ISSN: 0975-766X
CODEN: IJPTFI
*Available Online through* *Research Article*
**www.ijptonline.com**

# TEXT ENCRYPTION AND DECRYPTION STRATEGY USING MATRIX OPERATIONS

**Nirmala.M, C S Pavan Kumar, Ansu Miriam Varghese, Neethu Santhosh**
School of Information Technology & Engineering, VIT University, Vellore, India.
*Email: nirmaladhinesh@gmail.com*

*Received on 25-10-2016* *Accepted on 02-11-2016*

**Abstract**

Text Encryption and decryption method havebeen implemented with a symmetric key cipher technique. A symmetric key cipher method converts plain text into its appropriate numerical form and generates a secret key during encryption. The same key is required to decrypt the message during decryption. This method can be used to encrypt passwords to save in the database in an encrypted form. The digital form of data is stored in a matrix. Several operations are performed on the matrix to make the data, secure and less accessible. A slightly different approach has been used to share the secret key during the encryption and decryption mechanisms. The encryption and decryption technique has been implemented using c#.

**Keywords:** Matrix operations, Symmetric Cipher Key, Encryption, Decryption.

## 1. Introduction

Cloud computing technologies [1-3] made individuals to store the information in remote storage. The information in the remote storage needs cryptography to secure the information [4-6]. Cryptography refers to different methods to secure information or hide information. Research has advanced widely in this field to protect confidential information of various sorts of attacks made by hackers. Several algorithms have been devised to hide data. NIST which is abbreviated as the National Institute of Standards and Technology has declared the AES algorithm as the standard for Encryption. Here, a different method using the Symmetric Cipher important technique has been implemented. Symmetric key algorithms [10] are algorithms that use the same shared secret key to encrypt the message and also to decrypt the message. This technique uses a very traditional method of encrypting the message. The technique is similar to the Caesar Cipher technique. The Caesar Cipher technique involves replacing an alphabet with another alphabet, where as in this paper, the alphabets are replaced by their corresponding ASCII values. Furthermore, these numbers are then stored in a matrix format, and several matrix operations are performed on it to secure the data.

**A. Existing Methods**

*1) Method 1:* The present technique is known as Byte Rotation Encryption algorithm(BREA) [7]. This technique converts the alphabets of the message to numbers and stores it in a matrix P of size 4x4.A random key of 16 numbers is generated in the range 1 to 26. The key matrix K is converted into a binaryformat with the formula K = K mod 2. The matrix P is then added to the matrix K. The resultant matrix further undergoes horizontal rotation, followed by vertical rotation [8]. The last position in the matrix, position (3, 3) of the matrix always remains 0. The numbers in the resultant matrix are converted back to alphabets. Thus the message is encrypted.To decrypt the message, again a random key matrix is made generating 16 random numbers in the range 1 to 26. It is further used to decrypt the message by re-rotating the matrix both vertically and horizontally. The matrix is then separated from the binary key matrix to obtain the binary matrix of the alphabets. The numbers in the matrix are further replaced by the alphabets to get the message

*2) Method 2:* Another technique "Crypt21" involves a block cipher method with substitution and transposition mechanisms. These mechanisms can be repeated many numbers of times to strengthen the encryption of the given plain text.

Here a key length of 4 to 8 characters is used. The plain text entered by the user undergoes Caesar substitution to obtain ciphertext. The mechanisms involved in encrypting the plain text are:

*A: Key Extension method:* Here a key is selected, and it is rotated by one position to the left in all possible ways of permutation. The new key is calculated using the formula:

N***k***= Sum(key) mod key length.

Further Nnumber of keys is concatenated together to form the final key [9].

*B: Substitution Method:*From the newly obtained long key and the user given plain text, cipher text is obtained using the formula:

C1=P+K mod 26.

*C: Transposition Method:* Matrices of order 3x3 consisting of 0s and 1s are used to depict the key. The positions of 1s in the matrix show the corresponding pattern of the important letter.

**2. Procedure Of Implemented Technique**

The same random key generated during the encryption mechanism is used to decrypt the message during decryption mechanism. This is the major difference from the existing work that has been implemented in this paper.

