ISSN:0975-9646

A Novel Approach to Design Confidentiality Encryption Algorithm

Shalinee Singh Baghel
Department of Computer Science
Truba Institute of Science & IT
Bhopal, India

Prof. Amit Saxen
Department of Computer Science
Truba Institute of Science & IT
Bhopal, India

Dr. Manish Manoria
Director
Truba Institute of Science & IT
Bhopal, India

***Abstract*-- Today, everyone in the world is dependent on internet; it is required for communication, information storage, data transmission, e-business, entertainment, knowledge gathering and many more. The issue with this system is security, it is always required doing the above things securely. Internet is a public network and the most unsecure network. Many algorithms have been evolved to fulfil the above requirement. This paper has lighten many such algorithms and discussed the problem in such algorithms also this paper have proposed their own algorithm and its implementation result proves it the optimal solution for the above problem.**

***Keywords*-- Computer Security, Confidentiality, Name based Algorithm, Encryption Decryption Algorithm.**

I. INTRODUCTION

To secure the digital data, many cryptographic algorithms have been structured and developed. Whenever a word security comes, it involves three words: authentication, integrity and confidentiality. Confidentiality means to ensure that information will be transmitted or stored secretly means no one can read or understand the secret text. Integrity on the other part ensures that data does not alter during transmission or the time of storage and authentication ensure that only authenticated parties communicate or stored the data.

This paper pays attention on confidentiality algorithms. There are two different categories of algorithms that are used to ensure the confidentiality. First encryption/decryption algorithm and next is stegnography algorithm.

Encryption/ Decryption algorithm shuffles the secret text in such a manner that no unauthorized person can read it. This shuffling is based on key such that it rearrange only when if the same key is applied to the other end where rearrangement of secret text is required. Because only authenticated parties know the key therefore secret text cannot be understand by any unauthorized user.

In encryption algorithm, a secret text and a key is passed to the encryption algorithm and as a result it generates cipher text. This cipher text is unreadable to any unauthorized person don't have a key. Now at the other end this cipher text passed to the decryption algorithm with the same key used in encryption algorithm and generates the original secret text.

Many algorithms have been designed to implement encryption and decryption process but there is always a competition going to develop an algorithm which should be time efficient and secure too. Many pioneer have tried to develop such algorithms but a common problem have been found that is algorithms tries to improve security in it but degrades the time efficiency, and if improves the time efficiency than degrades the security.

Authors have discussed many such algorithms in paper [1]. In paper [1], Authors had reveal some facts on latest algorithm on this called NBA where it is found that this algorithm is time efficient but not secure to use for place where confidentiality required. This paper also proposed its own new algorithm on encryption/decryption and proved with its implementation that it is the best rectification among all.

II. PROPOSED WORK

Proposed algorithm is a block cipher symmetric key encryption algorithm. It divides the plaintext into 128 bits equal chunks and performs the encryption procedure on each chunk. It works on 128 bit key which make it secure and harder for intruder to recover the key. It requires 2^{128} combination to break the key. Block Diagram of Encryption is shown in Fig. 1

Steps for Proposed Encryption Algorithm:

1. First the complete plaintext is converted into binary form.
2. Now, the binary text (plaintext) is divided into 128 bit equal size chunks. If the last chunk having less number of bit then padding of zero will be performed.
3. Also take a 16 character key as an input by user.
4. Next, a random number is generated with the help of key. Process of generating a random number are as follows:
   a. Add all the integer value of characters in the key.
   b. Now, calculate the mod 128 operation on the result of step a) and result is a random number.
5. Convert the key into 128 bit binary form.
6. Now repeat the following operation to each 128 bit chunk
   a. Calculate XOR of each bit in chunk to its next random number position bit.
   b. Now, calculate XOR with 128 bit key. Now again calculate XOR of each bit in chunk to its next random number position bit.
   c. Result comes out from the last step is the cipher text of given chunk.
7. Finally, convert all the binary cipher text in to 8 bit character form.
8. Exit

