IJCAT - International Journal of Computing and Technology, Volume 3, Issue 2, February 2016
ISSN : 2348 - 6090
www.IJCAT.org

A Recent Survey on Different Symmetric Key Based Cryptographic Algorithms

[1] Pramod Gorakh Patil, [2] Vijay Kumar Verma

[1] M.Tech, RGPV Bhopal, Lord Krishna College of Technology Indore
Indore, MP, India

[2] Asst. Professor, M.Tech, RGPV Bhopal, Lord Krishna College of Technology Indore
Indore, MP, India

Abstract - Encryption is one the most effective approach to achieve data security and privacy. The Encryption 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 the encryption 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 any one. The original data is referred to as the plaintext and the encrypted data as the cipher text. Several symmetric key base algorithms have been developed in the past year. In this paper we proposed a comparative study over symmetric key based algorithm using some parameter like scalability, key size, security etc.

Keywords **- Symmetric, Encryption, Decryption, Scalability, Security, Plaintext, Chippertext.**

1. Introduction

Data can be read and understood without any special measures are called plaintext. Cryptography is the science of securing data. Cryptography is way of implanting mathematics to encrypt and decrypt data. Cryptography provides you to store sensitive information or transmit it across the insecure networksso that cannot be read by anyone except the intend recipient. 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 [9, 10].

2. Dimensions of Cryptographic Systems

Cryptographic Systems are characterized alone three independent dimensions.

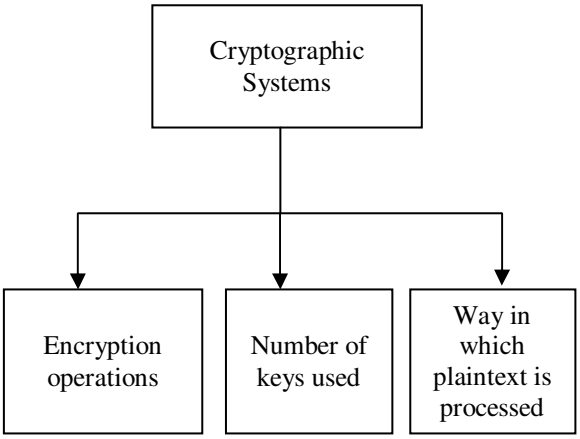

Fig. 1 Cryptographic Systems

2.1 Type of Encryption Operations Include

1. Substitution
2. Transposition
3. Product

2.2 Number of Keys Includes

1. Single-key or private
2. Two-key or public

2.3 Way in Which Plaintext is Processed

1. Block
2. Stream

3. Objectives of Cryptography

Cryptography provides a number of advantages to ensure the privacy of data, some of them are

1. **Confidentiality**: Transmitted Information has to be accessed only by the authorized party.

2. **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.

3. **Integrity** Only the authorized party is allowed to modify the transmitted information.