***A: Encryption algorithm:***

1. Enter text in the range 8 to 15 characters without spaces and access the text.
2. Convert alphabets to ASCII value and store in abyte array called “asciiBytes.”
3. Store ASCII values from byte array to a 4x4 matrix called “asciiMatrix.”
4. Generate random number in the range 65 to 122.
5. Subtract random number from 32767.
6. Convert result into binary value and store in amatrix called “keyMatrix.”
7. Add “asciiMatrix” and “keyMatrix.”
8. Resultant matrix is called the “sumMatrix.”
9. Place arandom number in the last position of thematrix.
10. Transpose matrix and perform horizontal rotation.
11. Make a 4x4 matrix called “FinalOpMatrix” with values one all columns of 1st row, value 2 in all columns of 2nd row, value 3 in all columns of 3rd row and value 4 in all columns of row 4.
12. Add transposed matrix with “FinalOpMatrix.”
13. Convert matrix to a byte array.
14. Obtain string from thearray.
15. Display obtained cipher text in cipher text textbox.

A. ILLUSTRATING ENCRYPTION ALGORITHM

UserInput is: HELLOHOWAREYOU

Length of asciiBytes is: 14

asciiMatrix:

| | | | |
|---|---|---|---|
| 72 | 69 | 76 | 76 |
| 79 | 72 | 79 | 87 |
| 65 | 82 | 69 | 89 |
| 79 | 85 | 0 | 0 |

Random Number: 1

Key: 32766

Binary string:111111111111110

Length of binaryBytes is: 15

keyMatrix:

| | | | |
|---|---|---|---|
| 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 |

Adding asciiMatrix and keyMatrix

SumMatrix:

| | | | |
|---|---|---|---|
| 73 | 70 | 77 | 77 |
| 80 | 73 | 80 | 88 |
| 66 | 83 | 70 | 90 |
| 80 | 86 | 0 | 1 |

Rotated Matrix:

| | | | |
|---|---|---|---|
| 77 | 73 | 70 | 77 |
| 80 | 88 | 80 | 73 |
| 80 | 70 | 90 | 66 |
| 80 | 86 | 0 | 1 |

Transpose of Rotated Matrix:

| | | | |
|---|---|---|---|
| 77 | 80 | 83 | 80 |
| 73 | 88 | 70 | 86 |
| 70 | 80 | 90 | 0 |
| 77 | 73 | 66 | 1 |

FinalOpMatrix:

| | | | |
|---|---|---|---|
| 1 | 1 | 1 | 1 |
| 2 | 2 | 2 | 2 |
| 3 | 3 | 3 | 3 |
| 4 | 4 | 4 | 4 |

Final Matrix:

| | | | |
|---|---|---|---|
| 78 | 81 | 84 | 81 |
| 75 | 90 | 72 | 88 |
| 73 | 83 | 93 | 3 |
| 81 | 77 | 70 | 5 |

Size of encrypted array is: 16

Cipher text is:NQTQKZHXIS] QMF

The length of cipher text is: 16

Decryption Algorithm:

1. Access string from encrypted text box.
2. Convert characters to ASCII value.
3. Store ASCII value into a byte array called "decryptAsciiBytes."
4. Store values from thearray into a matrixcalled"decryptAsciiMatrix."
5. Make a 4x4 matrix called "FinalOpMatrix" with values one all columns of 1st row, value 2 in all columns of 2nd row, value 3 in all columns of 3rd row and value 4 in all columns of row 4
6. Subtract FinalOpMatrixfrom"decryptAsciiMatrix".
7. Store resultant matrix as "decryptAsciiMatrix."
8. Transpose matrix.
9. Rotate matrix.
10. Remove number from thelast position of the matrix and set thelast position to 0.
11. Calculate random number= removed number-4.
12. Generate key= 32767-random number.
13. Convert key to thebinary matrix.
14. Subtract binary matrix from sum matrix.
15. Convert resultant matrix to ASCII byte array.
16. Convert the ASCII values to string.
17. Display the decrypted text in the decrypted text box.

B. ILLUSTRATING THE DECRYPTION ALGORITHM

Length of decryptAsciiBytes is: 16

The decryptAsciiMatrixis:

| | | | |
|---|---|---|---|
| 78 | 81 | 84 | 81 |
| 75 | 90 | 72 | 88 |
| 73 | 83 | 93 | 3 |
| 81 | 77 | 70 | 5 |

Decrypted Random Number: 1

FinalOpMatrix:

| | | | |
|---|---|---|---|
| 1 | 1 | 1 | 1 |
| 2 | 2 | 2 | 2 |
| 3 | 3 | 3 | 3 |
| 4 | 4 | 4 | 4 |