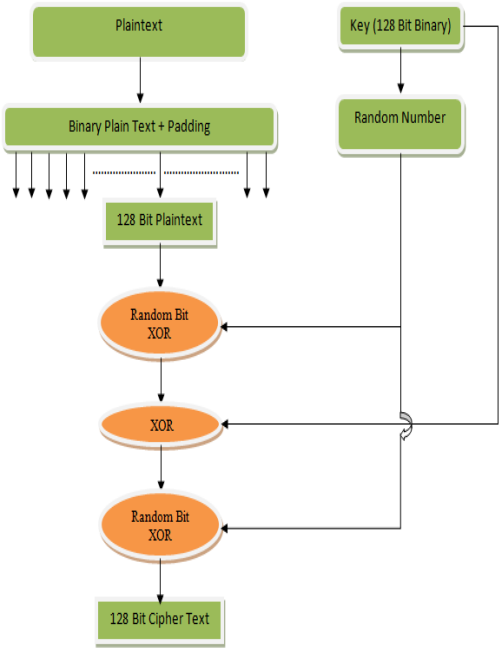


Fig.1 Encryption Block

Decryption of proposed algorithm is same, where input is cipher text and same key used for encryption.

III. RESULT AND ANALYSIS

This section discussed in details the strength and efficiency of proposed encryption/decryption algorithm. For this authors have implemented the proposed algorithm and compare it with NBE algorithm discussed in [1] to check the robustness of proposed algorithm. Authors have calculated the avalanche effect and perform key analysis to check the efficiency against timing.

A. Analysis of Avalanche Effect:

Avalanche effect is one of the parameter used to calculate the internal robustness of proposed algorithm. According to avalanche effect a change of single bit in a key change the cipher text up to 50%. The algorithm closed to this condition consider more efficient than other.

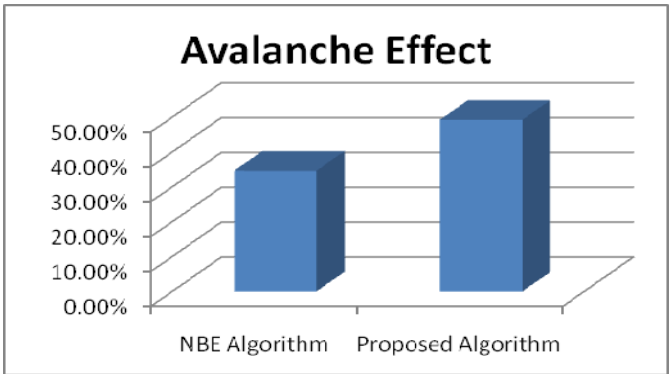
Table 1 showing the avalanche effect of proposed algorithm.

Table 1 Avalanche Effect of Proposed and NBE algorithm

File Size in KB	**Avalanche Effect**	
	NBE Algorithm	**Proposed Algorithm**
Single bit change in key	34.6%	49.24%

Graph 1 represents the difference of avalanche effect in both the algorithm graphically.

It is clearly visible that proposed algorithm is more efficient than the other algorithms.



Graph 1. Avalanche Effect of Proposed and NBE algorithm

Key Analysis

Key analysis is a again another important parameter to evaluate the strength of an algorithm. More bits in key makes difficult for intruder to break.

Proposed algorithm uses 128 bit key which take 2^{128} combination to break which is impossible for a super computer to break in a suitable time.

Time Analysis

Time efficiency is another parameter which shows how efficient this algorithm is to use in any real time circumstances. It is always required to do complete encryption/ decryption process with minimum delay.

Table 2 and Table 3 show the timing of process during encryption and decryption.

