

## A Recent Study of Various Symmetric Key Based Cryptographic Methods

Vismita Jain<sup>1</sup>

<sup>1</sup>M.Tech IV Semester

Lord Krishna College of Technology Indore

[jainvismita@gmail.com](mailto:jainvismita@gmail.com)

Vijay Kumar Verma<sup>2</sup>

<sup>2</sup>Asst. Prof. CSE Dept.

Lord Krishna College of Technology Indore

[vijayvermaonline@gmail.com](mailto:vijayvermaonline@gmail.com)

---

**Abstract-***In network communication systems, exchange of information mostly occurs on networked computers, mobile phones and other internet based electronic gadgets. Various cryptographic techniques are used to achieve data security and privacy during communication systems over networks. These cryptographic techniques hide the original content of a data in such a way that the original information is recovered only through using a key known as decryption process. The objective of these cryptographic techniques is to secure or protect data from unauthorized access in term of viewing or modifying the data. Encryption can be implemented occurs by using some substitute technique, shifting technique, or mathematical operations. By applying these techniques we can generate a different form of that data which can be difficult to understand by anyone.. In this paper we proposed a recent study over various symmetric key based methods for encryption and decryption of text data. Our study includes some comparison parameter like key size, security level, modification etc.*

**Keywords:** *Symmetric, Encryption, Decryption, Scalability, Security, Plaintext, Chipper text.*

---

### I. INTRODUCTION

In network security, cryptography has a long history by provides a way to store sensitive information or transmit it across insecure networks (i.e. the Internet) so that it cannot be read by anyone except the intended recipient, where the cryptosystem is a set of algorithms combined with keys to convert the original message (Plain-text) to encrypted message (Cipher-text) and convert it back in the intended recipient side to the original message (Plain-text). Cryptography is the science of securing data. Cryptography is way of implanting mathematics to encrypt and decrypt data. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

### II. DIMENSION OF CRYPTOGRAPHIC SYSTEMS

There are three important factors which makes effective of any cryptographic systems.

