Volume 4, Issue 9, September 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A New Encryption Algorithm to Increase Performance & Security through Block Cipher Technique

Surabhi Shah
CSE RGPV,
Bhopal, India

Megha Singh
CSE RGPV,
Bhopal, India

Neha Joshi
CSE RGPV,
Bhopal, India

Abstract— Data Security is the process of providing protection to the important information transferred over the network. Cryptography plays a very vital role in enhancing the security of any information or the data .This dissertation work aim to design and implement such a system that provides complete authenticity and confidentiality over the open network. The proposed system works over the implementation of new block cipher cryptography along with its comparison to other block cipher algorithm over efficiency.

Keywords— Encryption, decryption, cryptography, MSA, AES

I. INTRODUCTION

Information is an asset, which like other important business asset values to an organization. And consequently needs to be suitably protected. Information can be created, lost, processed, stored and corrupted. Cryptography plays a very important role in securing data over the network. Cryptography comprises of some basic terms:

- Confidentiality (privacy- Assurance)
- Authentication (claimed user only)
- Integrity (data is not disturbed by an unauthenticated person)
- Non-repudiation (denial protection)
- Access Control (prevents misuse of resource)
- Availability(performance, non-erasure)

1. Cryptography basically works over two algorithms Encryption and Decryption algorithm. Encryption converts plain text in to cipher text i.e. readable data in to unreadable data, where as Decryption performs the vice versa. This Encryption-Decryption process is performed with the help of a unique key. Depending over the key, algorithms is been divided in to two major categories- Symmetric key encryption and asymmetric key encryption. Symmetric algorithm uses only one key for encryption and decryption, such key is considered as private key. On the other hand Asymmetric algorithm uses two keys one for encryption (public key) and one for decryption (Private Key).In symmetric key or secret key encryption, strength of key is depended over the size of the key used. For the same algorithm, encryption using longer key is harder to break than the one done using smaller key. Asymmetric Encryption techniques are almost 1000 times slower than symmetric technique, because they require more computational process. Thus there is a need for an algorithm to have good efficiency along with less response time, less battery power consumption and less memory utilization. Hence the proposed approach tries to work over these factors.

II. RELATED WORKS

This section describes related works, "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" [1]. In this paper, comparison is been made between block size used in DES and AES. Data Encryption Standard (DES) uses 64 bits block size as well as 64 bits key size that are vulnerable to brute force attack. But for both efficiency and security, a larger block size is desirable. The Advanced Encryption Standard (AES) that uses 128 bits block size as well as 128 bits key size was introduced by NIST. In this paper an effect in security increment through AES methodology was showed. To do this an algorithm was proposed which is higher secured than Rijndael algorithm but less efficient than that. There was negligible efficiency difference between the Rijndael and the proposed algorithm. The difference was that Rijndael algorithm starts with 128 bits block size and then increases the block size by appending columns, whereas his algorithm starts with 200 bits.

In this paper"A new Symmetric Key Cryptography Algorithm using extended MSA method: DJSA Symmetric Key algorithm" [2]. Author introduced a new symmetric key cryptographic method for encryption as well as decryption of any file e.g. binary file, text file or any other file using a random key square matrix containing 256 elements, this was called MSA algorithm. The weak point of MSA algorithm is that if someone applies the brute force method then it has to give a trial for factorial 256 to find the actual key matrix. Later on author considered the size of the key matrix to be 65536 and in each cell store 2 characters pattern instead of 1 character. But this was intractable problem. After that author introduced a square matrix of size 256 by 256 where in each cell there are all possible 2-lettered words. The total