Table 2 Throughput and Execution Time of Proposed Encryption algorithm

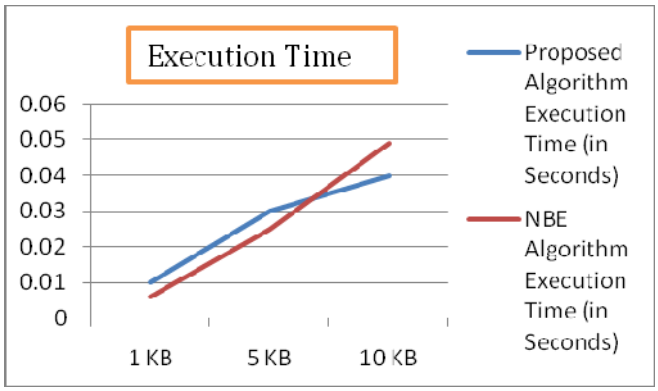
File Size (in KB)	**Proposed Algorithm**	
	Execution Time (in Seconds)	Throughput (Bytes/ Second)
1 KB	0.010	1,02,400
5 KB	0.030	1,70,666
10 KB	0.040	2,56,000

Table 3 Throughput and Execution Time of Decryption Encryption algorithm

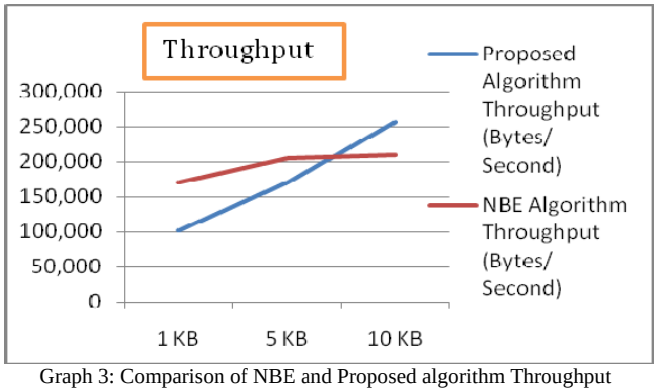
File Size (in KB)	**Proposed Algorithm**	
	Execution Time (in Seconds)	Throughput (Bytes/ Second)
1 KB	0.010	1,02,400
5 KB	0.030	1,70,666
10 KB	0.040	2,56,000

Again it is clearly concluded from Table 2 and Table 3 that proposed algorithm is time efficient and can be used for real time circumstances.

Graphical comparison of proposed encryption process and NBE algorithm is presented in Graph 2 whereas Graph 3 shows the throughput comparison with NBE Algorithm



Graph 2: Comparison of NBE and Proposed algorithm execution Time



Graph 3: Comparison of NBE and Proposed algorithm Throughput

IV. CONCLUSION

With the rapid development in the modern technology, security plays a vital role. It is important to update and recalculate the performance of existing algorithm that they fulfill the current needs. This paper discussed the problem that is running in the existing cryptographic algorithm. Authors also presented a new design for encryption/decryption algorithm and with its implementation also proved that proposed solution is the optimal solution. With reference to implementation results it is easily concluded that proposed algorithm have better avalanche effect which shows it strength against various attack also it is time efficient which makes it comfortable to use where Ad-Hoc network is required. Also its key size is large enough so that it cannot be breakable in reasonable time. It requires 2^{128} combination to guess the key.

REFERENCES

[1] AasifHasan, Neeraj Sharma," A New Method Towards Encryption Schemes (Name-Based-Encryption Algorithm)", in ICROIT-2014.

[2] M .Chapple., M Solomon,: " Information Security Illuminated " First Edition. Jones and Bartlett Publishers, (2005), USA.

[3] Ajay Kakkar, M. L. Singh and P.K. Bansal, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network, " International Joural of Engineering and Technology Volume 2 No. 1, January, 2012, IJET Publications UK.

[4] MohiuddinAhmed, T. M. Shahriar Sazzad and Md. Elias Mollah, " Cryptography and State-of-the-art Techniques, " in IJCSI International Joural of Computer Science Issues, Vol. 9, Issue 2, No3, March 2012.

[5] Abdel-Karim Al Tamimi, "A Performance Comparison of Data Encryption Algorithms, " Published by Washington university in St. Louis

[6] Neeraj Khanna, Joel James,Joyshree Nath, Sayantan Chakraborty, Amlan Chakrabarti and Asoke Nath: "New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm" Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 03-06 June 2011, Page 125-130.

[7] Vishwa Gupta, Gajendra Singh, Ravindra Gupta, "Advance cryptography algorithm for improving data security", in IJAR of Computer Science Issues, Vol. 2, Issue 1, January 2012.