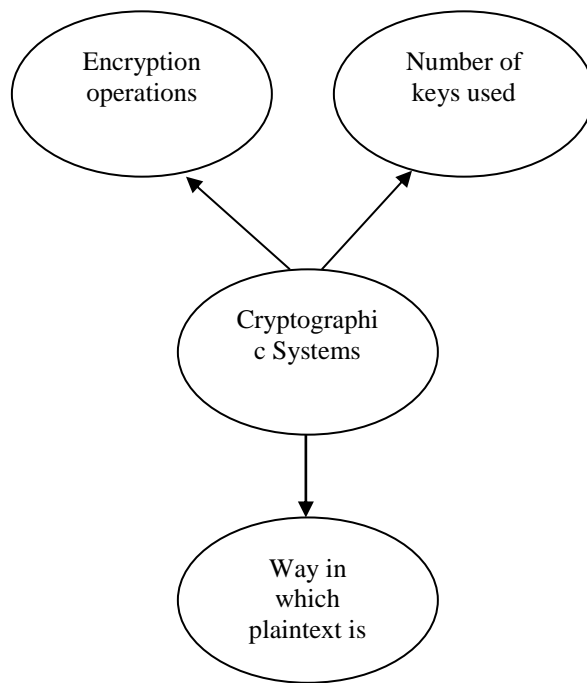


Figure 1:- Dimension Cryptographic Systems

Encryption operation includes

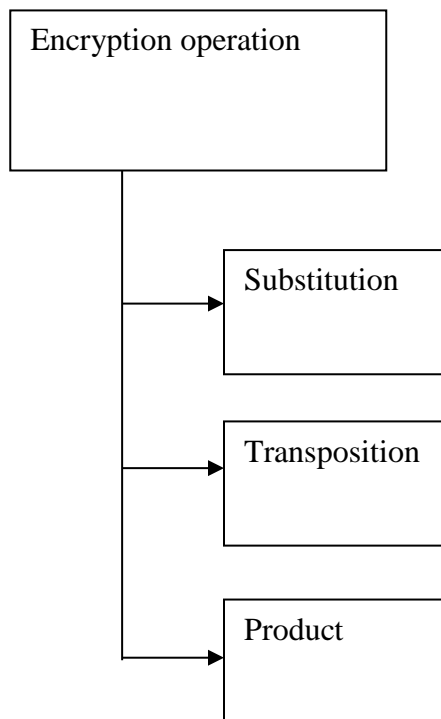


Figure 2:- Techniques used Encryption operation

Number of keys means how many key used for encryption and decryption includes

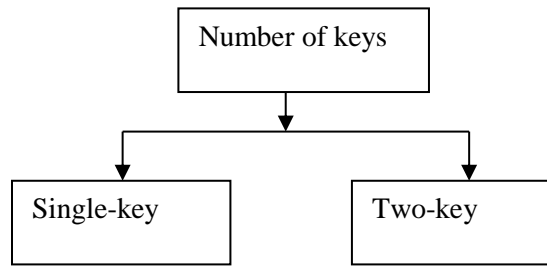


Figure 3:- Number of keys

Way in which plaintext is processed includes

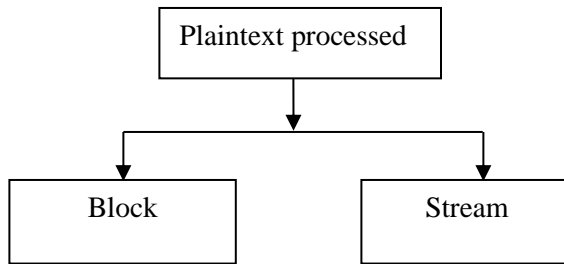


Figure 4:- Processing of plain text

### III. OBJECTIVES OF CRYPTOGRAPHY

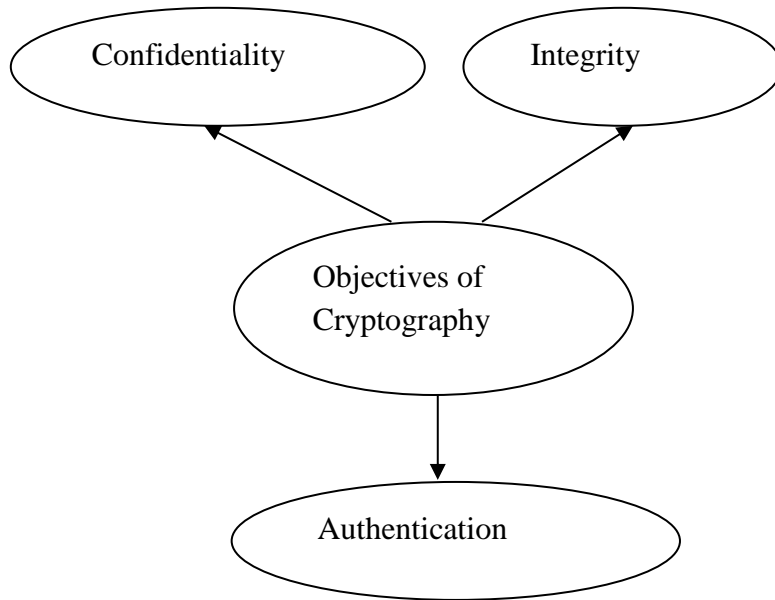


Figure 5:- Objective of cryptography

Cryptography provides a number of advantages to ensure the data privacy and security. Confidentiality Transmitted Information has to be accessed only by the authorized party. Authentication: The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person. Integrity Only the authorized party is allowed to modify the transmitted information.

