International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 02 , February 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

DESIGN AND IMPLEMENTATION OF SHELTERED TRANSPORTATION CRYPTOGRAPHY ALGORITHM

Er. Suraj Arya

Research Scholar Ph.D(CSE),Baba Mastnath University, Rohtak, Haryana,(INDIA)

ABSTRACT

Encryption is a process in which plain text takes as input and cliper text as output. It is based on some techniques and methods which are adopt for encryption. Thus after encryption information is not in the normal form and it cannot be understand or read by any unauthorized users only authorized can read that text. The output of the encryption process use as input for decryption. Thus decryption is a process in which is used to read the encrypted message and provide the output as plain text. Thus it is counter approach of encryption process. This paper presents a new cryptography algorithm which is based in transposition concept. It also presents the implementation of encryption decryption process using PHP language.

Keywords: ASCII, Transposition, Cipher & Plain Text

I INTRODUCTION

Cryptography involves creating written or generated codes that allows information to be kept secret. A given algorithm will always transform the same plaintext into the same cipher text [5][6][7]. Cryptography converts data into a format that is indecipherable for an unauthorized user, allowing it to be transmitted without anyone decoding it back into a readable format, thus compromising the data[5][6][7]. The information cannot be read without a key to decrypt it. The information maintains its reliability during transfer and while being stored. Cryptography also aids in non-repudiation. This means that neither the sender nor the receiver of the information may claim they did not send or receive it[5][6][7].

II SYMMETRIC CRYPTOGRAPHY

Symmetric cryptography divides the plaintext in the form of blocks which are of rigid length and transforms each block according to a particular method to produce a cipher text block. Such type of algorithms uses the same key for decryption also [5].

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

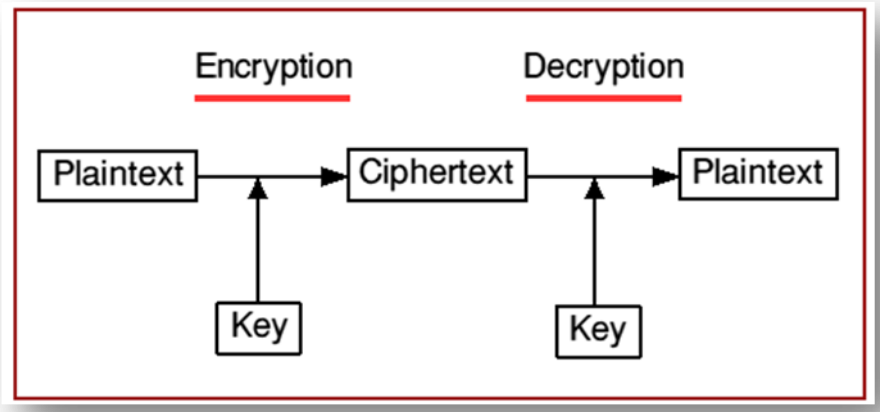

Figure 1: Symmetric cryptography (Source: http://www.queen.clara.net/pgp/art6.html**)**

III SUBSTITUTION TECHNIQUES

The two basic building blocks of all encryption techniques are substitution and transposition. A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols [Bose Ranjan., 2008]. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns. [Stallings W., 2005].

IV TRANSPOSITION TECHNIQUES

All the techniques examined so far involve the substitution of a ciphertext symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher [Stallings W., 2005]. [Bose, Ranjan.,2008].The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows [Stallings W., 2005]. [Bose, Ranjan. 2008].

V ENCRYPTION DECRYPTION TECHNIQUE

This Technique Is Based On The symbol table which consists different symbols for A to Z, a to z and 0 to 9 characters. These symbols are constant for alphabets and numerical. At first take the input string then reverse it character by character then find the corresponding symbols for input string from the table and replace with it. Secondly find out the ASCII values for the “Reverse” word and find the addition of the same for example Addition of REVERSE word ASCII values is 82+ 69+ 86+ 69+ 82 +83+ 69= 540.Thus data frame has two parts first part contain the addition of “reverse” word ASCII values. Second part has encrypted message. Thus receiver has and uses the same table by using this table and reverse value from the data frame receiver can decrypt the original message.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

ASCII Values	Encrypted Message

Figure 2: Data frame

Advantages

- intruder cannot detect the message
- Information Change between sender and receiver can not affect original message as both sender and receiver has common table.

Symbols Used for Transposition

```
('A'=>'77','B'=>'999','C' => '~','D' => '□,'E' => '<','F' => '‰','G' =>
'}','H' => 'æ','I' => '>','J' => 'Æ','K' => '§','L' => 'ÿ','M' =>'£' ,'N' =>
'OE','O' => '{','P' => '(','Q' => 'Xx','R' => 'à','S' => ']','T' => '©','U' =>
'ë','V' => '^','W' => '_','X' => 'Ø','Y' => 'ñ','Z' => 'š','a' => 'zz','b' =>
'aa','c' => 'VVV','d' => 'MM','e' => '88','f' => 'D','g' => 'CC','h' =>
'hh','i' => "oo",'j' => 'AAA','k' => 'LL','l' => 'PPP','m' => 'CCC','n' =>
'S','o' => 'fff','p' => 'QQQQ','q' => 'WWW','r' => 'EEEE','s' => 'W','t'
=> 'IIII','u' => 'sss','v' => 'RRR','w' => 'HHHHH','x' => 'nnnn','y' =>
'55','z' => '333','0' => '=','1' => 'vvv','2' => '*','3' => '+','4' => '22','5' =>
```

