IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661 Volume 4, Issue 5 (Sep.-Oct. 2012), PP 33-39
www.iosrjournals.org

Design and Implementation of New Encryption algorithm to Enhance Performance Parameters

[1]Rajni Jain, [2]Ajit Shrivastava
[1]M. Tech. Scholar CSE Dept., TRUBA College, Bhopal (M.P.),India,
[2]Prof. CSE Dept., TRUBA College, Bhopal (M.P.),India,

Abstract: *The study of cryptography has always had interesting research area. It is already known that security of data is the primary concerned in the public network. Encryption and decryption is the process of cryptography technique which should be provided secrecy of the data over the network. In the real world there are so many organizations working on large databases over a public network like the banking sector, so there the security is of prime concern. Encryption is exhaustively used to keep confidential data. Other than encryption, there are so many cryptography techniques like digital signature, digital time-stamping, digital certificates etc. Used for security purpose. But encryption is the most used technique where transactions take place continuously between users. This paper has suggested new block cipher encryption algorithm. Suggested algorithm is the combination of different type of operation (logical and mathematical) to perform encryption. To calculate the performance of the suggested algorithm, the two parameters were used; these parameters are avalanche effect and execution time. The results achieved by applying the proposed technique show better performance of the algorithm as compared existing algorithm.*

Key Word: *Cryptography, Encryption, Decryption, Security, Algorithm, Network.*

I. Introduction

Use of the Internet is not always just clicking around and passively taking the information, such as fetching information and sending information. Purchasing something over the Internet from an online vendor, or signing up for an online account, requires entering into a good deal of sensitive personal information. A typical transaction might include not only names, e-mail addresses and physical address and phone number, but also passwords and personal identification numbers. The incredible growth of the Internet has excited businesses and consumers alike with its promise of changing the way to live and work. It's extremely easy to buy and sell goods all over the world while sitting in front of a laptop. But security is a major concern on the Internet. Especially, when using it to send sensitive information between parties. There are various types of information that are not concerned for everyone such as: Credit-card information, Social Security number, Private correspondence, Personal details, Sensitive company information, and Bank-account information.

Encryption can be an effective method of protecting information, and is widely used for data security in many applications. Cryptanalysis is used for discovering encryption methods and decoding encrypted messages, and can be used to compromise data security. Certain encryption methods are more susceptible to cryptanalysis attacks than others. Systems that employ an encryption mechanism for data security should be aware of its susceptibility to cryptanalysis. This paper has presented the design and implementation of the new encryption algorithm. The motive of the development of this new encryption algorithm is to improve performance parameters. Avalanche effect and execution time are of main concerned with results comparison. The rest of the paper is organized in the following sections. Section 2 is the literature survey and problem identification. Section 3 explains proposed work. Section 4 explains the Results Comparison, conclusion.

II. Literature Survey and Problem Identification

Cryptography technique is used for hiding messages in the form of a cipher, but brute force attack is the main drawback of the cryptography technique. It's known that modern methods are less affected by brute force attack because of the usage of keys. At present there are so many algorithms that combine the process of scrambling of bits and substitution boxes resulting in high avalanche effect [1]. There are various functions available to perform encryption and decryption like matrix operation, logical operation, feistel structure, mathematical operation etc. In matrix function revision was done on the Hill cipher by developing an iterative procedure [2]. The procedure defines different type of matrix operation like the plain text matrix is multiplied with the key matrix on one side and with its inverse on the other side; furthermore, the plain text matrix is mixed thoroughly by using mixing function. At last, the plain text matrix is modified by using the XOR operation between the plain text matrix and the key metrics. At the start of the cryptography technique alphabetical cipher technique has been used for increasing confusion in messages, but there are some drawbacks that are associated with alphabetic techniques like concealment of key and plaintext [2]. [3] Proposed an encryption technique that

is the combination of both classical encryption as well as modern technique, generally this type of technique referred as hybrid technique. [5] Developed a block cipher by introducing a pair of keys-one as a left multiplicand of the plaintext and the second one as a right multiplicand of the plaintext. The same utilizes different type of character code like EBCDIC code for converting characters into decimal numbers and using math function like mod 256. In the same, iterative procedure and permutation function is used to produce the cipher text. The avalanche effect, execution time and the cryptanalysis can be used to measure the performance of any encryption algorithm. [6] Shows comparison results between different type of performance parameter like CPU time, memory, and battery power, these parameters is calculated by existing various encryption algorithm Encryption algorithms play a main role in information security systems. It provides an evaluation of six of the most common encryption algorithms namely: AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. [7] Analyzed the time-consuming of the known cryptographic algorithms: triple-DES, AES and RSA. In this they designed a new timing evaluation model based on random number generating mechanism. In this model for evaluation, there are two evaluating modes: different plaintexts in the same key (DPSK), the same plaintext in different keys (SPDK). As the basis of the evaluating model, the plaintext and the corresponding key are both generated by random numbers. The results show that, under the same key length and for the same size of the processed data, RSA is about several hundred times slower than AES, triple-DES is about three times slower than AES, and there are other runtime characteristics which further highlights the difference between these three cryptographic algorithms and provides a reference value for people's rational using.

