# A HYBRID APPROACH FOR DATA SECURITY USING MODIFIED RECURSIVE MODULO AND KEY ROTATION OPERATIONS

**Sonali Sahu[1], Ms. Prateeksha Pandey[2]**

*[1]M.Tech.Scholar, [2]Assistant Professor, Dept.of Computer Science & Engg.,*

*CSIT, Durg, Chhattisgarh (India).*

## ABSTRACT

*When it happens data security, communicating something specific needs to be secured keeping in mind the end goal to shield the message from being utilized by an un-approved client. As I contemplated different paper there are having different calculations that protected the information like RSA, DES, TDES moreover. This paper helps in giving more security to the message as it scramble the message first to a muddled organization as it rearranges the letter of the data message keeping in mind the end goal to ensure the message and afterward recursive modulo-2 is connected lastly taken after with key Rotation operation. In Recursive Modulo-2 and key Rotation operation a square of n bits is taken as an information stream where n differs from 4 to 256, from a nonstop stream of bits and the strategies works on it to produce the middle encoded stream. This method specifically includes all the bits of pieces in a Boolean operation and a session key. Utilizing of scramble gives more security to the message send by the sender.*

***Keywords: scramble, securing message using Recursive MODULO-2 and Key Rotation operation, Cipher text, Block cipher, Session key***

## I INTRODUCTION

In the creating district of the cryptography strong traditions are used feasibly as a piece of the technique for guaranteeing mystery information in the midst of its transmission more than a framework. Information is encoded at the senders end using an encryption tradition and a key. On landing at the goal point, the endeavor of translating is executed utilizing an unscrambling tradition close by a key to recoup the source information. Encryption and disentangling are in nutshell termed as cryptography. On the reason of the keys used as a piece of the entire methodology, there exists two grouping of cryptography. The current field of cryptography can be partitioned into a few ranges of study: Symmetric key cryptography, open key cryptography, cryptanalysis, cryptography primitives, cryptosystems. Symmetric key cryptography alludes to encryption system in which both sender and collector have the same key .symmetric key figure are executed as either piece figure or stream cipher. A square figure and enciphers enter in pieces of plain content instead of individual character. The info structure utilized by a stream figure. key cryptography alludes to encryption technique in which both sender and collector utilizes diverse key public key cryptography can likewise be utilized for

actualizing computerized marks key. The goal of cryptanalysis is to find a couple of deficiency or feebleness in a cryptographic arrangement, thusly permitting its subversion or avoidance. it is a commonplace distortion that every encryption system can be broken.

Region 2 of the paper deals with the proposed technique, Expected.Results are given in area 3, conclusion are given on area 4, References are given in area 5 .

## II METHODOLOGY

Figure shown the overall flow of our proposed technique.

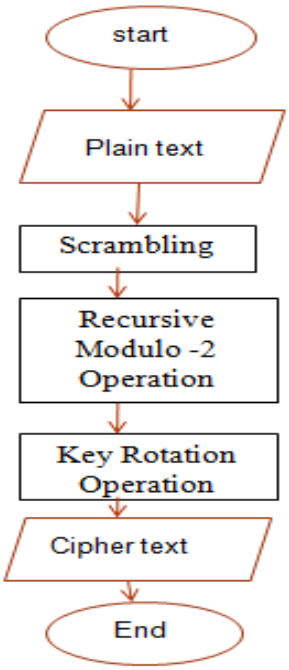



Fig: Encryption process

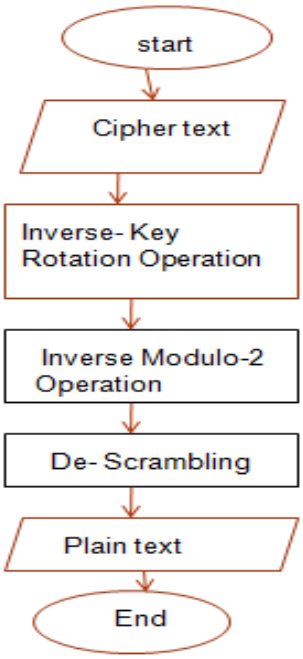
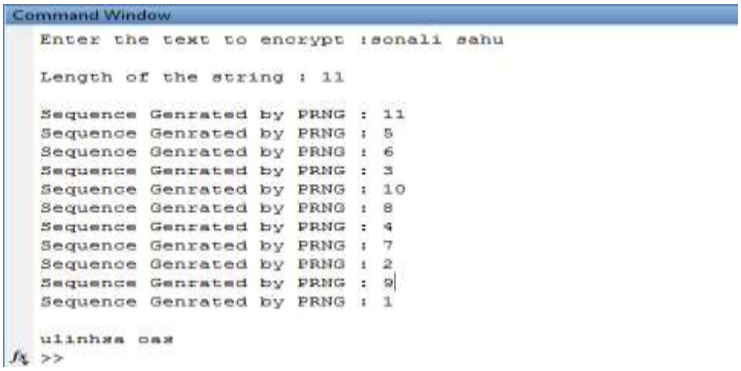



Fig: Decryption process

This techniques operates in three phases:

### a. First phase scramble the message using scrambler.

It takes the plaintext then calculate the length of the string then generate pseudo random sequence of length string and permute the input the input string index to the pseudo random sequence pattern. here snapshot shown the process of scrambling. Here the first snapshot shows the output of scrambling process other snapshot shows the ASCII form then converted into binary form which is then used by Modulo operation.




