# An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security

Krishna Kumar Pandey
Assistant Professor
AISECT Bhopal

Vikas Rangari
M.Tech Scholar (CSE)
AISECT Bhopal

Sitesh KumarSinha
Professor
AISECT Bhopal

## ABSTRACT
This work uses enhanced symmetric key encryption algorithm, in which same structure of encryption and decryption procedure algorithm is used. In conventional encryption methods the key for encryption and decryption is same and remain secret. The algorithm uses key generation method by random number in algorithm for increasing efficiency of algorithm. The algorithm use key size of 512 bits for providing better security and it also provide the concept of internal key generation at receiver end on the basis of 512 bits key which will entered by the sender. This internal key will store in the sender end database and send to the receiver end by other path for preventing brute force attack and other harmful attacks on security. This algorithm is more efficient for large data where existing algorithms provides efficient encryption and decryption only for 2MB data. This work provides better speed in comparison to existing algorithms for large size of files with less overhead.

## Keywords
Information security, Encryption, Decryption, Cryptography, Brute force attack.

Before doing this work study of all the aspects on Information security using cryptography technique and various cryptography algorithms is done. This survey is very beneficial for us to understand how to remove loop hole of security of information in public network and how to improve the efficiency and security of proposed algorithm. After the detailed study of network security using cryptography, proposed work is developed. The research paper is distributed in four sections. In section-I, presents basic introduction about Information Security using cryptography, in section-II, Existing work on Information security using cryptography and various algorithms is discussed, section-III describes proposed work, section IV gives implementation details and in section V and VI presents conclusion and references.

## 1. INTRODUCTION

Cryptography has an important role for preventing private data from being stolen. Encryption and decryption are the synonym of Cryptography. Encryption is the process that converts plain text into cipher text by using encryption algorithms with key that process performed on sender end and decryption is the reverse process of encryption performed on receiver end [9]. The main feature of the encryption/decryption program implementation is the generation of the encryption key. Now a day, cryptography has many commercial applications. If anyone is protecting confidential information then cryptography provides high level of privacy of individuals and groups. However, the main purpose of the cryptography is not to only provide confidentiality, but also to give solutions for other problems like: Integrity of data, authentication and non-repudiation. Cryptography is the method that allows information to be sent in a secure form in such a way that the only receiver is able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is very difficult to find out the specific algorithm, because they must consider many factors like: security, the features of algorithm, the time complexity and space complexity. Figure 1 is representing conventional encryption model.

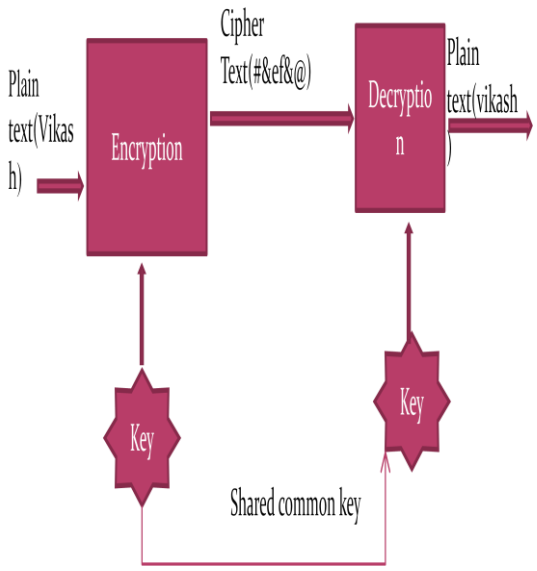


**Figure 1: A Simplified Model of Conventional Encryption**

Security Services: If any security algorithm providing security of information then following voices come in mind.

- Confidentiality
- Authentication
- Integrity
- Non-repudiation
- Access control Availability

## 1.1 CRYPTOSYSTEM

A cryptosystem is the ordered list of finite possible plaintexts, finite possible cipher text, finite possible keys, and the encryption and decryption algorithms .In this keys are important, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless (or even counter-productive) for most purposes. In some cases ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.