Problem Identification: From the study of the previous research it is analyzed that there are so many issues in the existing algorithms where improvements required. In order to apply an appropriate technique in a particular application it's required to know these issues. All the issues are described as follows.

Execution time of algorithm directly depends on the functionality of the algorithm and it's clearly defines that more complex structure originates poor execution time. Security of the data directly depends on the key length, higher key length will provide higher security but it can increase the execution time of the algorithm so it is very important that what should be the key length and how execution time got controlled, if selected key length is higher. Avalanche effect is a desirable property of any encryption algorithm, in this a small change in either the plaintext or the key, produces a significant change in the cipher text. So it can play an important role in security issue. Another issue is the memory utilization because different encryption algorithms require different memory size for implementation. This memory requirement depends on the number of operations to be done by the algorithm. It is desirable that the memory required should be as small as possible. Selection of operation is also responsible to increase or decrease the overall performance of the proposed algorithm.

III. Proposed Work

Here the proposed system design is divided into two phases; phase 1 and phase 2. Both phases are shown in fig. 1 and fig. 2.

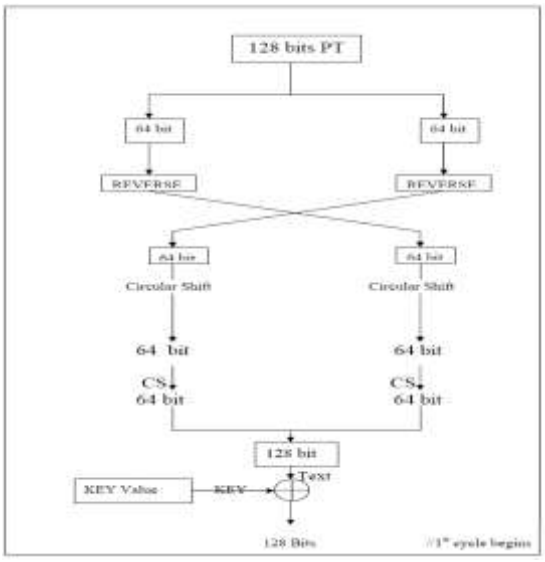

Figure 1: system architecture of proposed algorithm in phase 1

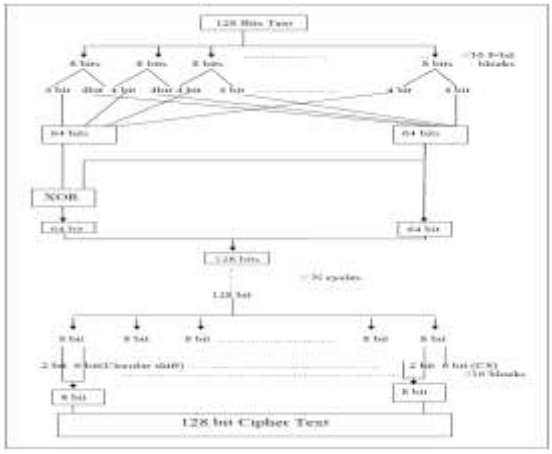

Figure 2: system architecture of proposed algorithm in phase 2

1. Encryption Process of Proposed Algorithm: - Proposed algorithm is divided into two phases, phase 1 and phase 2.

1.1 Step in the Phase 1

1. Take any 128 bit plain text.
2. Now divide this plain text into 2 parts, 64 bits each.
3. Reverse each part and then swap both.
4. Now apply a circular shift operation on both the parts twice and again combine parts to get 128 bit data.
5. Select 128 bits key value.
6. Perform XOR operation between plain text and key value and the final results should be in text data form.
7. Phase 1 is completed.