#### IV. SINGLE KEY BASED CIPHER MODEL

There are six components are used in single key based cipher model

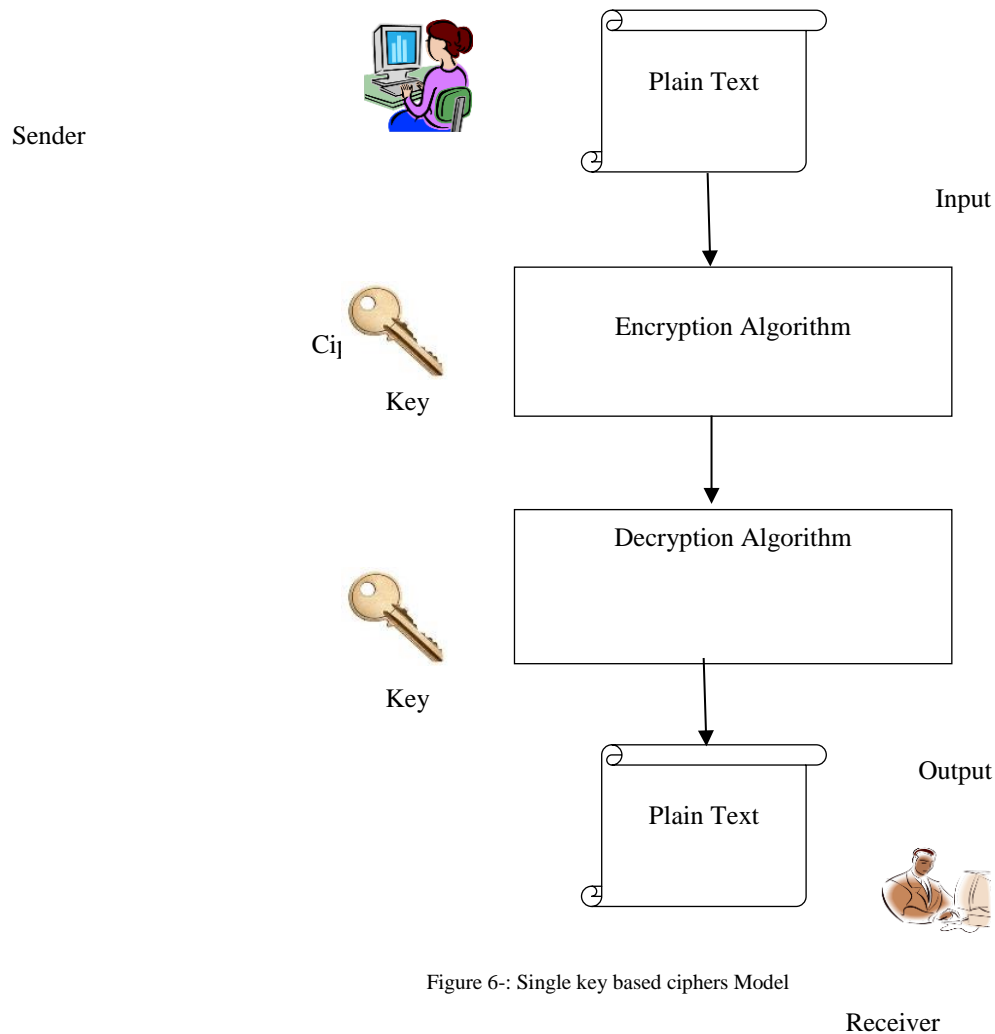


Figure 6-: Single key based ciphers Model

1. Plaintext - The original message.
2. Cipher text - The coded message.
3. Cipher - algorithm for transforming plaintext to cipher text.
4. Key - info used in cipher known only to sender/receiver.
5. Encipher (encrypt) - converting plaintext to cipher text. ,,
6. Decipher (decrypt) - recovering cipher text from plaintext.

## V. LITERATURE REVIEW

In 2011 Uttam Kr. Mondal Satyendra Nath Mandal proposed “Frame Based Symmetric Key Cryptography”. They proposed symmetry key block cipher algorithm to encrypt plain text into cipher text or vice versa using a frame set. A comparative study have been made with RSA, DES, IDEA, BAM and other algorithms with Chi-square value, frequency distribution, bit ratio to check the security level of proposed algorithm. Finally, a comparison has been made for time complexity for encryption of plain text and decryption from cipher text with the well-known existing algorithms [1].

In 2012 Aarti Soni, Suyash Agrawal proposed “Using Genetic Algorithm for Symmetric key Cryptography”. Genetic algorithms are a class of optimization algorithms. Many problems can be solved using genetic algorithms through modeling a simplified version of genetic processes. They proposed a method based on Genetic Algorithm which is used to generate key by the help of pseudo random number generator. Random number will be generated on the basis of current time of the system. Using Genetic Algorithm they keep the strength of the key to be good, still make the whole algorithm good enough. Symmetric key algorithm AES has been proposed for encrypting the image as it is very secure method for symmetric key encryption[2].

In 2012 Somdip Dey proposed “An Integrated Symmetric Key Cryptographic Method”. They proposed a new integrated symmetric-key cryptographic method, named SJA, which is the combination of advanced Caesar Cipher method, TTJSA method, Bit wise Rotation and Reversal method. The encryption method consists of three basic steps Encryption Technique using Advanced Caesar Cipher, Encryption Technique using TTJSA Algorithm, and Encryption Technique using Bit wise Rotation and Reversal [3].

In 2012 Monika Agrawal, Pradeep Mishra proposed “A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm” They presented a new approach for data encryption based on Blowfish algorithm. The blowfish algorithm is safe against unauthorized attack and runs faster than the popular existing algorithms. With this new approach we are implementing a technique to enhance the security level of blowfish algorithm and to further reduce the time for encryption and decryption [4].

