ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
*Vol. 2, Issue 6, June 2013*

# ENCRYPTION AND DECRYPTION USING ONE PAD TIME ALGORITHM IN MAC LAYER

ShachiSharma[1], VintiGupta[2]

P.G. Student, Department of Computer Engineering,Jayoti Vidyapeeth University Women's, Jaipur, Rajasthan[1]

Assistant Professor, Department of Computer Engineering,Jayoti Vidyapeeth University Women's, Jaipur, Rajasthan[2]

**Abstract**:This paper provides standard instructions on how to protect messages, text, audio, video with one-time pad encryption.The encryption is performed with nothing more than a pencil and paper, but provides absolute message security. If properly applied, it is mathematically impossible for any eavesdropper to decrypt or break the message without the proper key. Although the Internet can be used to provide high connectivity between two parties, it does not always provide strong protection for private communications. Here we describe a strong cryptographic solution to this problem using one-time pads.

**Keywords**: cryptography, one-time pad, encryption, Decryption.

## I. INTRODUCTION

*Encryption :*Encryption is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text . this is usually done with the use of an encryption key, which specifies how the message is to be encoded. encryption is the most effective way to achieve data security. to read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text ; encrypted data is referred to as cipher text. Show Fig (1)

Plain Text
Encryption
Cipher text

Fig 1 : Encryption process

To encrypt, convert the message into digits and subtract (without borrowing) the one-time pad from the text digits. Skip the first group of the one-time pad during the encryption process and use it as key indicator at the beginning of the ciphertext.

*Decryption :*Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords. The process of decoding data that has been encrypted into a secret format. Decryption requires a secret key or password. Decryption is the reverse process of encryption. While encryption is coding thedata into a secret format so that others cannot read or access it, decryption is decoding the data back to the original format .Showing fig 2

Cipher text
Decryption
Plain Text

.

Fig 2: Decryption process

To decrypt , verify whether the first group of the ciphertext (key indicator) is identical to the first group on your one-time pad. Write the one-time pad underneath the ciphertext digits and add both together (without carry). Convert the resulting digits with the conversion table back into readable text.

*Media Access Control Layer :* The Media Access Control (MAC) data communication Networks protocol sub-layer, also known as the Medium Access Control, is a sub-layer of the data link layer specified in the seven-layer OSI model. The medium access layer was made necessary by systems that share a common communications medium. Typically these are local area networks.In LAN nodes uses the same communication channel for transmission. The MAC sub-layer has two primary
responsibilities: Data encapsulation, including frame assembly before transmission, and frame parsing/error detection during and after reception. Media access control, including initiation of frame transmission and recovery from transmission failure.

*One Time Pad Algorithm* :One-time pad encryption we need a key, called one-time pad. A one-time pad can be a single sheet, a booklet or a strip or roll of paper tape that contains series of truly random digits. A one-time pad set consists of two identical one-time pads, one pad called OUT and one called IN. To establish one-way communications,you only need one OUT pad for the sender and one IN pad for the receiver. To communicate in both directions, you need two different one-time pad sets: person A has an OUT pad of which person B has the IN copy, and person B has another OUT pad of which person A has the IN copy. Never use a single pad to communicate in both directions to avoid the risk of simultaneous use of the same pad sheet! The use of multiple IN copies of a pad, to enable more than one person to receive a message, is possible but not advisable. Multiple copies pose additional security risks and should only be used in a strictly controlled environment. Never use multiple OUT copies of a pad, as this will inevitable result in simultaneous use of the same pad and the risk of non destroyed copies of a pad.One-time pad encryption is only possible if both sender and receiver are in possession of the same key. Therefore, both parties must exchange their keys beforehand. This means that the secure communications are expected and planned within a specific period. Enough key material must be available for all required communications until a new exchange of keys is possible. Depending on the situation, a large volume of keys could be required for a short time period, or little key material could be sufficient for a very long period, up to several years.

*Encryption And Decryption Using One Time Pad Algorithm :*The one-time pad is a long sequence of random letters. These letters are combined with the plaintext message to produce the cipher text. To decipher the message, a person must have a copy of the one-time pad to reverse the process. A one time pad should be used only once and then destroyed . To encipher a message, you take the first letter in the plaintext message and add it to the first random letter from the one-time pad. For example, suppose you are enciphering the letter S (the 19th letter of the alphabet) and the one-time pad gives you C (3rd letter of the alphabet). You add the two letters and subtract 1. When you add S and C and subtract 1, you get 21 which is U. Each letter is enciphered in this method, with the alphabet wrapping around to the beginning if the addition results in a number beyond 26 (Z).To decipher a message, you take the first letter of the cipher text and subtract the first random letter from the one-time pad. If the number is negative you wrap around to the end of the alphabet.

*Example:*
plaintext : SECRETMESSAGE
one-time pad: CIJTHUUHMLFRU
ciphertext : UMLKLNGLEDFXY

## II. METHODOLOGY/ PLANNING OF WORK

Sender and receiver are in a safe environment, free from risk of surveillance, intrusion of the privacy or prosecution, they can send their encrypted communications by any means, even insecure. It does not matter if someone intercepts the encrypted message.