## 2. EXISTING WORK

This section describes existing work, "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" [1]. In this they are using a symmetric key method where they have used a random key generator for generating the initial key and that key is used for encrypting the given source file. In this method basically a substitution method is used where they take four characters from any input file and then search the corresponding characters in the random key matrix after getting the encrypted message they store this encrypted data in another file. For searching characters from the random key matrix they have used a method which was proposed by Nath in MSA algorithm. They are suggesting key matrix contains all possible words comprising of two characters each generated from all characters whose ASCII code is from 0 to 255 in a random order. The pattern of the key matrix will depend upon user entered text key. They have developed their own algorithm to obtain randomization number and encryption number from the initial text key. They have given a long trial run on text key and they have found that it is very difficult to match the above two parameters from 2 different text key which means if someone wants to break his encryption method then he or she has to know the accurate pattern of the text key. To decrypt any file any one has to know what is the key matrix which is use to find the random matrix theoretically one has to apply 65536! Trial run and which is intractable. They have apply method on possible files such as executable file, MS word file, MS excel file, MS access , FoxPro database, text file, image file, pdf file, video file, audio file, oracle database and they have found in all cases it giving 100% correct solution while encrypting a file and decrypting a file when file size is 2MB[1] **.** Some cover file to make the entire system full secured. In this section shows another newly developed technique named, "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" [10] is discussed. In this they describe about symmetric cipher algorithm which is much more similar to Rijndael. The difference is that, Rijndael algorithm start with 128 bits block size, and then increase the block size [10], whereas this algorithm start with 200 bits.

## 3. PROPOSED WORK

This section describes a new symmetric cryptography algorithm. This technique apply, presenting a random number for generating the initial key, where this key will use for encrypting the given source file using proposed encryption algorithm with the help of encryption number. Basically proposed technique gives the concept of substitution method which is using block based technique. In this technique multiple times message encrypting is possible. The proposed key blocks contains all possible words comprising of number (n) of characters each generated from all characters whose ASCII code is from 0 to 255 in a random order. The pattern of the key blocks will depend on text key entered by the user. This system is using 256*2=512 bit key size to encrypt a text message. To decrypt any file one has to know exactly what the key blocks is and to find the random blocks theoretically one has to apply $2^{512}$ trial run which is difficult for attackers. Initially this technique is only possible for some files such as Microsoft word file, excel file, text file. Proposed method is very secure from network attacks because of 256*2 bit key size and by attaching new concept of internal key generation on the basis of 256*2=512 bit key which will be entered by the sender. This internal key, will be send by the sender from other network path to the receiver for enhance security whenever attackers tried to attack on message.

## 3.1 SIGNIFICANCE OF ENCRYPTION APPROACH USED:-

By using symmetric encryption approach. The symmetric encryption approach is divided in to two types one is block cipher symmetric cryptography technique and another is stream cipher symmetric cryptography but here block cipher type is used because its efficiency and security is good as compared to other. Proposed technique uses a common key between sender and receiver, which is known as private key. Basically private key concept is the symmetric key concept, where plain text is converted into encrypted text known as cipher text using private key and cipher text is decrypted by same private key into plain text. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transform to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain private information [9].

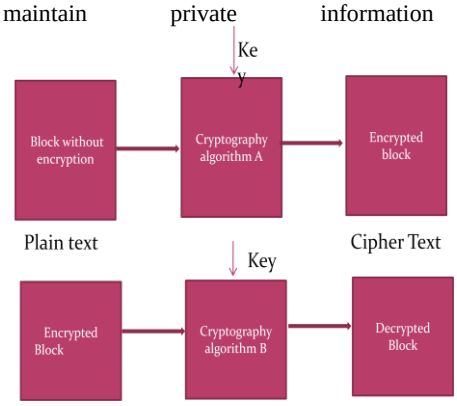


**Fig 2: Basic Concept for Symmetric cryptography**

## 3.2 PROPOSED ALGORITHM:

1. Define variable length from 1 to 64 and base value from 65 to 2.
2. To calculate random number following steps are used.
3. Calculate variable Total

$$Total = \sum_{m=1}^{n} ASCII\ code * b^m$$

= ways

4. Convert these xwyz into binary String
   (wxyz ⟶ 00011…)
5. Calculate Random Value
   RanValue = (w * b1 +x * b2 + y * b3 + z * b4)
6. Select another variable value V1 (Represent as a Random num.)
   V1 = Mod (Total, RanValue)
   V1 = xy

7. If V1 == 0 then V1 = RanValue1
   Else if V1 > 64 then
   V1 =V1 – 64

8. Calculate Encryption Number.
9. Calculate Encryption Value
   EncValue1 = (w * b1 +x * b2 + y * b3 + z * b4 )

10. Now select another variable V2 which will represent as an Encryption Number.

    V2 = Mod (Total, EncValue1)
    V2 = xy

11. If V2 = = 0 then
    Set V2 = EncValue1 Else if V2 > 64 then
    Set V2 = V2 – 64
12 . Finally we have Random Number and encryption number in V1 and V2 respectively.