Figure 3: Symbols Used for Transposition

Example

Step 1

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Step 2

GOD YZAL EHT REVO SPMUJ XOF NWORB KCIUQ EHT

Step 3

Encrypted Message

}{□ñš77ÿ.<æ©.à<^{.](£ëÆ.Ø{‰.OE_{à999.§~>ëXx.<æ©

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Figure 4: Encrypted Message

Step 4

GOD YZAL EHT REVO SPMUJ XOF NWORB KCIUQ EHT

Step 5

Decrypted Message

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Figure 5: Decrypted Message

This technique is based on symbol table and that table is used by both sender and receiver after consider the message as input reverse the string character by character. Then pick the symbols from the symbol table and generate the encrypted message. To decrypt this message apply the same operation in the reverse order as shown in step 4 and step 5 shows the decrypted message thus encryption is performed in the single phase that is way it is one phase encryption and decryption method.

VI IMPLEMENTATION OF ALGORITHM

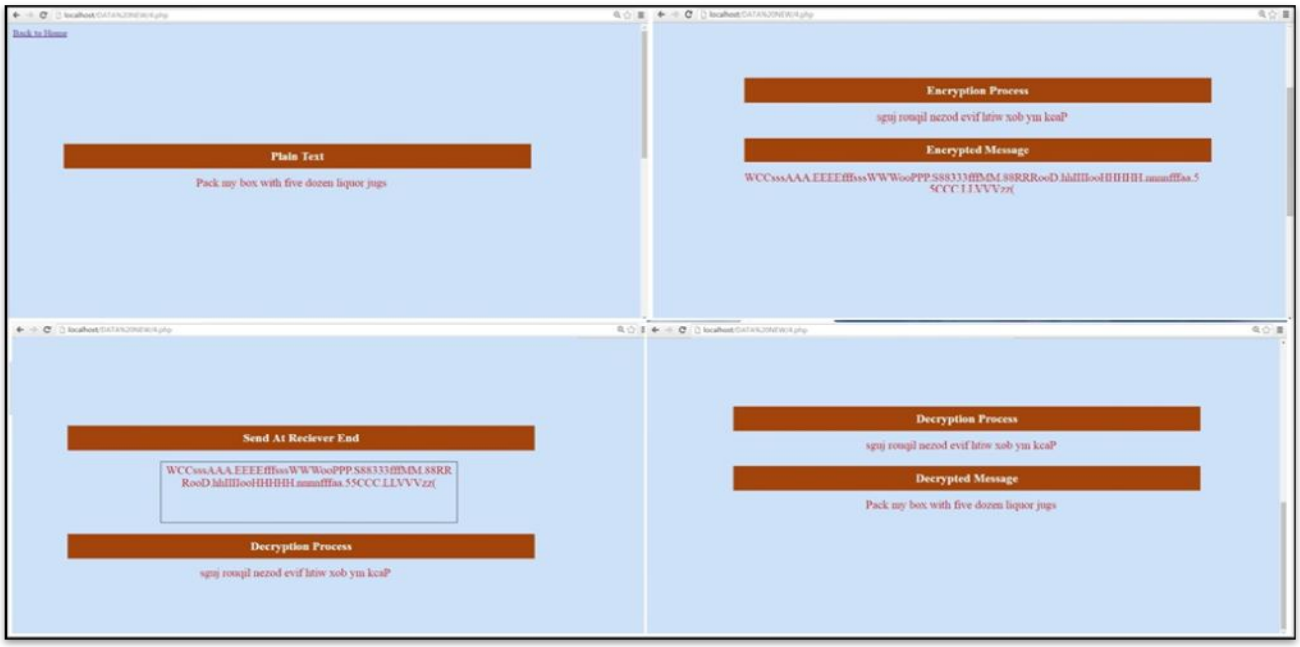

Figure 6: Implementation of Algorithm

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

The figure 6 shows an interface which takes plain text as an input. It is based on plain text transposition values and by applying further operation on it to convert the plain text in to encrypted form. The Algorithm is based on a symbol table and that particular table is used for encryption and decryption operations. Symbol table consists symbols according of A to Z, a to z and 0 to 9 thus table has a special symbol for each character between A to Z, a to z and 0 to 9.as the plain text entered in the technique. At first it will invert it as shown in figure 6 which 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. The decryption process after the transposition operation perform on the plain text and convert these in to special symbols then text is in encrypted form and ready for receiver end thus by using a secure channel pass this encrypted message on it and at the receiver end by using same symbol table that message can be decrypted easily. As it is very clear that decryption is the opposite process of the encryption. Thus during decryption from table symbols characters can be are generated in the reverse order.

Before message fully decrypted by the technique. It is in reverse form then during the final step message is fully decrypted and comes in the original shape which is also plain text. Thus Algorithm based on symbol table and both sender and receiver use this table during encryption sender use that table and during decryption receiver can use that table to find out the corresponding symbols to get the plain text.

VII CONCLUSION

This Encryption, Decryption Technique executes encryption process in a single phase. A symbol table is used by both sender and receiver for encryption and decryption process. This symbol table contains the special characters, symbols corresponding to all alphabets from a to z, A to Z and 0 to 9 numeric. A data frame is also used in this technique to contain the information which is used by the receiver during decryption. Data frame has two parts, first part has the details regarding reverse operation through ASCII values and second parts contain the encrypted message based on symbol table. Thus this technique is based on Substitution and Transposition Techniques concepts and also implemented using PHP.

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.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[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/