Volume 8, No. 4, May 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

A Review on Symmetric Key Cryptography Algorithms

Sangeeta
MCA Student, Department of Computer Science applications, University Institute of Computer Applications and Information Science, SBBS University, Jalandhar Punjab, INDIA.
sangeetavirdi2@gmail.com

Er. Arpneek Kaur
Assistant Professor, Department of Computer Science applications, University Institute of Computer Applications and Information Science, SBBS University, Jalandhar Punjab, INDIA.
arpneek@gmail.com

***Abstract*- Security is the most important aspect in the field of internet and network application. It is an important task to secure information over the network. To secure information, cryptography can be used. Cryptography play very important role in information or communication security on network. Cryptography is a technique which is used to encrypt and decrypt data or information in a secret form. There are cryptography can be divided into two parts that are Symmetric key cryptography and Asymmetric key cryptography. In this paper, we discuss briefly in Symmetric key cryptography algorithms such as AES, DES, 3DES, Blowfish etc.**

Keywords*— *Symmetric key cryptography, AES, DES, 3DES, blowfish;

I. *INTRODUCTION*

Cryptography is the art of achieving security by encoding messages to make them non-readable. Cryptography not only protects the information but also provides authentication to the user. Here the original information and encrypted information are referred as plaintext and cipher text respectively. The transformation of plaintext into unintelligible data known as cipher text is the process of encryption. Decryption is the reverse process of encryption i.e. conversion of cipher text into plain text. During communication, the sender performs the encryption with the help of a shared secret key and the receiver performs the decryption. Cryptographic algorithms are broadly classified as Symmetric key cryptography and Asymmetric key cryptography.[3]

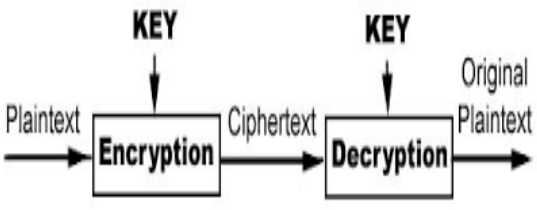

Fig 1: Cryptography process

There are two types of cryptography algorithm that are given below:

I.1. Symmetric key cryptography algorithm
I.2. Asymmetric key cryptography algorithm

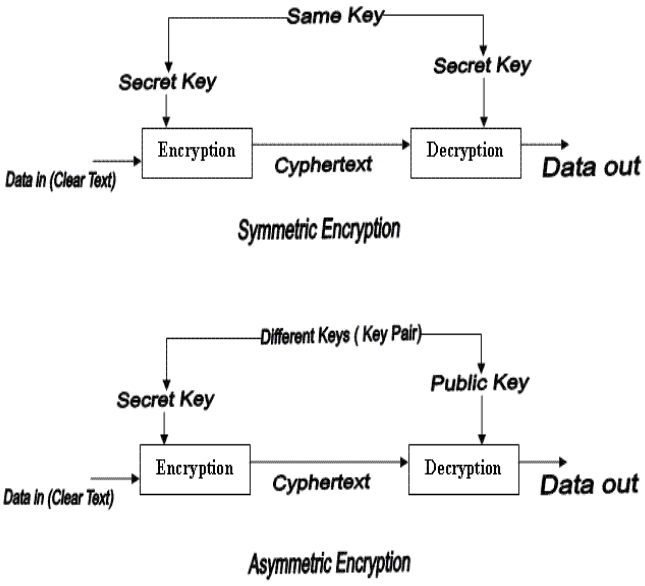

Fig 2: Types of Cryptography Algorithms

I.1. Symmetric Key Cryptography

Symmetric key cryptography or private key cryptography, in layman language can be understood as the technique which uses a single key for the encryption as well as the decryption of data. Technically, it is a technique which converts plaintext into cipher text and vice verse using the same key. The symmetric key cryptography system involves the following. [2]

Plaintext: original information that is fed as input to the algorithm.

Encryption algorithm: algorithm which performs various permutations and substitutions on the plaintext

Secret key: also an input to the encryption algorithm, changing the key results in the generation of different output.

Cipher text: statement in which the actual information is hidden.

Decryption algorithm: reverse of the encryption algorithm; produces the original information.