1.2 Step in the Phase 2

1. The 128 bits obtained after key mixing are divided into 16 equal parts of 8 bits each.
2. Again divide each 8 bit block into 2 parts of 4 bits each.
3. Now combine all the left 4 bit blocks to get a 64 bit block and perform the same with the right ones to get another 64 bit block.
4. XOR both the 64 bit blocks. And the output is combined with the right 64 bit block (without any change) to obtain 128 bit text.
5. Repeat the process 1 to 4 for N number of cycles.
6. Then the final 128 bits are divided into 16 blocks of 8 bits each.
7. Each 8 bit block is then split into 2 parts, of 2 bits and 6 bits, and circular shift is performed on the last 6 bits of each block.
8. Combine the 2 bit part and the modified 6 bit part to get 8 bit block (16 blocks in all).
9. These blocks are combined to finally obtain a 128 bit cipher text.
10. Exit.

2. Decryption Process of Proposed Algorithm: Decryption is the just reverse process of the encryption. Here decryption process is also divided into two phases, phase 1 and phase 2.

2.1 Step for Phase 1

1. Select 128 bits cipher text.
2. The 128 bits cipher texts are divided into 16 equal parts of 8 bits each.
3. Each 8 bit cipher block is then split into 2 parts, of 2 bits and 6 bits.
4. Apply reverses circular shift on the second part of 6 bits
5. Combine the 2 bit part and the modified 6 bit part to get 8 bit block (16 blocks in all).
6. These blocks are combined to finally obtain a 128 bit cipher text.
7. Now divide this cipher text into 2 parts, 64 bits each, left and right.
8. XOR both the 64 bit blocks. And the output is a 64 bit block (without any change) to obtain left 64 bit block 128 bit text.
9. After performing the XOR operation we will get both parts left and right parts of 64 bits each.
10. Now again divide both left and right 64 bits part into 4-4 bits part respectively.
11. Rearrange these 4 bits part in reversely to get original 64 bit parts (see architecture).
12. Finally combine all these blocks to get 128 bits.
13. Repeat process 7 to 12 for N number of cycles.

14. Then the final 128 bits will produce.
15. Phase 1 is completed.

2.2 Step for Phase 2

1. Select 128 bits key value.
2. Perform XOR operation between 128 bits key values and 128 bit cipher text (final results of phase 1).
3. Now divide this cipher text into 2 parts, 64 bits each.
4. Now apply the reverse circular shift operation on both the parts twice
5. Swap both parts and apply re-reverse operation on both parts.
6. Finally combine both parts to get 128 bit plain text data.
7. Exit.

3. Advantage of Proposed Model:-

- Efficient
- Robustness
- Secured
- Simple

IV. Result Comparison

Here two different parameters are used to evaluate performance of the proposed system. First is avalanche effect and second is encryption and decryption time. The proposed system is built on dot net platform, Comparison of results performed between proposed algorithm and two existing algorithms. The observations were made using a personal computer with the specifications of Intel Pentium Dual Core E2200 2.20 GHz, 1 GB of RAM and Window-XP SP2 as the platform. At the time of results evaluation, plain text and key value both were written randomly. To calculate encryption and decryption time proposed system run so many times on different-different text file with the same key value and then final results were observed. Similarly, in the case of avalanche effect evaluation, after running proposed systems several times, the final results are the same i.e. in numeric form.

1. Avalanche Effect Comparisons: Avalanche Effect is the important property of security in cryptographic algorithms where, if an input is changed slightly (changing a single bit) the output changes significantly. In our case, we have chosen two different input plain text as "**welcometomycolle**" and "**welcometomycollewelcometomycolle**"
Because of key length used in existing algorithm, "proposed algorithm" and "A Block Cipher Having a Key on One Side of the Plain Text Matrix and its Inverse on the Other Side" are using 128 bits key length where "A Modified Hill Cipher Involving a Pair of Keys and a Permutation" is using 256 bits key length. Changing one bit from the plain text, we get "**welcometomycolla**" (on changing me to a) for "proposed algorithm" and "A Block Cipher Having a Key on one side of the Plain Text Matrix and its Inverse on the other side. Changing one bit from the plain text, we get "**welcometomycollewelcometomycolla**" (on changing e to a) for "A Modified Hill Cipher Involving a Pair of Keys and a Permutation".

