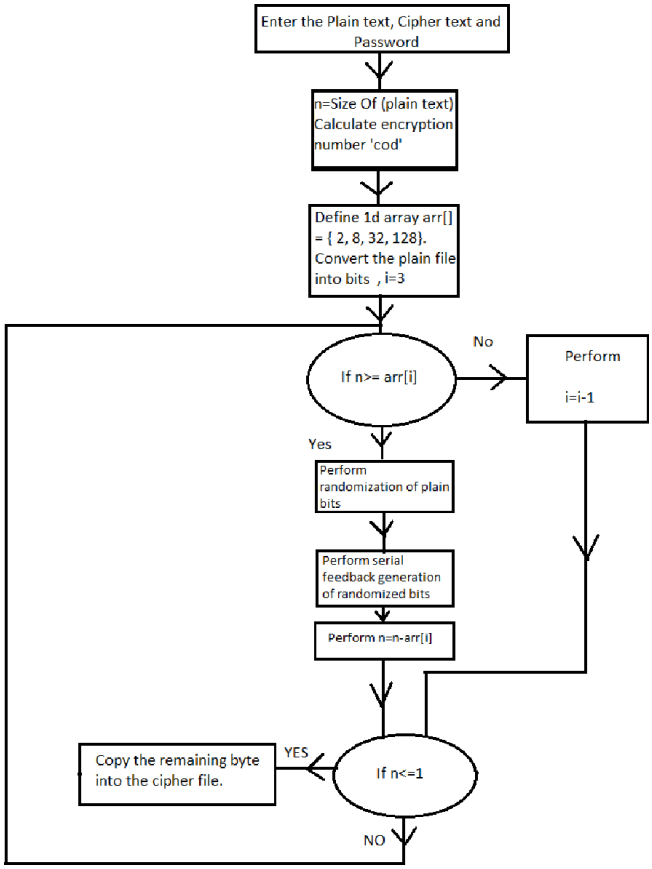
**Bit level encryption: -** In bit level encryption techniques, the data which is to be encrypted is first converted into blocks of bits and then it is further encoded or decoded accordingly, as shown in figure 5.

Volume 9, Issue 2
April 2020

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X






Figute 5. Bit Level Encryption

**Types of Bit level encryption: -**

Data as text, graphics, audio, or video are divided into blocks of bits first and then altered by any of the following techniques:

- encoding/decoding
- permutation
- exclusive OR
- rotation
- others

a) **Encoding/Decoding**:- The decoder converts an input of n bits into the output of $2^n$ bits and encoder works reverse of decoder in this method.
b) **Permutation**:-Permutation is in fact transposition at the bit level. In straight permutation the number of bits in the input and output are preserved: only positions are changed.
c) **Substitution**: - Substitution of n bits by n bits can be achieved using a combination of P-boxes, Encoders & decoders.
d) **Product**: - P-boxes & S-boxes combination called product. A product unit is made of several stages of P-boxes and S- boxes.
e) **Exclusive OR:**-In this method Exclusive–OR operation is done on the input bits.
f) **Rotation:**-Rotate one bit to left at one time, then next and after that send this Cipher text on transmission path, on the receiver side apply the reverse process to recover original text.

**Symmetric Challenges: -**

Main challenges are:-

1. Agreeing on the key while maintaining secret.
2. Trusting the phone system or same transmission medium.
3. The intercepts can read, modify or forge all messages.

**2. Public Key Encryption**

There are two types of keys used in public key encryption which are private key and public key. Both the keys have their own specific functions. Only your system has the access to the private key whereas the public key is visible to all the systems and computers with whom the communication is to be done. When the encrypted data is received by a computer, then it decodes the information with the help of its own private key and public key sent by the sender computer. Encryption is done very easily with the help of public key encryption. The data is encrypted with the help of symmetric key. Then this is encrypted again with the public key which is sent by the computer at the receiving end. Now when this encrypted data is received at its destination, then the receiving computer decodes the symmetric key with the help of its private key, see figure 6. Then the original information or the document is decoded with the help of symmetric key [9].

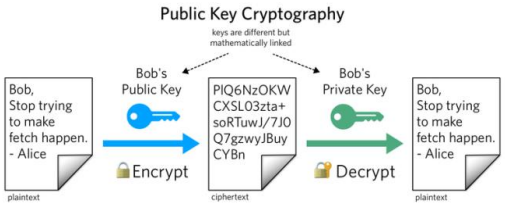


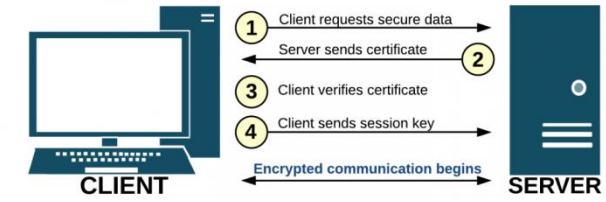

Figure 6. Public Key Cryptography

Digital certificates are used to implement the public key encryption as it needs different approach since encryption nowadays is done on large scale. The bits of information in the digital certificate is highly dependent on the trusted source called certificate authority. It is the middleman for both the computers in between which the information is being carried. It ensures that that the public key of both the computers are exchanged to each other.

