SECURING DATA USING MODIFIED RECURSIVE MODULO -2 AND KEY ROTATION OPERATION

[1]Sonali sahu, [2]Prateeksha Pandey
[1]M.Tech Scholar, Department of Comp. Sci. & Engg.,
Chhatrapati Shivaji Institute of Technology, Durg, Chhattisgarh, India
[2]Assistant Professor, Department of comp.Sci. & Engg.
Chhatrapati Shivaji Institute of Technology
Email: [1]sonalisahu181990@gmail.com, [2]Prateekshapandey@csitdurg.in

***Abstract*- When it comes about information security, sending a message needs to be secured in order to protect the message from being used by an un-authorized user. As I studied various paper there are having various algorithms that secure the data like RSA, DES, TDES also. This paper helps in providing more security to the message as it scramble the message first to an unintelligible format as it shuffles the letter of the input message in order to protect the message and then recursive modulo-2 is applied and finally followed with key Rotation operation. In Recursive Modulo-2 and key Rotation operation a block of n bits is taken as an input stream where n varies from 4 to 256, from a continuous stream of bits and the techniques operates on it to generate the intermediate encrypted stream[1]. This technique directly involves all the bits of blocks in a Boolean operation and a session key. Using of scramble provides 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 developing region of the cryptography solid conventions are utilized viably as a part of the method of ensuring secret data amid its transmission over a system.

,

Data is encoded at the senders end utilizing an encryption convention and a key. On arriving at the objective point, the undertaking of decoding is executed using an unscrambling convention along side a key to recover the source data. Encryption and decoding are in nut shell termed as cryptography. On the premise of the keys utilized as a part of the whole process, there exists two classification of cryptography. The modern field of cryptography can be divided into several areas of study: Symmetric key cryptography, public key cryptography, cryptanalysis, cryptography primitives, cryptosystems.

Symmetric key cryptography refers to encryption method in which both sender and receiver share the same key .symmetric key cipher are implemented as either block cipher or stream cipher. A block cipher and enciphers input in blocks of plain text as opposed to individual character. The input form used by a stream cipher.

In public key cryptography refers to encryption method in which both sender and receiver uses different key. public key cryptography can also be used for implementing digital signatures key. The objective of cryptanalysis is to discover a few shortcoming or frailty in a cryptographic plan, along these lines allowing its subversion or evasion. it is a typical misinterpretation that each encryption technique can be broken.

A significant part of the hypothetical work in cryptography concerns cryptographic primitives calculations with essential cryptographic properties and their relationship to other cryptographic problems.

One or more cryptographic primitives are frequently used to create a more intricate calculation, called a cryptographic framework, or cryptosystem. Cryptosystems are intended to give specific usefulness while ensuring certain security properties . Cryptosystems utilize the properties of the basic cryptographic primitives to help the framework's security properties.The main objective of this project is

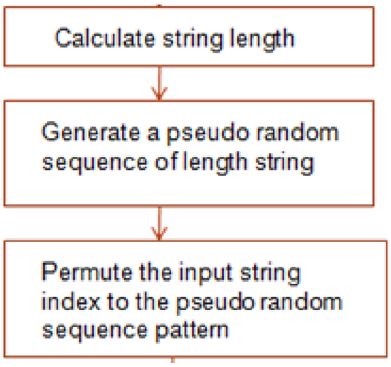
- To develop one system which provide the high security to the information.
- Reduces the crypt analysis.

Area 2 of the paper manages the standard of his paper. . A proposal for key generation described in section 3. Results are given in section 4. . Conclusions are given in section 5 and references are drawn in section 6.

II. PROPOSED TECHNIQUE

This techniques operates in three phases:

a. first phase scramble the message using scrambler.


Calculate string length
Generate a pseudo random sequence of length string
Permute the input string index to the pseudo random sequence pattern

b. second phase encrypt the message using Recursive Modulo-2 Operation of Paired bits of a stream[1].

