International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 02, February 2017
www.ijates.com
ijates
ISSN 2348 - 7550

DESIGN AND IMPLEMENTATION OF TWO LAYERS BASED UNIFORM ENCRYPTION DECRYPTION ALGORITHM (TLBUED)

Er. Suraj Arya

Research Scholar P.hd(CSE),Baba Mastnath University, Rohtak, Haryana,(INDIA)

ABSTRACT

Most of the task in the current age depend on computers and can execute through internet so information security is the major challenge for the programmers, information sender and receiver. Every second many new hacking methods came into existence to break the information security so new invention and updation always required in the field of cryptography. This paper presents a technique which has a new concept of uniformity in encrypted message. Two layers perform the encryption and decryption process in through two layers with the help of symbol table. Second feature of this algorithm is uniformity it means that after encryption an encrypted message will use same symbols to represent every character. Thus by doing this intruder cannot differentiate or detect the message. In this technique first layer take Input message and convert character by character as per symbol table. In second layer first level conversion use as input and provide the special character according to input which makes the message uniform. To perform the uniformity typical symbols are used in the technique.

Keywords: TLBUED

I INTRODUCTION

Cryptography describes a process of encrypting information so that its meaning is unknown to those who do not know how to decrypt the information. It is impossible to overemphasize the importance of cryptography, both in the past and present. Without cryptography in computing it would be impossible to perform tasks. Secure log in, credit cards, remotely log into servers can not be possible without security techniques [8],[1],[2]. A cryptographic algorithm is a step by step sequence of mathematical calculations used to encrypt and decrypt information. There are currently three different types of cryptographic algorithms [8],[1],[2].

- Hashing algorithms,
- Symmetric-key algorithms
- Asymmetric key algorithms

II HASHING ALGORITHMS

A hash is a mathematical algorithm designed to perform one-way encryption. one-way means that once the information has been encrypted there is no way to retrieve the original information from the hashed form. Hashing is commonly used in password files and for ensuring the integrity of data. As an example, a hash may be created for an email message in the form of a Message Authentication Code (MAC) [8],[1],[2]. When the message is received the receiver would also generate a hash from the message. If the recipient's hash matches the code which accompanied the message the receiver knows the message is authentic and has not been tampered with during transmission[8],[3],[4].

1. **Symmetric Encryption Algorithms (Private Key Encryption)**

- Symmetric encryption is one of the most basic forms of cryptography and is based on the premise that both the sending and receiving parties are in possession of the key used to encrypt the data[5],[8],[6].
- Symmetric key encryption is performed using two methods
- Block cipher
- Stream cipher.

  As the names suggest, block ciphers encrypt data in sections of bits whereas a stream cipher encrypts data one bit at a time until the entire message is encrypted[7],[8],[6]..

III ASYMMETRIC ALGORITHMS (PUBLIC KEY ENCRYPTION)

Asymmetric Algorithm is based on the concept of using a pair of keys, one private and one public. The private key is held by the host or application which is to receive the encrypted data. The corresponding public key is made available to anyone who wishes to encrypt data such that it can be decrypted by the holder of the private key[1],[8],[4].

RSA (Ron Rivest, Adi Shamir and Leonard Adleman)**:**RSA is named after the last names of its three inventors (and is used for both encryption and digital signatures. The algorithm works by multiplying two very large prime numbers. Through further mathematical calculations public and private keys are derived[3],[8],[7].

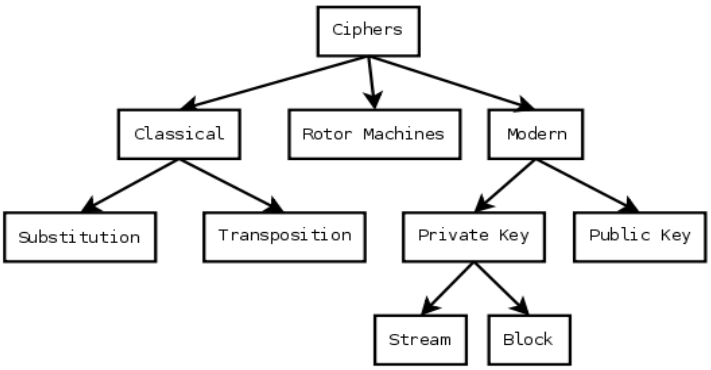

Figure 1: Classification of Encryption Type (source: http://en.wikipedia.org/wiki/Cipher).

International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 02, February 2017
www.ijates.com
ijates
ISSN 2348 - 7550

IV TWO LAYERS BASED UNIFORM ENCRYPTION DECRYPTION TECHNIQUE (TLBUEDT)

This technique is based on two layers approach and uniformity. Two layers perform the encryption and decryption process in through two layers with the help of symbol table. Second feature of this method is uniformity it means that after encryption an encrypted message will use same symbols to represent every character. Thus by doing this intruder cannot differentiate or detect the message. In this technique first layer take Input message and convert character by character as per symbol table. In second layer first level conversion use as input and provide the special character according to input which makes the message uniform. To perform the uniformity typical symbols are used in the technique.