1.1 A Block Cipher Having a Key on one side of the Plain Text Matrix and its Inverse on the other side

Plain Text: welcometomycolle
00001100000011100000101010100010000001001100000000000000100110000000101000100011010110000010100000000000011110000100000000000000
Change in Plain Text: welcometomycolla
00001000000101000001010101001100000000010101000100000000001100000000110001001110111000001101000000000000111000011000000001000000
Avalanche Effect: 18

1.2 A Modified Hill Cipher Involving a Pair of Keys and a Permutation

Plain Text: **welcometomycollewelcometomycolle**

00000000000000000000000000000000000000000000000000010000000000000000000000000000
00100000000000011010000000000000000000000010011000000000001010011000000000101011000000000000010
0000001000110100011000100000100000000110100000010111001010010111110010110010

Change in Plain Text: welcometomycolle welcometomycolla

1000000100000010000001000000100001110000000000111000110000011100010100011000110000001111100
00100111111110011010000000000000000000000010011000000000001010011011000011101011000000111111O
0000001111110100011000101100101111000110100111101110010111111111110010110010

Avalanche Effect: 59

1.3 Proposed Algorithm

Plain Text: welcometomycolle

0101101010100000001011110011101100001111111110001101111111010000010011000100110010000111111
00000100111000101111110000111111000101

Change in Plain Text: welcometomycolla

1010011111111110111101111111110111010000000111110000100000111111111100111011001101110000O
1111101100011101000000111100011111010

Avalanche Effect: 96

Table 1: Avalanche Effect Comparisons

Encryption Technique	Avalanche Effect
"A Modified Hill Cipher Involving a Pair of Keys and a Permutation"	**18**
"A Block Cipher Having a Key on One Side of the Plain Text Matrix and its Inverse on the Other Side".	**59**
"Proposed Algorithm"	**96**

A graphical representation of the TABLE 1 is shown in Fig.3 blue lines represent a comparison between "Existing Algorithm" and "**Proposed Algorithm"**. According to the graph, there is a tendency that the avalanche effect increases with file size. But the total avalanche effect through Proposed Algorithm is higher than avalanche effect for comparing algorithms.

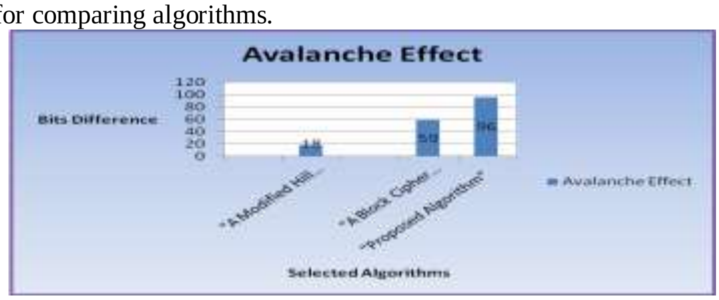

Figure 3: avalanche effect comparisons

2. Execution Time Comparison: Here, the proposed algorithm (with 128 bit block size in this) and selected algorithms have been implemented in a number of different data files like text, pdf and image in varying types of content and sizes of a wide range. But here we are using result of text file. Encryption and Decryption time of Various Text file comparisons shown in TABLE 2 and TABLE 3 respectively.

Table 2: Encryption Time Comparison between Proposed Algorithm and Selected Existing Algorithm on Various Text File

S. NO	FILE SIZE in KB	A Modified Hill Cipher Involving a Pair of Keys and a Permutation	A Block Cipher Having a Key on One Side of the Plain Text Matrix and its Inverse on the Other Side	Proposed Algorithm

1	10	11	9	1
2	70	14	12	5
3	300	22	19	13
4	700	43	37	20

Table 3: Decryption Time Comparison between Proposed Algorithm and Selected Existing Algorithm on Various Text File

S. NO	FILE SIZE in KB	A Modified Hill Cipher Involving a Pair of Keys and a Permutation	A Block Cipher Having a Key on One Side of the Plain Text Matrix and its Inverse on the Other Side	Proposed Algorithm
1	10	11	9	1
2	70	14	12	5
3	300	22	19	13
4	700	43	37	20

A graphical representation in the TABLE 2 and TABLE 3 is shown in Fig.4 and Fig.5 with blue line and orange line for encryption and decryption time of "Existing algorithm**"** and the green line is for "Proposed Algorithm". According to the graph, there is a tendency that encryption/decryption time for proposed algorithm, and compared algorithms increases with file size. But the required time for the encryption/decryption through proposed algorithm is much smaller than the encryption / decryption time for another two.