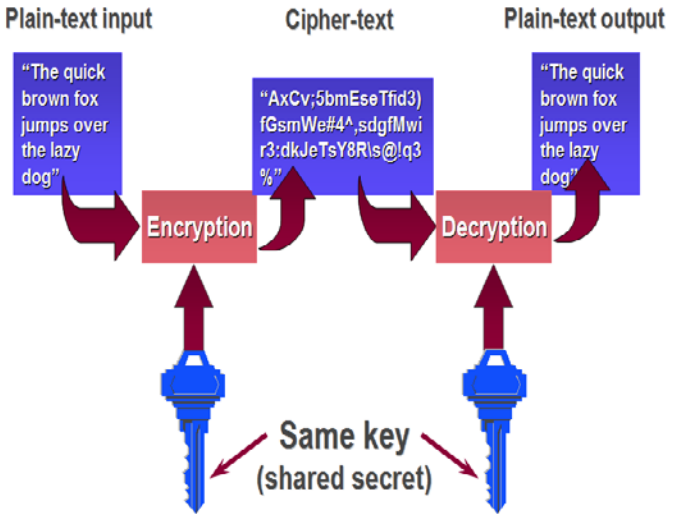

Fig 2: Symmetric key cryptographic algorithms process

Some widely used Symmetric key cryptographic algorithms are given below:

i. DES (Data Encryption Standard)
ii. Triple Data Encryption Algorithm (TDEA or Triple DEA)
iii. AES (Advanced Encryption Standard).
iv. BLOWFISH

i. DES (Data Encryption Standard)

Data Encryption Standard (DES) is a cryptographic standard that was proposed as the algorithm for the secure and secret items in 1970 and was adopted as an American federal standard by National Bureau of Standards (NBS) in 1973. DES is a block cipher, which means that during the encryption process, the plaintext is broken into fixed length blocks and each block is encrypted at the same time. Basically it takes a 64 bit input plain text and a key of 64-bits (only 56 bits are used for conversion purpose and rest bits are used for parity checking) and produces a 64 bit cipher text by encryption and which can be decrypted again to get the message using the same key.[5]

ii. 3-DES(Triple–Data Encryption Standard)

As an improvement on Data Encryption Standard (DES), in the late 1970's IBM developed the Triple Data Encryption Standard (3DES). The Triple Data Encryption Algorithm (3DES) is simply the DES used three times in succession. It is this successive use which makes 3DES much harder to crack than DES. 3DES solves the problem of the too-short 56 bit key length used in DES by utilizing a key length of 168 bits (three separate 64 bit keys are used to process the same bit of unencrypted text). 3DES is still being widely used in financial transactions today and is seen as being fairly secure.[4]

iii. AES (Advanced Encryption Standard):

AES is a symmetric block cipher that can Block size 128 bit, three different Cipher keys 128, 192 and 256 bits. Basically, AES is based on a design principle encryption algorithmsknown as – transposition, substitution, and transposition-substitution technique. Most AES calculation are uses a round function in special finite field that is compared of four different byte-oriented transformation such as Sub byte, Shift row, Mix column , Add round key. Number of rounds to be used depend on the length of key e.g. 10 round for 128 bit key, 12 rounds for 192-bit key and 14 rounds for 256 bit keys. At present the most common key size likely to be used is the 128 bit key. Rijndael was selected as the AES in Oct-200 designed to have the following characteristics:[1]

- Resistance to protect from all known attacks.
- Speed and code compactness depends on a wide range of platforms.
- Design simpler.