Advantages

- Two layer approaches makes the technique Robust.
- Uniformity makes it more secure as message cannot be break or detected between sender and receiver.

Example

Step 1

The Quick Brown Fox Jumps Over The Lazy Dog please call at

Step 2

3216547890 ta llac esaelp goD yzaL ehT revO spmuJ xoF

Step 3

+*yyyJ%22kk1bbbb=.IIIIzz.PPPPPPzzVVV.88Wzz88PPPQQQQ.CCfff
□55333zzÿ.88hh©.EEEE88RRR{.WQQQQCCCsssÆ.nnnnfff‰.SHHH
HHfffEEEE999.LLVVVooosssXx.88hh©

Step 4

$##########@$$$$$$$$$$##########TTTTTTTTTTTTTTT#######TTTTTTTT
TTTTTTTT##########TTTTTTTTTTTTTTTTTTTTTTT###########@@@@@@@@@@@
@@@@@@##########TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT#####
##########@@@@@@@@$$$$$$$$$$$$$#####TTTTTTT##########################T
TTTTTTTTTTTTTTTTTTTT@$$$##########################$$$$$$$$$$$$$@$##########
####@$$$$$$$$$$##########TTTTTTTTTTTTTTT#######TTTTTTTTTTTTTTTT##########
##########TTTTTTTTTTTTTTTTTTTTTTT###########@@@@@@@@@@@@@@@@@@@##########
##########TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT##########
@@@@@@@@$$$$$$$$$$$$$#####TTTTTTT##########################TTTTTTTTTTTTTTTTTT
TTT@$$$##########################$$$$$$$$$$$$$@TTTT##########################
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$TTTTTTT$$$$$$$##########TTTTTTTTTTTTTTTTTTTTT

Step 5

+*yyyJ%22kk1bbbb=.IIIIzz.PPP PPPzzVVV.88Wzz88PPPQQQQ. CCfff□55333zzÿ.88hh©.EEEE8 8RRR{.WQQQQCCCsssÆ.nnnn fff‰.SHHHHHfffEEEE999.LLV VVoosssXx.88hh©	###############TTTTTTTTTTTTTTTTTTTTTT@@@@@ @@@@@@@@@@TTTTTTTTTTTTTTT#########@@@ @@@@@@@@@@@@@@@@@@TTTTTTTTTTTTTTT TTTTT######TTTTTTTTTTTTTT###################### ##TTTTT###############################@@@@@@@ @@@@@#######$$$$$$$$$$$$$$##################### ###TTTTTTTTTTTTTTTTTTTTTTT@@@@@@@@###### #TTTTTTTTTTTTTTTTTTTTTTT@@@@@@$$$$$$$$$$$ $########################@$$$$$$$$$$############### #########TTTTTTTTTTTTTTT#######TTTTTTTTTTTTTT TT########################TTTTTTTTTTTTTTTTTTTT TTT############@@@@@@@@@@@@@@@@@##### ###################TTTTTTTTTTTTTTTTTTTTTTTTTTT TTTTTTTTTTTTTTTTT###########################@@ @@@@@@$$$$$$$$$$$$#####TTTTTTT############### ###################TTTTTTTTTTTTTTTTTTTTT@$$$## ##############################$$$$$$$$$$$$$@TTTT## ####################################$$$$$$$$$$$$$$$$ $$$$$$$$$$$$$TTTTTTT$$$$$$$####################### #TTTTTTTTTTTTTTTTTTTTTTT############@@@@@ @@@@@@@@@@@@

Figure 2: Encrypted Message of TLBUEDT

V IMPLEMENTATION OF ALGORITHM

Figure 3 shows the implementation of first phase of uniform based Encryption Decryption Technique it based on two symbol tables first Symbol table, consists symbols according of A to Z, a to z and 0 to 9 and table has a special symbol for each character between A to Z, a to z and 0 to 9. Second table has uniform symbols corresponding to a character. As the plain text entered in the technique at first it will reverse it as shown in figure it shows the entered plain text in the reverse order. In the second step technique choose the symbols form table and perform the transposition operation on it is also shown in figure. The second phase encryption of two layers Based Uniform

Encryption Decryption Technique. In that phase as the transposition operation performed the particular character set for corresponding to a plain text character.