The decryptAscii matrix is :

| | | | |
|---|---|---|---|
| 77 | 80 | 83 | 80 |
| 73 | 88 | 70 | 86 |
| 70 | 80 | 90 | 0 |
| 77 | 73 | 66 | 1 |

The transposed matrix is:

| | | | |
|---|---|---|---|
| 77 | 73 | 70 | 77 |
| 80 | 88 | 80 | 73 |
| 83 | 70 | 90 | 66 |
| 80 | 86 | 0 | 1 |

The re-rotated matrix is:

| | | | |
|---|---|---|---|
| 73 | 70 | 77 | 77 |
| 80 | 73 | 80 | 88 |
| 66 | 83 | 70 | 90 |
| 80 | 86 | 0 | 1 |

The matrix after removing the random number is:

| | | | |
|---|---|---|---|
| 73 | 70 | 77 | 77 |
| 80 | 73 | 80 | 88 |
| 66 | 83 | 70 | 90 |
| 80 | 86 | 0 | 0 |

Binary string:111111111111110

Length of binaryBytes is: 15

KeyMatrix:

| | | | |
|---|---|---|---|
| 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 |

dasciiMatrix:

| | | | |
|---|---|---|---|
| 72 | 69 | 76 | 76 |
| 79 | 72 | 79 | 87 |
| 65 | 82 | 69 | 89 |
| 79 | 85 | 0 | 0 |

Size of encrypted array is: 16

Decryptedtext: HELLOHOWAREYOU

The length of decrypted text is: 14

**3. Results**

This method successfully generates a cipher text. It does not depend on a totally new key that is generated randomly during the decryption technique to decrypt the cipher text. It uses the same key that was used for encryption in decryption as well.

This method cannot involve less than eight characters and more than 15 characters in this technique since it uses a 4x4 matrix.Hence it cannot be used for encrypting and decrypting a message to be transferred, but can only be used for encryption and decryption of passwords for a website, etc.

**4. Conclusion**

A simple, but theeffective technique has been used for the encryption and decryption of small sized text messages. This paper can be concluded by restating the different techniques utilized in this mechanism. A small sized text after being replaced by numbers is stored in amatrix format. It is further summed up with a key matrix followed by

performing transpose and rotation operations on the resultant matrix. The above mechanisms are reversedto decrypt the encrypted message.

Encryption and decryption of a text message can be made further stronger with more added operations on the matrix or the key.

**References**

1. Krishna, P. V. Honey bee behavior inspired load balancing of tasks in cloud computing environments. Applied Soft Computing.2013;13(5): 2292-2303.
2. Raj E.D, Babu L.D, Area E, Nirmala M, Krishna,P.V.Forecasting the Trends in Cloud Computing and its Impact on Future IT Business.Green Technology Applications for Enterprise and Academic Innovation; 2014.p.14.
3. Babu L. D, & Krishna P. V. An execution environment oriented approach for scheduling dependent tasks of cloud computing workflows. International Journal of Cloud Computing. 2014; 3(2): 209-224.
4. DhineshBabu L. D, Gunasekaran A, Krishna, P. V. A decision-based pre-emptive fair scheduling strategy to process cloud computing work-flows for sustainable enterprise management. International Journal of Business Information Systems. 2014; 16(4): 409-430.
5. Raj E. D, Nivash J. P, Nirmala M, Babu L. D. A scalable cloud computing deployment framework for efficient MapReduce operations using Apache YARN. In Information Communication and Embedded Systems (ICICES), 2014 International Conference on IEEE, 2014.
6. Babu L. D, Krishna P. V, Zayan A. M, Panda V. An analysis of security related issues in cloud computing. In International Conference on Contemporary Computing, Springer Berlin Heidelberg, pp. 180-190, 2011.
7. Gouttam, N. Implementation Of Simulation Of Byte Rotation Encryption Algorithm. International Journal of Technology Enhancements and Emerging Engineering Research.2014;2(5);1-10.
8. Appaji S. V, Acharyulu G. V.Recent Advancements on Symmetric Cryptography Techniques-A Comprehensive Case Study. Global Journal of Computer Science and Technology.2014;14(2-F): 19.
9. Malik, S. A Novel Key-Based Transposition Scheme for Text Encryption. In Frontiers of Information Technology (FIT): IEEE; 2011.p. 201-205).
10. Thakur J, Kumar, N. DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. International journal of emerging technology and advanced engineering.2011; 1(2):6-12.