**3. SSL**

In order to exchange the information which is sensitive in nature, SSL (Secure Socket Layer) is used which is the protocol for security. SSL is used by the web servers and

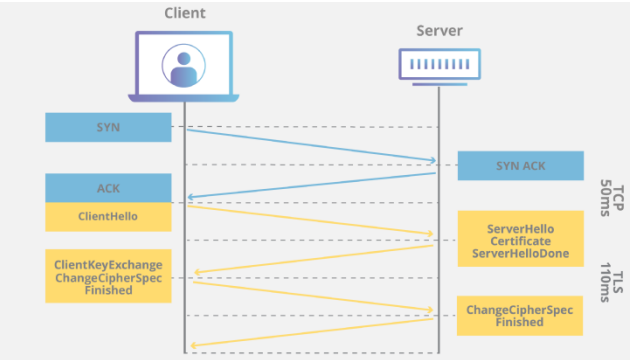
internet browsers. SSL is the part of TLS (Transport Layer Protocol) which is the overall security protocol.




**Advantages:**

There are many advantages of SSL and TLS which includes addition of latest techniques, switching of encryption algorithms is made possible and most importantly it has no link with the application layer.

TLS helps in letting us know that the secure protocol is being used in the browser if there is 's'after http. So whenever any sensitive information is to be entered while using internet, it is very important to look for the minor details which guides in letting know whether the protocol being used is secured or not. There is a window at the bottom of the browser. If there is some padlock shown there then the data used is fully encrypted [10].




**4. Cryptography advantages & disadvantages**

Both public key and symmetric key are used by the systems since public key encryption alone requires loads of computing. Whenever the information is to be communicated between two computers and to secure or encrypt that information, a symmetric key is created by the sender computer. This symmetric key is passed to the receiver computer with the help of public key encryption. This symmetric key helps in the secure communication in between two computers and is discarded when the information is carried on securely. The process is repeated for the additional sessions [8].

**Advantages:**

The advantages include construction of cryptographic mechanisms, smaller size and higher throughput of the data.

The disadvantages include large sizes of the keys used for encryption and decryption.

The advantages include efficient mechanism of digital signature, key life time and verification key is smaller.The disadvantages include large sizes of the keys used for encryption and decryption.

## 5. FUTURE TRENDS

Security is must when we send data from one Machine to another. It is today's need to transmit data over a long distance without any loss of data. So Scientists are going to invent new methods to change data into coded form so that any unauthorized person can't read or alter information. In this way Security is must in transmission and Cryptography is the heart of security.

## 6. CONCLUSIONS

Cryptography works great to maintain the privacy of data over the transmission path.So that we can get our original information without any loss on the destination point. Privacy of data is also depends which method of cryptography is used by us to change the data into coded form.

## REFERENCES

[1]. Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha "Performance Evaluation of Symmetric Cryptographic Algorithms", International Journal of Electronics and Communication Technology Vol 2 Issue 3, Sep 2011.

[2]. Pratap Chandra Mandal "Superiority of Blowfish Algorithm", International Journal of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, Sep 2012

[3]. Monika Agrawal, Pradeep Mishra", A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol.4 May 2012

[4]. C. Gu and Y. Zhu, "New efficient searchable encryption schemes from bilinear pairings", International Journal of Network Security, 10, 25-31, 2010.

[5]. M. Hassouna, N. Mohamed, B. Barry, and E. Bashier, "An end-to-end secure mail system based on certifticateless cryptography in the standard security model", International Journal of Computer Science Issues, 10, 264-272, 2013.

[6]. S. Swathi, P. Lahari and B. Thomas," Encryption Algorithms: A Survey", International Journal of Advanced Research in Computer Science & Technology (IJARCST), Volume 4, Issue 2, 2016.

[7]. G. Yadav and A. Majare," A Comparative Study of Performance Analysis of Various Encryption Algorithms", International Conference on Emanations in Modern Technology and Engineering (ICEMTE), Volume: 5 Issue: 3, 2017.

[8]. M. Pandey and D. Dubey, "Survey Paper: Cryptography The art of hiding Information", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 12, 2013.

[9]. S. Almuhammadi and A. Al-Shaaby, "A Survey on Recent Approaches Combining Cryptography and Steganography", Computer Science & Information Technology (CS & IT), 2017.

[10]. Rajput A.S., Mishra N., and Sharma S.,-Towards the growth of image Encryption and Authentication Schemes‖, (ICACCI), 2013.

## AUTHOR PROFILE

**Dr. Anuj Kumar Gupta** is working as Professor and Head at Chandigarh Group of Colleges. He has completed his Phd in Computer Science & Engineering from IKG Punjab Technical University. He has a vast teaching and research experience of above 18 years. His area of research is Wireless Networks & Security. He has guided 20+ MTech thesis and 6 PhD thesis. He has published over 80 research papers in various National & International Journals and Conferences.