International Journal of Innovative Research in Science and Engineering
Volume 7, Issue 10, 2021
www.ijirse.com
ISSN: 2454-9665

A Block Cipher Encryption Mechanism with Image Key

G Sowjanya[1], M Ramesh[2]

[1,2] *Department of Information Technology, RVR & JC College of Engineering, Guntur, Andhra Pradesh, India.*

{ G Sowjanya, sowjanyagorantla01@gmail.com, M Ramesh, mrameshmailbox@gmail.com;}

Abstract

We introduce a new encryption mechanism that is applied on individual blocks of size sixteen bytes. Each block undergoes different stages which will transform the block either by substitution or transposition mechanisms. The selection of operations at each stage is decided by an image key. Proposed technique presents a sophisticated encryption mechanism that is feasible to implement in all conditions. Operations used are very simple and at same time it presents very difficult situation for the attacker to break it. This technique also performs compression in addition to encryption and sender, receiver doesn't need to transfer keys for each communication.

Keywords—Block Cipher, Substitution, Transposition, Secret Key

I INTRODUCTION

Security has become an essential need in our daily life because of every one trying to transform to using digital equipments in today's digital communication era. Increased use of digital transactions also leads to increase of cyber threats and vulnerable attacks. To cope with such situations, information must be shielded with security area known as cryptography. Many cryptographic techniques exist that try to protect confidential information from unwanted thefts and misuse.

II PROPOSED MECHANISM

Compression phase

Proposed technique comprises of two major steps one is compression and other is encryption which are presented in figure 1.

Compression process is adapted from **[4]** which tries to transform eight bytes into seven bits. This is done by padding unused MSB bit of first seven bytes with bits of the eighth byte. Compression phase yields two benefits. One is data size reduces to 12.5% and second one is each byte contains full packed eight bits which are required for encryption process.

Encryption process reads compressed file resulted from compression phase and partitions them into independent blocks of size sixteen. Each sixteen byte block then undergoes different stages which gets shuffled and modified there and finally get written to cipher text file. All operations performed on each stage are randomly selected by an image that acts as key where sender and receiver must keep it secret. The encryption phase has the following stages.

A. Direction Transposition

B. Splitter
C. Matrix Transposition
D. Exchanger
E. Mixer
F. Key Appler

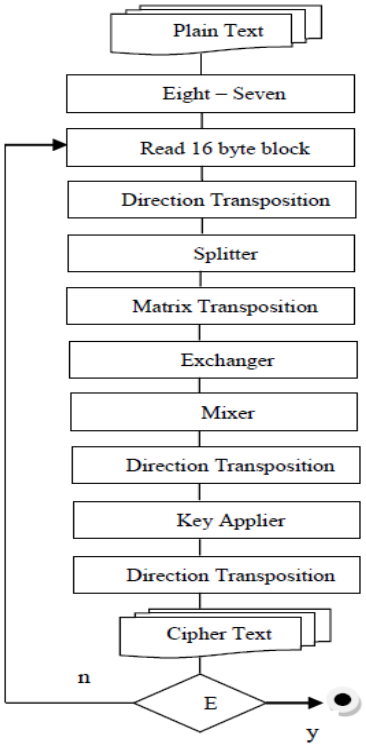

Figure 1- Proposed Mechanism

Direction Transposition

This phase changes contents of sixteen byte block based on 48 directions as shown in figure 2 where direction is decided using image values which acts a key throughout the entire process. This phase is applied in three stages as shown in figure and direction deciding equation is given in step 1.

$$D = x \% 48 \quad (1)$$

Here x takes three different values in three stages. x will be w(IM), h(IM) and sum(w(IM)+h(IM)) where IM is the image acting as key, w is width of IM and h is its height. The values of x can be varying with time and communicating parties selection.

Splitter

It divides 16 byte block coming from previous stage into two binary blocks of 64 bits each. First half of 16 byte block forms first binary block and next half forms second binary block.

Matrix Transposition (MT)

Two binary blocks resulted from splitter phase will undergo matrix transposition operations in this stage. It uses masking bits read from image file that decides on which block matrix transposition operation is applied.

ISSN: 2454-9665

Masking Bits	Block 1	Block 2
0 0	No	No
0 1	No	Yes
1 0	Yes	No
1 1	Yes	Yes

Table 1- Masking bits used in Matrix Transposition

2.1 Above tables shows masking bits where 00 indicate MT is not applied on two blocks and are left without any modification. 01 indicate MT is done only block 2, similarly 10 indicate MT is done only on block 1 and finally 11 indicate MT is done on both blocks.

Exchanger

Exchanger phase takes two binary blocks from matrix transposition phase and interchanges them using a bit selected from image. If image value is 0 no exchange is performed and if it is 1 then both blocks get swapped.