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 = $s_0^0\ s_1^0\ s_2^0\ s_3^0\ s_4^0\ \ldots.s_{n-1}^0$ is a block of size n in the plaintext. Then the first intermediate block $I_1 = s_0^1\ s_1^1\ s_2^1\ s_3^1\ s_4^1\ \ldots..s_{n-1}^1$ can be generated from P in the following way:

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

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

$s_i^1\ s_{j+1}^1 = s_{i-j}^0\ s_{i-j+1}^0 \oplus s_{i+j+2}^0\ s_{i+j+3}^0$, 0<=i<(n-1), 0<=j<(n-1); ⊕ stands for the exclusive-OR operation.

In the same way, the second intermediate block $I_2 = s_0^2\ s_1^2\ s_2^2\ s_3^2\ s_4^2\ \ldots..s_{n-1}^2$ of the same size (n) can be generated by:

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

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

$s_i^2\ s_{j+1}^2 = s_{i-j}^1\ s_{i-j+1}^1 \oplus s_{i+j+2}^1\ s_{i+j+3}^1$,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[1].

The technique considers the encrypted message from the first phase (here third encrypted block) 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 rules to be followed for generating a cycle are as follows:

1. Consider any source stream of a finite number (where N=2n, n =3 to 8) and divide it into two equal parts.

2. Consider any key value (key= 2n, where n=1 to 7) depends upon the source stream that is, key value is the half of the source stream).

3. Make the modulo-2 addition (X-OR) with the key value to the first half of the source stream, to get the first intermediate block.

4. Make the modulo-2 addition with the key value (but now the key value is reversed) to the last half of the source stream to get the second intermediate block.

The same operation is performed for whole stream number of time with a varying block sizes. K such iteration is done and the final intermediate stream after k iterations generates the cascaded form of the encrypted stream. All of the different block sizes and k constitute the key for the session.

This key may be considered as session key for that

particular session. This process is repeated until the source stream is generated.

If this process continues for a finite number of iterations, the source block P is regenerated forming a cycle, which depends on the value of block size n. Any intermediate block in the recursive process may term as intermediate encrypted block and any block can be taken as the input for the second phase.

III. Generation of Session Key

To ensure the successful encryption of the proposed technique with varying size of blocks, a 114-bit key format consisting of 12 different segment has been proposed here [2,3,4,5,6,7,8] For the segment of rank the R, there can exist a maximum of N=218-R blocks, each of unique size of S=218-R, R starting from 1 and moving till 14[1].

- Segment with R=1 formed with the first maximum 131072 blocks, each of size 131072 bits
- Segment with R=2 formed with the next maximum 65536 blocks, each of size 65536 bits
- Segment with R=3 formed with the next maximum 32768 blocks, each of size 32768 bits
- Segment with R=4 formed with the next maximum 16384 blocks, each of size 16384 bits
- Segment with R=5 formed with the next maximum 8192 blocks, each of size 8192 bits
- Segment with R=6 formed with the next maximum 4096 blocks, each of size 4096 bits
- Segment with R=7 formed with the next maximum 2048 blocks, each of size 2048 bits
- Segment with R=8 formed with the next maximum 1024 blocks, each of size1024 bits
- Segment with R=9 formed with the next maximum 512 blocks, each of size 512 bits
- Segment with R=10 formed with the next maximum 256 blocks, each of size 256 bits
- Segment with R=11 formed with the next maximum 128 blocks, each of size 128 bits
- Segment with R=12 formed with the next maximum 64 blocks, each of size 64 bits
- Segment with R=13 formed with the next maximum 32 blocks, each of size 32 bits
- Segment with R=14 formed with the next maximum 16 blocks, each of size 16 bits.

IV. Result

When we using this proposed approach definitely we will protect out data by attackers. it provides level of security. In connection with the Brute-force attack of decrypting the message by the hackers ,it may be difficult to decrypt the message if the message is encrypted using the proposed key system or like manner.

V Conclusion

The 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. In table 2 it is seen that as 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.

VI. 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 RSA"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.

[8] M. Wiener, "Cryptanalysis of Short RSA Secret Exponents", IEEE Transactions on Information Theory, vol 36, pp 553-558,1990.