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

# Technical Review on Symmetric and Asymmetric Cryptography Algorithms

Sonia Rani [1]
M.Phil Scholar, Department of Computer Science applications, University Institute of Computer Applications and Information Science, SBBS University, Jalandhar Punjab, INDIA.
virdisonia22@gmail.com

Harpreet Kaur [2]
Assistant Professor, Department of Computer Science applications, University Institute of Computer Applications and Information Science, SBBS University, Jalandhar Punjab, INDIA.
er.harpreetarora@gmail.com

***Abstract*- If you want to keep your information safe and secret, you have the possible strategies are: hide the existence of the information, or make the information unintelligible. Cryptography is the art and science of keeping information secure from unintended audiences, of encrypting it. Cryptography is a method used to store and transmit data in a secret form so that only those for whom it is intended can read and process it. Cryptography is of two types such as symmetric key cryptography and asymmetric key cryptography. This paper gives the review/survey of various cryptography algorithms used to secure network , some related work already done by various authors, problems in existing work and some proposals for proposed work.**

**Keywords—Symmetric key cryptography, asymmetric key, cryptography algorithms.**

## I. INTRODUCTION

Cryptography is the technique used to avoid unauthorized access of data. Data can be encrypted using a cryptographic algorithm by using different keys. It is transmitted in an encrypted state, and decrypted by the intended party. If a third party intercepts the encrypted data, it will be difficult to decipher. The security of modern cryptosystems is not based on the secrecy of the algorithm, but on the secrecy of a relatively small amount of information, called a secret key. Cryptography plays an important role in the security to maintain the confidentiality, authentication, integrity and non- repudiation of the information and encryption is the backbone of cryptography.[1]

*Cryptography Goals:* There are five main goals of cryptography. Every security system must provide a many of security functions that can assure the secrecy of the system. These functions are usually referred to as the goals of the security system. These goals can be listed under the following five main categories:

a. *Authentication:* The process of proving one's identity. This includes verifying the message's source. Authentication is of two types: (i) Peer entity authentication, and (ii) Data origin authentication.
b. *Privacy/confidentiality:* Confidentiality means protection against unauthorized disclosure of information. It may be applied to whole messages, parts of messages, and even existence of messages. Confidentiality provides the protection of transmitted data from passive attacks.
c. *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original. The basic form of integrity is packet check sum in IPv4 packets.
d. *Non-repudiation:* Sender or receiver cannot deny for a transmitted message. When a message is sent, the receiver can prove that the sender in fact sent the message.
e. *Service Reliability and Availability:* Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems provide a way to grant their users the quality of service they expect. [1]

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

a. Symmetric key cryptography algorithm
b. Asymmetric key cryptography algorithm

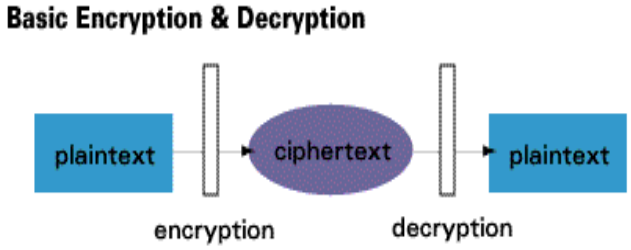


Fig 1: Cryptography Algorithms.

1) *Symmetric (Secret) Key Cryptography*

Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key. [2]





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)

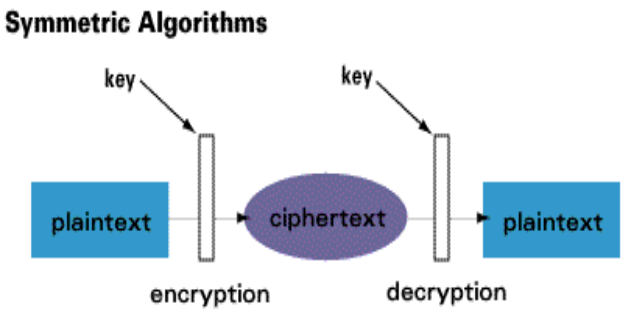


Fig 2: Symmetric key cryptographic algorithms process

Some widely used Symmetric key cryptographic algorithms are given below:

- DES (Data Encryption Standard)
- Triple Data Encryption Algorithm (TDEA or Triple DEA)
- AES (Advanced Encryption Standard).
- BLOWFISH
- RC4 (Rivest Cipher 4)

*a) DES (Data Encryption Standard)*

DES designed by IBM in 1972 and it was adopted by the U.S. Government as standard encryption technique. It is a symmetric key block cipher encryption algorithm based on Feistel Network. DES uses 64 bit block of text and 56 bit key length, it performs total 16 rounds of processing to encrypt data . In DES, the key was 64 bits but due to some restrictions from NSA (National Security Agency) IBM decided to use 56 bit key length for encryption and the remaining 8 bits is used as a parity bit for error detection, it also uses 8 boxes. DES divides the 64 bit block into two equal parts and then applies F - function on each part. F function performs four different tasks- Expansion, Key_ Mixing, Substitution and Permutation. Decryption is the same process of encryption in DES.[3]