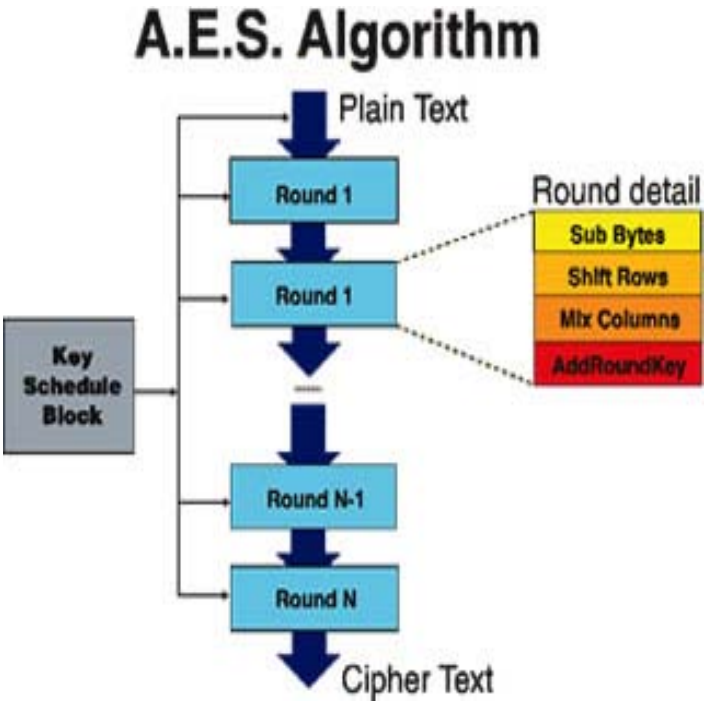

Fig 3: AES algorithm process

1) *Substitution bytes* – In this step, each byte ($a_{i,j}$) of matrix is replaced with a sub byte ($s_{i,j}$), that is Rijndeal S-Box. At the decryption end, the sub bytes are inversed to reach the original state.

2) *Shift Rows* - The shift rows operation, shift each rows with a certain constraint. That is first row of matrix is left same, the second, third and forth rows are shifted to one place left.

3) *Mix Columns* – In this step, the each column is multiplied with a fixed polynomial and the new value of the columns is placed.

4) *Add Round Key* – This sub key is derived from the main key and the sub key is added into this step by applying XOR to the matrix.

iv. Blowfish:

Blowfish is a symmetric block cipher that can be effectively Blowfish was designed in 1993 by Bruce Schneider as a fast alternative to existing encryption algorithms .Blowfish is a symmetric key block cipher that uses a 64 bit block size and variable key length. It takes a variable-length key from 32 bits to 448 bits. Blowfish has variants of 14 rounds or less. Blowfish is one of the fastest block ciphers which has developed to date. Slowness kept Blowfish from being used in some applications. Blowfish was created to allow a nyone to use encryption free of patents and copyrights. Blowfish has remained in the public domain to this day. No attack is known to be successful against it, though it suffers from weak keys problem (Bruce, 1996) .[6]

II. RELATED WORK:

This section gives the overview of related work by various authors in network security algorithms

Pratap Chnadra Mandal et al. [2012], provides a fair comparison between four most common and used symmetric key algorithms: DES, 3DES, AES and Blowfish. A comparison has been made on the basis of these parameters: rounds block size, key size, and encryption / decryption time, CPU process time in the form of throughput and power consumption. These results show that blowfish is better than other algorithm. AES has advantage over the other 3DES and DES in terms of throughput & decryption time.[6]

Krishna Kumar Pandey et al. [2013], 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.[9]

Preeti Singh et al [2014] , Some ciphers are better than others in some aspects but lack behind on others. Each method has its own advantages & shortcomings. To sum up, all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security. To overcome the problems in Symmetric Ciphers, Public Key Cryptography was developed, but it has its own loopholes.[10]

Rejani. R et al [2015], performed considering security, throughput, speed, encryption/decryption, power consumption and other factors, it is shown that blowfish algorithm having good performance than other symmetric algorithm like DES and 3DES, AES having better performance. The memory requirement of symmetric algorithms is lesser than asymmetric encryption algorithms and symmetrickey algorithms runs faster than asymmetric key algorithms.Further, symmetric key encryption provides more security thanasymmetric key encryption.

Sonia Rani et al [2016] gives the review of various cryptography algorithms for network security, some related work already done by various authors, problems in existing work and some proposals for proposed work. In order to protect the intended data from hacking, cryptography is performed. In this paper we briefly discussed about cryptography and various symmetric and asymmetric algorithms [7].

Md. Alam Hossain et al. [2016], describes the basic characteristics (Key Length, Block size) of symmetric (AES, DES, 3DES, BLOWFISH, RC4), Asymmetric (RSA, DSA, Diffie-Hellman, EI-Gamal, Paillier), Hashing (MD5, MD6, SHA, SHA256) algorithms. Also we implemented five well-known and widely used encrypt techniques like AES, DES, BLOWFISH, DES, RC4, RSA algorithms and compared their performance based on the analysis of their encryption and decryption time for different file sizes in the local system. [8]

Dr. T. Christopher et al [2016] analysis is made between symmetric key algorithms such as AES, RC6 and Blowfish. The algorithms are compared in terms of various factors such as key length, cipher type, block size, resistance, security, possible keys, CPU time, encryption time, memory utilization and throughput. To analyze the performance of the algorithms it is required to know its strength and limitation.[8]

Swati Kashyap et al. [2105], conclude that the performance evaluation of cryptography algorithm depends on throughput of encryption scheme, CPU time taken & packet size. The throughput of the encryption scheme is calculated by dividing the total plaintext in MB by total encryption time in Second for each algorithm. If the throughput value increases, the power consumption by this encryption technique is decreased. AES is the far better algorithm in terms of performance and security but its power consumption is on high..[12]