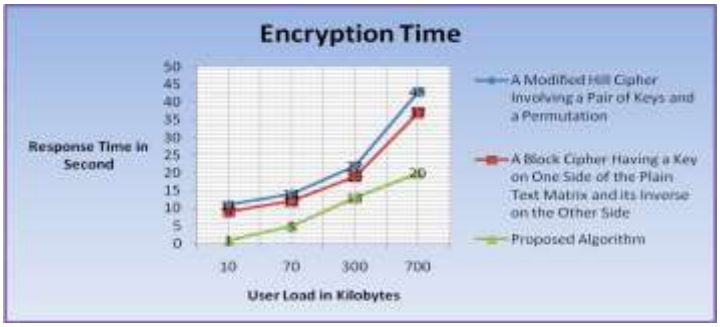

Figure 4: encryption time comparison between proposed algorithm and selected existing algorithm on various text File

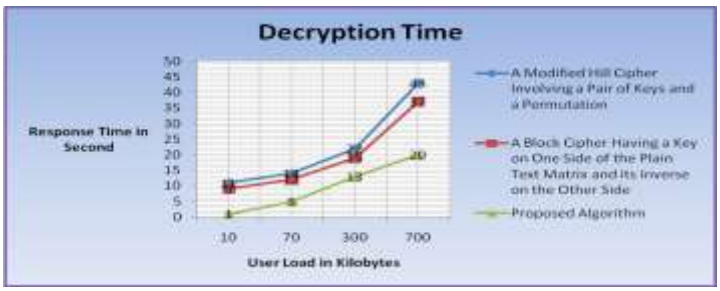

Figure 5: decryption time comparison between proposed algorithm and selected existing algorithm on various text file

V. Conclusion

This paper has suggested and developed encryption algorithm and encryption system using a block cipher symmetric technique. With the above, the performance between existing algorithm and suggested algorithm has examined .Suggested algorithm has used logical functions like XOR and circular shift. Due to these operations suggested algorithm becomes more secure because shifts and XOR cause changes to be propagated left and right, and change in single bit results propagation in the full word, in about 4 iterations. Measurements showed the diffusion was complete at about six iterations. It is quite easy and reducing response time as shown in TABLE 2 and TABLE 3. The hacker cannot see the original key even if he knows the plaintext

and the cipher text. The suggested algorithm will help to reduce response time taken by them for the authentication protocols. The suggested system ensure without any problem on the decrypt of the text, image or any other type of data, and. It is efficient and useable for the security in the different type of network. The selected algorithms and Proposed Algorithm were tested. Several points can be concluded from the Experimental results. Firstly; there is no significant difference when the results are displayed either in hexadecimal base encoding or in base 64 encoding. Secondly; in the case of changing packet size, it was concluded that proposed Algorithm has better performance than other common encryption algorithms used. Thirdly; the avalanche effect of the proposed algorithm is producing very high as comparison other algorithm as shown in TABLE 1. Fourth; memory utilization of proposed algorithm is also better than the other algorithm.

Future Enhancement: To achieve higher security proposed algorithm will include more complicated process and will increase number of logical operations in such a way where performance cannot be decreased. Increase Key length is also future work.

References

[1] Ramanujam and Marimuthu Karuppiah "Designing an algorithm with high Avalanche Effect" IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011

[2] Dr. V. U. K. Sastry, Prof. D. S. R. Murthy, Dr. S. Durga Bhavani "A Block Cipher Having a Key on One Side of the Plain Text Matrix and its Inverse on the Other Side" published in International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October, 2010 1793-8201.

[3] Fauzan Saeed and Mustafa Rashid " Integrating Classical Encryption with Modern Technique" IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010

[4] V. U. K. Sastry, D. S. R. Murthy, S. Durga Bhavani, "A Block Cipher Involving a Key Applied on Both the Sides of the Plain Text", International Journal of Computer and Network Security (IJCNS), Vol. 1, No. 1, pp. 27 -30, Oct. 2009.

[5] V. U. K. Sastry, V. Janaki, "A Modified Hill Cipher with Multiple Keys", International Journal of Computational Science, Vol. 2, No. 6, 815 – 826, Dec. 2008.

[6] Diaa Salama Abdul. Elminaam1, Hatem Mohamed Abdul Kader2 and Mohie Mohamed Hadhoud3"Performance Evaluation of Symmetric Encryption Algorithms" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008

[7] Yan Wang and Ming Hu "Timing evaluation of the known cryptographic algorithms" IEEE International Conference on Computational Intelligence and Security 2009

[8] B. Schneier, Applied Cryptography, John Wiley & Sons, New York, 1994.

[9] B. Schneier, "Data Guardians," MacWorld, Feb 1993, 145-151.

[10] William Stallings, "Cryptography and Network Security: Principles & Practices", second edition.

[11] Hardjono, "Security in Wireless LANS and MANS," Artech House Publishers 2005.