Mixer

Mixer phase receives two binary blocks from exchanger as input and merges themto constitute sixteen byte block again.

Key Applier

Key applier is the primary phase in the encryption process in which 128 bit key is applied on sixteen byte block. For each sixteen byte block a separate 128 bit key is read from image key. To do this sixteen byte intermediate block is converted to 128 bits and X-ORed with 128 bit key values read from image.

III ILLUSTRATIVE EXAMPLE

We show the consequences of the encryption process in this section. The complete picture of an initial plain text sixteen byte block undergoing various stages is depictedin figure 3 using numbers.

Step1 performs direction transposition operation. Let the direction decided be 33 then it reads plain text content in a ziz-zag direction as shown in directions figure 2. Step2 partitions 16 byte block into two 64 bit binary blocks. Step 3 performs matrix transposition and let masking bit values are 01 then only second binary block gets changed by performing matrix transposition. In step 4, let masking bit value is 1 then both binary blocks gets exchanged. Step 5 is a mixer function which again combines two binary blocks from previous phase into sixteen byte block. Step 6 is againdirection transposition phase which transforms block using direction 1. Step 7 is the key applier phase which reads 128 bit key from image and XOR operation is applied on block contents. A sample 128 bit key converted in 16 byte is shown in figure 3. Step 8 is the final phase in the encryption process which is again direction transposition phase that transforms final block as per direction 16. At last the resulted block is written to cipher text file.

ISSN: 2454-9665

IV RECEIVER S MECHANISM

The receiver at other side performs reverse operations of encryption process to get sixteen byte blocks. Later the generated file is decompressed by expanding seven bytes to eight bytes. To do this all operations must be done using same image file which are kept secret by sender and receiver.

V STRENGTH OF PROPOSED APPROACH

In the entire encryption process keys are used only in direction transposition, matrix transposition, exchanger and key applier phases. There are two alternatives for attacker to break this algorithm. One possibility is he must succeed in achieving image accepted by sender and receiver as key. Next possibility is attacker must go for brute force attack. To do brute force analysis number of trails required to break the algorithm is presented below.

In direction transposition phase each block is read and changed in one of 48 directions. Hence to guess this phase 48 trials are required and also it is applied in three stages of encryption. Matrix Transposition requires 4 trials and Exchange

operation require 2 trials. Key Applier phase uses 128 bit key and hence 2^{128} trials are needed for this stage.

$$T = 48 \times 4 \times 2 \times 48 \times 2^{128} \times 48$$

$$= 16 \times 3 \times 4 \times 2 \times 16 \times 3 \times 2^{128} \times 16 \times 3$$

$$= 2^4 \times 3 \times 2^2 \times 2 \times 2^4 \times 3 \times 2^{128} \times 2^4 \times 3$$

$$= 2^{143} \times 3^3 \quad (2)$$

Above equation shows number of trials required to break a single block of sixteen byte.

$$N = T \times B \quad (3)$$

But the total number of trials needed for breaking the entire message is given in equation 3 where B is the number of sixteen byte blocks resulted after compression phase.

VI CONCLUSIONS

In this paper we have introduced a new block cipher mechanism using image as key. It also performs compression besides doing encryption. The algorithm is easily understood, operations are quite simple, can be implemented with minimum data structures and in quick time bounds. Compression mechanism reduces data size to

12.5 % irrespective of file size. To break this algorithm, attackers must strive hard for $2^{143} \times 3^3 \times B$ attempts which create a huge task for them. As each block is independent of others this approached can be implemented on a multiprocessor systems to achieve further fast results. In our future sections we try to establish relationship between blocks as to provide more security.

ISSN: 2454-9665

References

1. W Stallings, *Cryptography and Network Security: Principles and Practice, 5e*. (Prentice Hall, 2010).
2. Ramesh Makala, Venkateswarlu Bezavada, Ranganath Ponnaboyina, A Fast Encription and Compression Techinic on SMS Darta, In 2017 IEEE Int. Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 1240-1244, 2017.
3. M Ramesh, B Hemantha Kumar, and A Srinagesh, A Novel Block-Cipher Mechanism for Information Security in Cloud System, In 2016 IEEE 6th Int. Conference on Advanced Computing (IACC), Bhimavaram, India, 524-528, 2016.
4. Subhas Barman, Debasis Samanta and Samiran Chattopadhyay, Fingerprint based crypto-biometric system for network security EURASIP Journal on Information Security (2015).
5. A Jain, U Uludag,. IEEE Trans. Pattern Anal. Mach. Intell. 25, 1494–1498 (2003).
6. Dr. Salah M. and Dr. Feryal I. Haj Has-san, "Fingerprint Minutiae Extraction," Journal of Computing Press, vol. 2, November 2010.