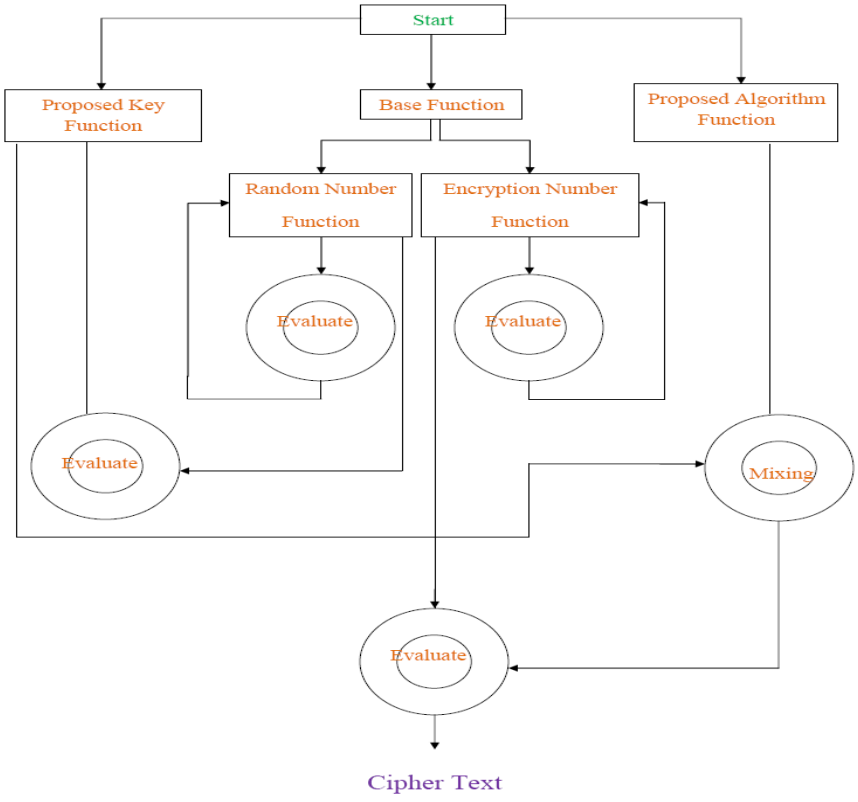
number of words possible 65536.The maximum length of text key should be 16 characters long. In this paper they used a random key generator for generating the initial key and that key is used for encrypting the given source file.In the present work we use the maximum encryption number=64 and the maximum randomization number=64. The present work is basically the extension of MSA Algorithm. It has used the key matrix of size 256x256x2. This key may be generated in 65536! Ways. So in principle it will be difficult for anyone to decrypt the encrypted text without knowing the exact key matrix. Our method is essentially block cipher method and it will take more time if the files size is large and the encryption number is also large. The merit of this method is that it is almost impossible to break the encryption algorithm without knowing the exact key matrix.

III. PROPOSED WORK

In this section I am proposing a work based on block symmetric cryptography concept, providing solution for the problem discussed in the papers. Generally symmetric cryptography algorithm is divided into two parts

- first one is stream cipher where bit by bit encryption performed and
- Second is block cipher where encryption performed on block of bits.

Here I am using block cipher symmetric cryptography technique because of its efficiency and security. In this a common key is used between sender and receiver, which is known as private key. Below fig shows the simple architecture of proposed System. Architecture is divided in to three major blocks. Block-1 is proposed key evolution block, block-2 is base function block and block-3 is the proposed encryption algorithm. In the proposed system base function block is firstly executed to calculate random number function and encryption number function, after that proposed key evolution block executed because to evolutes key it is required random number, finally proposed algorithm block executed to generated cipher text. Basically In this algorithm block based method are using and number of round of the proposed algorithm are calculating by encryption number function. The length of the proposed key blocks have 256 bits, contains all possible word comprising of number (n) of characters each generated from all characters whose ASCII code is from 0 to 255 in a random order. Proposed algorithm is possible for files such as Microsoft word file, excel file, text file, images file, pdf files, audio files and many more.



IV. CONCLUSIONS

The difference of efficiency between proposed and the existing algorithm is very high. The security, efficiency, CPU Utilization is of primary concern. The proposed encryption algorithm is very simple, direct mapping algorithm using some logical operation. This cipher text generation provides a good strength to the encryption algorithm, with the increasing importance of video security more enhanced better methods are required to improve security in a broad way. As such it is quite essential to improve our algorithms performance in future. Here a new approach for data security using block cipher symmetric key cryptography was proposed. This new approach uses the concept of encryption number and random number from paper to enhance the complexity of key. This results increases efforts for brute force attacks. The proposed approach also uses the logical shift and X-or operations to reduce the CPU utilization and processing time of algorithm. The proposed system successfully encrypt and decrypt the files in Text, Pdf, xml, image, mp3 format.

ACKNOWLEDGMENT

I sincerely thank MS. Megha Singh (Guide), Mr.Jitendra Choudhary (Co-guide) and Mr.Aditya Sharma for supporting and contributing there valuable points in my Paper.

REFERENCES

[1] [1]Md. Nazrul Islam, [1]Md. Monir Hossain Mia, 2Muhammad F. I. Chowdhury, 3M.A. Matin "*Effect of Security Increment to Symmetric Data Encryption through AES Methodology"* Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing

[2] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath "*A new Symmetric Key Cryptography Algorithm using extended MSA method: DJSA Symmetric Key algorithm"* 2011 International Conference on communication Systems and Network Technologies.

[3] Diaa Salama Abdul Minaam1, Hatem M. Abdual-Kader2, and Mohiy Mohamed Hadhoud2 "*Evaluating the Effects of Symmetric Cryptography Algorithms on power consumption for Different Data types"* International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept. 2010

[4] 1.Vishwa gupta,2. Gajendra Singh ,3.Ravindra Gupta *"Advance cryptography algorithm for improving data security"* Volume 2,Issue 1, January 2012 ISSN:2277 128X International Journal of Advance Research in Computer Science and Software Engineering.

[5] Krishna Kumar Pandey Vikas Rangari Sitesh KumarSinha "*An Enhanced Symmetric Key cryptography Algorithm to Improve Data Security*" International Journal of Computer Applications (0975 – 8887) Volume 74– No. 20, July 2013