12. Store binary string into table for next iteration.
14. Exit.

## 3.3 STEPS OF PROPOSED KEY GENERATION:

1. Select any private key of size 512 bits.
2. Size of selected key will be varying from 128 bits to 512 bits.
3. Choose any character from 0 to 255 ASCII code with binary string.
4. Use 512 bit key in length.
5. Make 4 blocks of 16 bytes likes Key_Block1, Key_Block2, Key_Block3, and Key_Block4.
6. Apply XOR operation between Block1 and Block4. Results will store in new Key_Block14.
7. Apply XOR operation between Block2 and Block14. Results will store in new Key_Block214.
8. Apply XOR operation between Key_Block413 and Key_Block2. Results will store in new Key_Block4132.
9. Repeat Step 7, 8, 9 till (random number / 4).
10. Store this key into database at sender end for using at receiver end.
11. Exit.

## 3.4 SIGNIFICANCE OF PROPOSED ALGORITHM:

- Reduce Time complexity.
- More Flexibility.
- Better Security.
- More Reliance on users.
- Binary string (for fast access).

## 4. IMPLEMENTATION DETAILS

This section describes all important aspects of implementation details**.** The result evaluation model shows that how implementation process works?

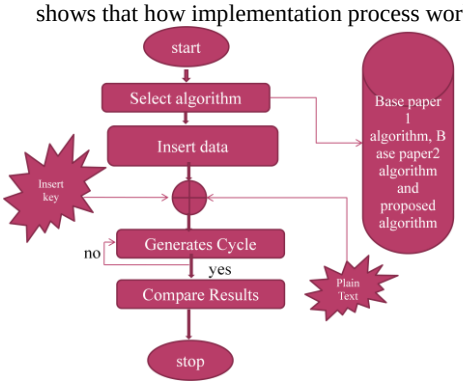


**Fig 3: Result Evaluation Model**

By using two parameters for execution time one is encryption value and second is decryption time which is shown in table 1 and table 2. This comparison shows the performance of proposed algorithm with the others. During processing, the content of the plaintext and the key are both written by the random number. For evaluation mode, there are two parameters: the number of evaluated plaintexts and the size of evaluated plaintext, where the number of evaluated plaintexts is the number of plaintexts that are generated randomly and the size of evaluated plaintext can be chosen from two kinds that are mentioned above. In this mode n cycles (i.e., the number of the evaluated plaintexts).In each cycle, same plaintexts are respectively encrypted by "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm (BP1)", "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" (BP2) and "Proposed Algorithm (PA)" by copying them. Finally, the outputs of the evaluation system execution time, and measured in numeric form. Actually, for an encryption algorithm, the execution time of encryption not only depends on the algorithm's complexity, but also the key and the plaintext have certain impact. After comparison the results that were obtained can be well represented in form of tables. Here, The Proposed Algorithm (with 512bit block size in this Paper) and "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm"[1](BP1) algorithm (with 128-bit block size) and "Effect of Security Increment to Symmetric Data Encryption through AES Methodology"[10](BP2) algorithm (with 128 -bit block size) have been implemented on a number of different data files like text, pdf ,MP3,Word file, Excel file and image varying types of content and

sizes of a wide range. But this only shows result of text file. Encryption and Decryption time of various text files comparisons shown in table 1 and table 2 respectively. Showing proposed algorithm through output screen.
This output shows which type of files are encrypted and decrypted through proposed method. By providing text box for entering key when user click on key generation button internal key will be generated and store this key in sender end database for future use.

**Table 1: - Encryption time comparisons of text file**

| Text size | Algorithm of Base paper 1 | Algorithm of Base paper 2 | Proposed Algorithm |
|---|---|---|---|
| | Execution time in seconds | | |
| 1.2 Mb.txt | 0:01:12 | 0:01:10 | 0:01:03 |
| 440 kb.txt | 0:00:20 | 0:00:18 | 0:01:11 |
| 150kb.txt | 0:00:15 | 0:00:13 | 0:00:06 |
| 28 kb.txt | 0:00:11 | 0:00:09 | 0:00:02 |
| 18 kb.txt | 0:00:10 | 0:00:08 | 0:00:01 |

**Table 2: - Decryption time comparisons of text files**

| Text size | Algorithm of Base paper 1 | Algorithm of Base paper 2 | Proposed Algorithm |
|---|---|---|---|
| | Execution time in seconds | | |
| 1.2 Mb.txt | 0:01:12 | 0:01:10 | 0:01:03 |
| 440 kb.txt | 0:00:20 | 0:00:18 | 0:01:11 |
| 150kb.txt | 0:00:15 | 0:00:13 | 0:00:06 |
| 28 kb.txt | 0:00:11 | 0:00:09 | 0:00:02 |
| 18 kb.txt | 0:00:10 | 0:00:08 | 0:00:01 |