SurekhaThorat et al [2017] attempts to review major researches and developments occurred in Symmetric key cryptography .We analyses many Symmetric algorithm and there steps. Symmetric key cryptography understood as the technique which uses a single key for the encryption as well as the decryption of data. This paper provides an overview of Symmetric algorithm are implemented in the recent scenario which provide efficiency and effectiveness. Today research start on role of symmetric algorithm in DNA cryptography, quantum cryptography. [14]

III. CONCLUSION:

To protect the data/ information from hacking, cryptography is performed. In this paper we briefly discussed about cryptography and its type symmetric key cryptography algorithms. Cryptographic algorithms play a very important role in the field of information security. I studied the various symmetric key cryptographic algorithms. From the literature survey, the symmetric key cryptography algorithms have their own pros and cons. These algorithms are more used as compare to asymmetric key algorithms.

REFERENCES

[1] Gaurav Yadav, Mrs. Aparna Majare “Comparative Study of Performance Analysis of Various Encryptio Algorithms” International Conference On Emanations in Modern Technology and Engineering (ICEMTE-2017) Volume: 5 Issue: 3, 2017.

[2] Md. Sarfaraz Iqbal, Shivendra Singh , Arunima Jaiswal , “ Symmetric Key Cryptography: Technological Developments in the Field” International Journal of Computer Applications (0975 – 8887) Volume 117 – No. 15, May 2015 .

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

[3] SARANYA K, MOHANAPRIYA R, UDHAYAN J, "A Review on Symmetric Key Encryption Techniques in Cryptography" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014.

[4] Same O.O. Adekanmbi, O.O. Omitola, T.R. Oyedare, S.O. Olatinwo, "Performance Evaluation of Common Encryption Algorithms for Throughput and Energy Consumption of a Wireless System" JOURNAL OF ADVANCEMENT IN ENGINEERING AND TECHNOLOGY" Voume3 /Issue1, June 2015.

[5] Nimmi Gupta "Implementation of Optimized DES Encryption Algorithm upto 4 Round on Spartan 3" International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2 , Issue 1.

[6] Pratap Chnadra Mandal, " Superiority of Blowfish Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 9, September 2012.

[7] Sonia Rani, Harpreet Kaur, " Technical Survey on Cryptography Algorithms for Network Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 9, September 2016.

[8] Dr. T. Christopher, Mohana Priya. A, "Study of Symmetric Key Network Security Algorithms" IJSRD - International Journal for Scientific Research & Development| Vol. 3, Issue 11, 2016.

[9] 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.

[10] Preeti Singh, Praveen Shende, "Symmetric Key Cryptography: Current Trends" International Journal of Computer Science and Mobile Computing, Vol.3 Issue.12, December- 2014.

[11] Rejani. R , Deepu.V. Krishnan, "Study of Symmetric key Cryptography Algorithms" International Journal of Computer Techniques -– Volume 2 Issue 2, Mar - Apr 2015.

[12] Swati Kashyap, Er. Neeraj Madan, "A Review on: Network Security and Cryptographic Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, April 2015.

[13] Shivani Sharma, Yash Gupta, " Study on Cryptography and Techniques" International Journal of Scientific Research in Computer Science, Engineering and Information Technology ,Volume 2 ,Issue 1,2017.

[14] SurekhaThorat5, Rohini Sharma, Shivaji Pansare, "ANALYSIS OF SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS" International Research Journal of Engineering and Technology (IRJET) , Volume: 04 Issue: 02 | Feb -2017.

[15] Nisha Satankar and Vijay Kumar Verma, "A SELF-GENERATED PRIVATE KEY BASED CRYPTOGRAPHICALGORITHMS" International Journal of Recent Innovation in Engineering and Research, Volume: 02 Issue: 03 March– 2017 (IJRIER).

[16] Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz, "Performance Analysis of Different Cryptography Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 3, March 2016.

[17] Sumedha Kaushik, Ankur Singhal, "Network Security Using Cryptographic Techniques" International Journal of Advanced Research in Computer Science and Software Engineering 2 (12), December - 2012, pp. 105-107.

[18] Kalyani Ganesh Kadam, Prof. Vaishali Khairnar, "HYBRID RSA-AES ENCRYPTION FOR WEB SERVICES" International Journal of Technical Research and Applications, September, 2015.