4. Symmetric Cipher Model

There are five components are used in symmetric cipher model

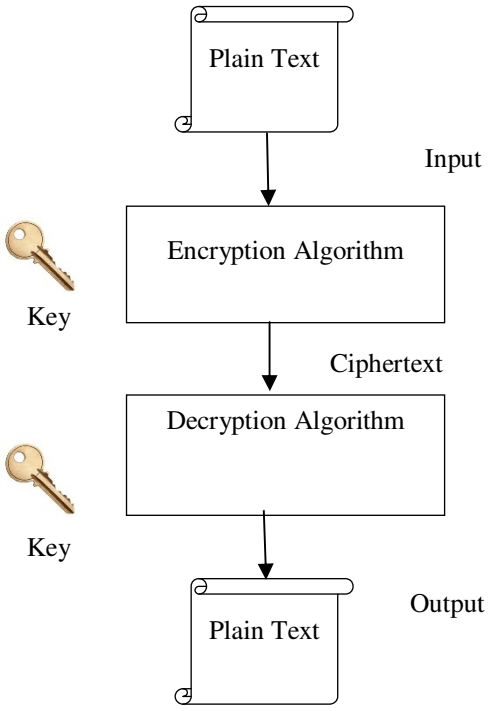

Fig. 2 Symmetric Encryption/Decryption Model

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

5. Literature Review

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

In 2012 AartiSoni, Suyash Agrawal proposed "Using Genetic Algorithm for Symmetric key Cryptography". Genetic algorithms are a class ofoptimization algorithms. Many problems can be solvedusing genetic algorithms through modeling a simplifiedversion of genetic processes. They proposed amethod based on Genetic Algorithm which is used togenerate key by the help of pseudo random numbergenerator. Random number will be generated on the basisof current time of the system. Using Genetic Algorithm they keep the strength of the key to be good, still make thewhole algorithm good enough. Symmetric key algorithmAES has been proposed for encrypting the image as it isvery secure method for symmetric key encryption [2].

In 2012 SomdipDey proposed "An Integrated Symmetric Key Cryptographic Method". Theyproposed 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 Techniqueusing Bit wise Rotation and Reversal [3].

In 2012 Monika Agrawal, Pradeep Mishra proposed "A Modified Approach for Symmetric KeyCryptography Based on Blowfish Algorithm"They presented a new approach for dataencryption based on Blowfish algorithm. The blowfish algorithmis safe against unauthorized attack and runs faster than thepopular existing algorithms. With this new approach we areimplementing a technique to enhance the security level ofblowfish algorithm and to further reduce the time for encryptionand decryption [4].

In 2013 Sombir Singh, Sunil K. Maakarand 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 Gargproposed "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].

In2014 Saranya K Mohanapriya R proposed "A Review on Symmetric Key EncryptionTechniques in Cryptography". They proposeda study on various symmetric key encryptiontechniques, its comparison and the attacks to which theyare 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].

6. Symmetric Algorithms Comparisons

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

6.1. Key Size

Table 1 Comparisons using key size

Algorithm	Key Size
DES	56
3DES	168
Blowfish	128
IDEA	128

6.2. Security Level

Table 2 Comparisons using Security level

Algorithm	Security level
DES	Insecure for large corporations
3DES	High level of security
Blowfish	high level of security,
IDEA	strong security

6.3. Modification

Table 3 Comparisons using Modification

Algorithm	Modification
DES	None
3DES	168
Blowfish	64-448
IDEA	none

6.4. Flexibility

Table 4 Comparisons using Flexibility

Algorithm	Flexibility
DES	No
3DES	Yes
Blowfish	Yes
IDEA	No

7. Conclusion

Cryptography plays an important role in data security and privacy. Several algorithms have been developed in the past year and by comparison of different parameters used in algorithms give significance of the algorithms. Wecompare some algorithm on the basis of certain parameters. Some of algorithm are flexible some ofthem provides high security and some of them are modifiable.

References

[1] Uttam Kr. MondalSatyendraNathMandal "Frame Based Symmetric Key Cryptography" Int. J. Advanced Networking and Applications 762Volume: 02, Issue: 04, Pages: 762-769 2011.

[2] AartiSoni, SuyashAgrawal "Using Genetic Algorithm for Symmetric keyGeneration in Image Encryption" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)Volume 1, Issue 10, December 2012 ISSN: 2278 – 1323.

[3] SomdipDey "An Integrated Symmetric Key Cryptographic Method Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal Method: SJA Algorithm"

I.J.Modern Education and Computer Science, 2012, 5, 1-9 Published Online June 2012 in MECS.

[4] Monika Agrawal, Pradeep Mishra "Modified Approach for Symmetric KeyCryptography 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. MaakarDr.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

[7] Computer Science and Software Engineering Volume 4, Issue 6, June 2014 ISSN: 2277 128X

[8] 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

[9] Sanket A. Ubhad, Prof. Nilesh Chaubey, Prof. Shyam P. DubeyASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id International Journal of Computer Science and Mobile ComputingIJCSMC, Vol. 4, Issue. 8, August 2015.

[10] Mohammad ShahnawazNasir, PrakashKuppuswamy "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.

[11] RachnaArora and AnshuParashar"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.

[12] Satyajeet R.Shinge, Rahul Patil"An Encryption Algorithm Based on ASCII Valueof Data" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7232-7234

[13] 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