The message is unbreakable anyway. Unfortunately, this ideal world hardly exists. Since it is mathematically impossible to break a one-time pad encrypted message by cryptanalysis, any eavesdropper will try to get his hands on either the original readable message or the one-time pad key, used to encrypt that message . In the real world, the eavesdropper will attempt to retrieve the identity and location of sender or receiver.

Identification of the involved persons is the first step in reading their communications. The mere identification of a person who sends or receives encrypted communications, even unintelligible, might have serious consequences under an oppressive regime. Once identified,the eavesdropper can start surveillance and use technical means to retrieve information from that person’s computer or perform a surreptitious search of his house to copy one-time pads that will be used in the future. The person might never know his security has been breached and his messages are read.

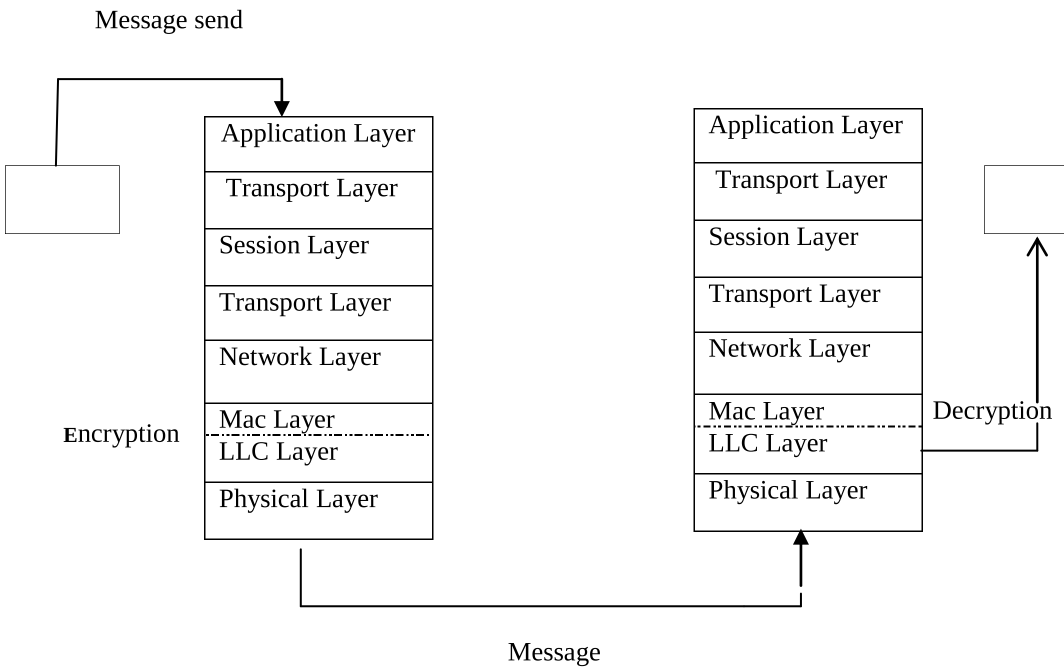

Fig 3 : Encryption and decryption process between client and server

## III. CONCLUSION

This algorithm has a lot of scope to enhance the security by using combining the different approaches. We have proposed a new methodology through which one time pads can be practically used for secure communication between client and server.

## ACKNOWLEDGMENTS

The Author would like to thank Mr. R.K Sharma. Department of CSE (Agra Engineering College ,Agra ) for his valuable support and would also like to thank Ms. Anuradha (H.O.D, Department of CSE) and Ms. Vinti Gupta for contributing material on Encryption And Decryption Using One Pad Time Algorithm.

## REFERENCES

[1] Douglas R, Stinson *" CRYPTOGRPHY Theory and Practice "* Second Edition.

[2] Charlie Kaufmanst al. *" Network Security "PRIVATE Communication in a PUBLIC World.* ,Prentice Hall of India PrivateLimited. 2008.

[3] Dirk Rijmenants, *"Cipher machines and cryptology, the one- time pad"* "http://users.telenet.be/d.rijmenants/en/onetimepad.htm"

[4] Neal R. Wagner *"The Laws of Cryptography: Perfect Cryptography: The One-Time Pad "*

[5] Ritter, Terry 2010. The Efficient Generation of Cryptographic Confusion Sequences. Cryptologia "15: 81-139

[6] *Modified One Time Pad Data Security Scheme: Random Key Generation Approach* " International Journal of Computer and Security Volume issue 2 March/April 2009 Malaysia (Published ) by Sharad Patil, Dr. Ajay Kumar:

[7] Michael E.Gruen, *"A secure low-power approach for providing mobile encryption"*, Proceedings of the Eleventh annual CCSC northeastern conference, 2006

[8] On wutalobi Anthony-Claret Department of Computer Science University of Wollongong "Using Encryption Technique