asinp <11x1 uint8>

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 105 | | | |
| 2 | 110 | | | |
| 3 | 117 | | | |
| 4 | 32 | | | |
| 5 | 115 | | | |
| 6 | 108 | | | |
| 7 | 115 | | | |
| 8 | 111 | | | |
| 9 | 97 | | | |
| 10 | 97 | | | |
| 11 | 104 | | | |
| 12 | | | | |
| 13 | | | | |
| 14 | | | | |
| 15 | | | | |
| 16 | | | | |
| 17 | | | | |
| 18 | | | | |

bintext <11x8 char>

```
val =

01101001
01101110
01110101
00100000
01110011
01101100
01110011
01101111
01100001
01100001
01101000
```

## b. Second phase encrypt the message using Recursive Modulo-2 Operation .

The technique consider the plaintext from the first phase as a stream of finite number of bits N , and is divided into a finite number of blocks, each also containing a finite number of bits n ,where , 1<=n<=N.

The principle of Recursive Modulo-2 Operation is discussed in following manner:

Let P = is a block of size n in the plaintext. Then the first intermediate block can be generated from P in the following way:

$$s_2^1\ s_3^1 = s_0^0\ s_1^0 \oplus s_4^0\ s_5^0$$

, 0<=i<(n-1), 0<=j<(n-1); ⊕ stands for the exclusive-OR operation.

In the same way, the second intermediate block
of the same size (n) can be generated by:

$$s_0^2\ s_1^2 = s_0^1\ s_1^1 \oplus s_2^1\ s_3^1$$

$$s_2^2\ s_3^2 = s_0^1\ s_1^1 \oplus s_4^1\ s_5^1$$

,0<=i<(n-1) ,1<=j<(n-1); ⊕ stands for the exclusive-OR operation.

## c. Third Phase encrypt the output of above phase by Recursive Key Rotation.

The rules to be followed for generating a cycle are as follows:

1. Consider any source stream of a limited number (where N=2n, n =3 to 8) and gap it into two a balance of.

2. Consider any key worth (key= 2n, where n=1 to 7) relies on the source stream that is, key quality is the a large portion of the source stream).

3. Make the modulo-2 expansion (X-OR) with the key worth to the first a large portion of the source stream, to get the first middle of the road piece.

4. Make the modulo-2 expansion with the key quality (however now the key worth is switched) to the last a large portion of the source stream to get the second transitional square.

The same operation is performed for whole stream number of time with a varying block sizes.

## III EXPECTED RESULT

When we using this proposed approach definitely we will protect out data by attackers. it provides level of security ,it may be difficult to decrypt the message if the message is encrypted using the proposed key system or like manner.

- Increase the security of data transmission.
- Minimize the encryption and decryption time.
- Reduce effect of crypt analysis.
- Reduced time complexity

## VI CONCLuSION

Technique presented here is implemented for different categories of files like .cpp, .exe,.doc,.dll, .sys.When this technique is implemented with X-NOR or other operations using the same logic it will not generate a cycle so this logic cannot be implemented with the other operations. This technique is implemented on 1.3 GHZ processor. the file size increases the encryption time as well as decryption time increases. For this technique only eight bits blocks are taken, and the third intermediate block is considered here as encrypted stream, so the time required to get the encrypted stream is always be larger than that of decryption because only one iteration is required to get the source stream in the decryption part.,since this technique generates a cycle.It can be easily implemented in any high level language in different form for practical application purpose to provide security in message transmission.

## REFERENCES

[1] J.K.Mandal , P.K.Jha, "Securing Message Using Recursive Modulo-2 and Key Rotation Operation", International Conference on computational intelligence Modeling Techniques and Applications (CIMTA)2013.

[2] Mandal J. K. and Dutta S. "A Space-Efficient Universal Encoder for Secured Transmission", International Conference on Modeling and Simulation (MS' 2000- Egypt), Cairo, April 11-14, pp-193-201,2000.

[3] Jha P. K.,Mandal .J.K, S. Shakya " Encryption through cascaded recursive key rotation and arithmetic operation of a session key (CRKRAO)" accepted to the Technical publication of the Engineering Association of Nepal, Kathmandu.

[4] D. Welsh , "Codes and Cryptography", Oxford: Claredon Press, 1988

[5] J.Seberry and J.Pieprzyk, "An introduction to computer security",Australia : Prentice hall of Australia 1989.

[6] C. Coupe, P. Nguyen and J. Stern," The Effectiveness of Lattice Attacks against Low-Exponent Proceeding of Second International Workshop on Practice and Theory in Public Key Cryptography, PKC'99, vol1560, of lecture notes in Computer Science, Springer-Verlag, pp 204-218,1999.

[7] RSA Vulnerabilities", Journal of Cryptology, vol 10, pp 233-260,1997.ss

**Biographical Notes**

**Sonali Sahu** is presently pursuing M. Tech. final year in Computer Science and Engineering Department from C.S.I.T , Durg ,Chhattisgarh, India.

**Ms Prateeksha Pandey** is **working** as a Assistant Professor in Computer Science and Engineering Department, C.S.I.T ,Durg , Chhattisgarh.