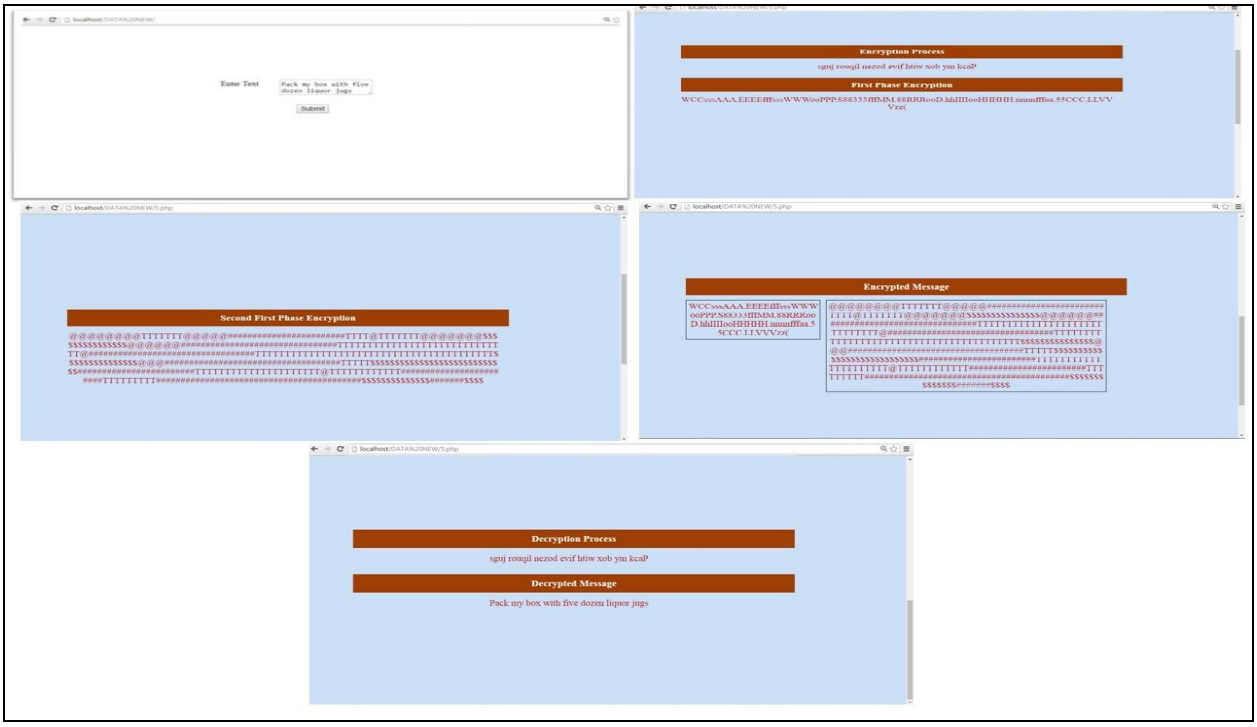

Figure 3: Implementation of TLBUEDT Algorithm Using PHP

Then second phase of the two layers Based Uniform Encryption Decryption Technique will execute in which almost uniform symbols select to the input of first phase. Thus the output of the first phase can work as input in the second phase. Thus these uniform symbols will assign to the output of the first phase and the encryption process will completed and the message is ready for receiver end. Figure show the encrypted message of two layers Based Uniform Encryption Decryption Technique. The main feature of this method is uniformity it means that after encryption an encrypted message will use same symbols to represent every character. Thus by doing this intruder cannot differentiate or detect the message. In this technique first layer take Input message and convert character by character as per symbol table. In second layer, first level conversion use as input and provide the special character according to input which makes the message uniform. To perform the uniformity typical uniform symbols are used in the technique. The decrypted message of two layers Based Uniform Encryption Decryption Technique. The decryption can be performed with the help of uniform symbols in reverse order. As it is very clear that this technique uses almost same symbols to represent every character. Thus during decryption receiver uses the table which contains the uniform symbols the matches these symbols with the decrypted text and find out the special characters according to these uniform symbols and on this basis receiver can decrypted the message in to two layers or phases

in first phase receiver read the uniform table for decrypted message and in second phase find out the plain text according to the special characters.

VI CONCLUSION

Two layers based encryption decryption Technique executes encryption process in two steps. These steps further divided in two layers. First layer take Input message and convert character by character as per symbol table. The second layer is used for uniformity purpose for the encryption of messages and uses first level conversion as input and provides the special character according to input which makes the encrypted message uniform.

VII FUTURE SCOPE

The scope of uniformity is very vast as it is also possible to generate the complete uniform encrypted message it means encrypted message will based on a single symbol and that is used to represent all the character of plain text. This uniformity makes the intruder uncomfortable as encrypted message will display same characters for encrypted message. Thus there is no possibility to read that message. It is also not really possible to relate these uniform characters with the actual characters or plain text.

REFERENCES

[1] Stallings, W [2005].Cryptography and Network Security Principles and Practice, 4th Edition, Pearson Education Prentice Hall, ISBN 10: 0-13-609704-9 ISBN 13: 978-0-13-609704-4

[2] Bose,Ranjan[2008].Information Theory, Coding and Cryptography, Tata McGraw-Hill Education, ISBN 0070669015, 9780070669017

[3] Gitanjali, J.; Jeyanthi, N.; Ranichandra, C.; Pounambal M(2014) ASCII based cryptography using unique id, matrix multiplication and palindrome number,in Networks, Computers and Communications, The 2014 International Symposium on,. IEEE 2014.

[4] Mittal Varun., and Murli Agawarl Piyush(2011). An Encryption and Decryption Algorithm for Messages Transmitted by Phonetic Alphabets; International Conference of Soft Computing
and Pattern Recognition. 978-1-4577-1196-1/11/$26.00_c 2011 IEEE

[5] http://www.queen.clara.net/pgp/art6.html

[6] https://www.techopedia.com/definition/1770/cryptography

[7] https://www.cigital.com/knowledge-database/cryptography/

[8] http://www.techotopia.com/index.php/Cryptography_Basics