This shows various text files by using base paper 1 algorithm, base paper 2 algorithm and Proposed algorithm and also shows there timings.
A graphical representation for the table 1 and table 2 is shown in figure 4 and figure 5 with blue line and red line for encryption time and decryption time of A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" [1] and "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" [10], respectively and 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 required time for the encryption/decryption through Proposed Algorithm is much smaller than encryption/decryption time for compared algorithms. The observations were made using personal computer with specifications of Intel Pentium I3 processor, 2GB of RAM and Window-XP SP3as the platform.

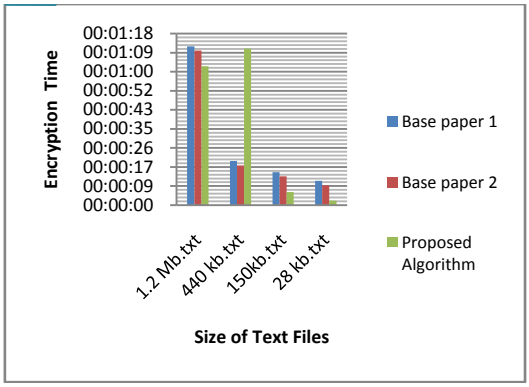


**Fig 4: Encryption time comparison of text files between various algorithms with proposed algorithm**

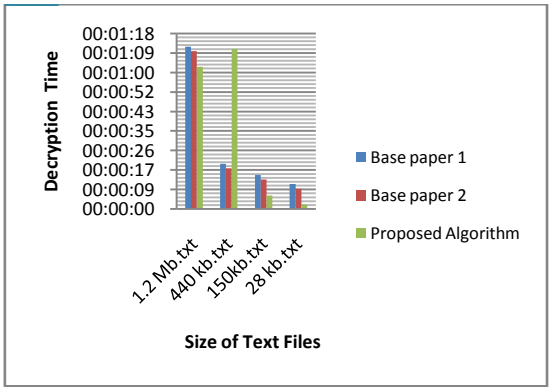


**Fig5: Decryption time comparison of text files between various algorithms with proposed algorithm**

## 5. CONCLUSION AND FUTURE ENHANCEMENT:

The result comparison shows that "proposed technique" gives better result as compared "BP1" and "BP2". When users are focusing on security then they can select proposed algorithm for better result with less time complexity. Proposed method is essentially block cipher method and it will take less time with providing security if the file size is large. Where existing algorithms efficiently works with 2 Mb file. The important feature of our proposed method is that it is almost impossible to break the encryption algorithm without knowing the exact key value because of internal key generation with the reference

of entered key. The proposed method for both encryption and decryption can be applied for any type of public application for sending confidential data and by sending internal key to the sender by using another secured path to the receiver. Proposed method prevents data from attackers and claim for less time complexity with large data. So it provides useful application in the field of network security.

## 6. REFERENCES

[1] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.

[2] Yan Wang and Ming Hu "Timing evaluation of the known cryptographic algorithms "2009 International Conference on Computational Intelligence and Security 978-0-7695-3931-7/09 $26.00 © 2009 IEEE DOI 10.1109/CIS.2009.81.

[3] Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas (USA) 12-15 July, 2010, Vol-2, and P-239-244.

[4] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.

[5] Neal Koblitz "A Course in Number Theory and Cryptography" Second Edition Published by Springer-Verlag.

[6] By Klaus Felten "An Algorithm for Symmetric Cryptography with a wide range of scalability" published by 2nd International Workshop on Embedded Systems, Internet Programming and Industial IT.

[7] Majdi Al-qdah & Lin Yi Hui "Simple Encryption/Decryption Application" published in International Journal of Computer Science and Security, Volume (1): Issue (1).

[8] T Morkel, JHP Eloff "ENCRYPTION TECHNIQUES: A TIMELINE APPROACH" published in Information and Computer Security Architecture (ICSA) Research Group proceeding.

[9] Text book William Stallings, Data and Computer Communications, 6eWilliam 6e 2005.

[10] Md. Nazrul Islam, Md. Monir Hossain Mia, Muhammad F. I. Chowdhury, M.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 978-0-7695-3263-9/08 DOI 10.1109/SNPD.2008.101 IEEE 2008.

[11] [Rijn99] Joan Daemen and Vincent Rijmen, AES submission document on Rijndael, Version 2, September 1999.