In 2013 Sombir Singh, Sunil K. Maakar and Dr.Sudesh Kumar proposed “Enhancing the Security of DES Algorithm Using transposition” Cryptography Techniques”. To improve the security of DES algorithm they added transposition technique before the DES algorithm to perform its process. By using an Enhanced DES algorithm the security has been improved which is very crucial in the communication and field of Internet. If the transposition technique is used before the original DES algorithm then the intruder required first to break the original DES algorithm and then transposition technique. So the security is approximately double as compared to a simple DES algorithm [5].

In 2014 Satish Kumar Garg proposed “Modified Encryption and Decryption Using Symmetric Keys at Two Stages: Algorithm SKG 1.2”. They introduced a modified symmetric key cryptographic method, called algorithm SKG 1.2, for data encryption and decryption of any file using symmetric key at two stages, by swapping the characters in the string of text and by shifting the characters to left or right. The proposed method can be applied to encrypt any data consisting of 30 or more characters [6].

In 2014 Saranya K Mohanapriya R proposed “A Review on Symmetric Key Encryption Techniques in Cryptography”. They proposed a study on various symmetric key encryption techniques, its comparison and the attacks to which they are vulnerable to [7].

In 2015 Sanket A. Ubhad, Nilesh Chaubey, and Shyam P. Dubey proposed “Advanced ASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id” Cryptography is only thanks to succeed. They proposed square measure

and new algorithm for cryptography technique, UPMM rule, which is applied on computer code worth of knowledge. Proposed technique to send information over the network in set of 3 keys. In this technique no new information is further so it becomes difficult to search out however cryptography is finished on the info. Even if the persona non grata get the message, it's powerful for him to rewrite the data since summation of personal keys accustomed generate palindrome range [8].

## VI. COMPARISON OF SINGLE KEY BASED METHODS

We compare some existing algorithm based on different parameters like key size, security level, modification and flexibility.

(A) Techniques used

Algorithm	Techniques
Ceaser Cipher	Simple Substitution
Hill Cipher	Based on leaner Algebra
Vernam Cipher	XOR between plain text and Keys

Table 1 Comparisons using Techniques

(B)Key Size

Algorithm	Key size
DES	56 Bits
AES	256 Bits
Blowfish	256 Bits
IDEA	128 Bits

Table 2 Comparisons using Key Size

(C) Flexibility

Algorithm	Flexibility
DES	No
3DES	Yes
Blowfish	Yes
IDEA	No

Table 3--: Comparisons using Flexibility

## CONCLUSION

Cryptography provides data security and privacy. Several algorithms have been proposed in the past year. We compare some algorithm on the basis of some parameters like key size techniques used and flexibility. Some of algorithm are flexible some of them provides high security and some of them are modifiable

## REFERENCES

1. Uttam Kr. Mondal Satyendra Nath Mandal “Frame Based Symmetric Key Cryptography” Int. J. Advanced Networking and Applications 762 Volume: 02, Issue: 04, Pages: 762-769 2011.
2. Aarti Soni, Suyash Agrawal “Using Genetic Algorithm for Symmetric key Generation in Image Encryption” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 10, December 2012 ISSN: 2278 – 1323.
3. Somdip Dey “An Integrated Symmetric Key Cryptographic Method Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal Method: SJA Algorithm” IJ.Modern Education and Computer Science, 2012, 5, 1-9 Published Online June 2012 in MECS.
4. Monika Agrawal, Pradeep Mishra “Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-6, August 2012.
5. Sombir Singh Sunil K. Maakar Dr.Sudesh Kumar “Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques”. International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June 2013 ISSN: 2277 128X
6. Satish Kumar Garg” Modified Encryption and Decryption Using Symmetric Keys at Two Stages: Algorithm SKG 1.2” International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 6, June 2014 ISSN: 2277 128X
7. Saranya K and Mohanapriya R “A Review on Symmetric Key Encryption Techniques in Cryptography “.International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014
8. Sanket A. Ubhad, Prof. Nilesh Chaubey, Prof. Shyam P. Dubey ASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 4, Issue. 8, August 2015.
9. Mohammad Shahnawaz Nasir, Prakash Kuppuswamy “Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm “International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 1, Issue 8, October 2013.
10. Rachna Arora and Anshu Parashar “Secure User Data in Cloud Computing Using Encryption Algorithms” International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926.
11. Satyajeet R. Shinge, Rahul Patil “An Encryption Algorithm Based on ASCII Value of Data” (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7232-7234
12. Ch. Santhosh Reddy, Ch. Sowjanya, P. Praveena, Prof Shalini L Poly-alphabetic Symmetric Key Algorithm Using Randomized Prime Numbers International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012 1 ISSN 2250-3153