*b) 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]

*c) AES (Advanced Encryption Standard):*

AES is a symmetric key block cipher encryption algorithm designed by Vincent Rijmen and Joan Daemen in 1998. It is based on Feistel network and support 128 bit block size and key length 128, 192 and 256 bits. AES performs 10, 12 or 14 round and the number of rounds depends on the key. It means for 128 bit key length AES performs 10 rounds, for 192 bit key it performs 12 rounds and for 256 bit key it performs 14 rounds. In AES each round performs some steps. Key-expansion, Initial-round, Rounds and Final-rounds. In Rounds step, Sub-byte generation, Shift-rows, Mix-columns and Add-round_key are performed whereas in Final-rounds step, same functions are performed except Mix-columns function.[3]

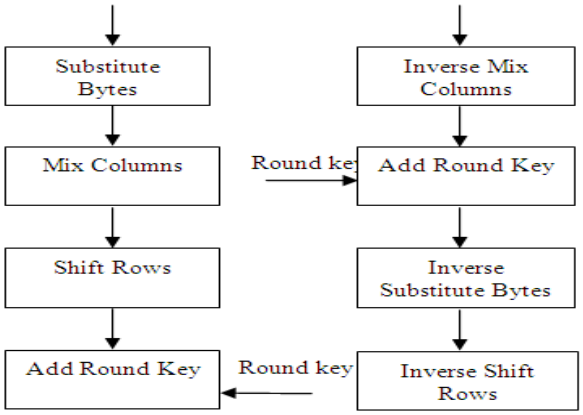


**Fig 3:** One Round of encryption and Decryption in AES

- *Substitution bytes* – In this step, each byte ($a_{i,j}$) of matrix is replaced with a sub byte ($s_{i,j}$), that is Rijindeal S-Box. At the decryption end, the sub bytes are inversed to reach the original state.
- *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.
- *Mix Columns* – In this step, the each column is multiplied with a fixed polynomial and the new value of the columns is placed.
- *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. [6]

*d) Blowfish:*

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses. Though it suffers from weak keys problem, no attack is known to be successful against it (Bruce, 1996). [7]

*e) RC4 (Rivest cipher 4):*

RC4 is developed by Ron Rivest also known as Rivest Cipher 4. Here the stream cipher is used for encryption of the plain text. Pseudorandom stream of bits (key stream) are generated by the RC4 algorithm, and bit-wise encryption/decryption has been performed. The generation key system involves two stages,

- One is the permutation of all 256 bytes.
- Another is two 8-bit index-pointers.

The key length for this RC4 is between 40-128 bits. If the common block ciphers are not used MAC strongly, bit-flapping attack is possible and the stream-cipher attack is also vulnerable if they are not correctly implemented. [10]

*2) Asymmetric (public) Key Cryptography*

The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys-a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it. Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. [2]

The some widely used Asymmetric key cryptographic algorithms are given below:

- RSA
- DIFFIE-HELLMAN
- PAILLIER
- Elgamal

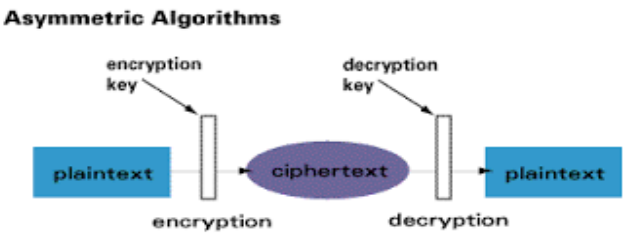


Fig 4: Asymmetric key cryptographic algorithms process

*a) RSA (Rivest –Shamir-Adlemen)*

RSA is a most popular and proven asymmetric cryptography algorithm. RSA is based on the mathematical fact that is easy to find the private and public keys based on the very large prime numbers.

**Encryption:** compute $c = m^e \bmod n$, where the $e$ and $n$ are the public key, and $m$ is the message block. The $c$ is the encrypted message.

**Decryption:** The private key $d$ is used to decrypt messages. Compute: $m = c^d \bmod n$, where $n$ is the modulus and $d$ is the private key.

In RSA, compare to encryption process, decryption process takes more time. [5]

*b) DIFFIE-HELLMAN:*

The scheme was first revealed by Whitfield Diffie and Martin Hellman in 1976. Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It permits two parties that have no prior knowledge of each other to jointly make a shared secret key over an insecure communications channel. This key can then be used to encrypt posterior communications using a symmetric key cipher.[8]

*c) PAILLIER:*

The Paillier cryptosystem is an asymmetric algorithm. It has homomorphic property permits this scheme to do normal addition operations on several encrypted values and achieving the encrypted sum, the encrypted sum can be decrypted later without even knowing the values ever that made up the sum.[8]

*d) ELGAMAL:*

El-Gamal is the asymmetric key cryptography. It is a public key cryptography which is based on Diffie Hellman key exchange. It was introduced by Taher El-Gamal in 1985. It is consist of signature, encryption algorithms as well as discrete logarithm problems [9]. ElGamal encryption consists of three components: the key generator, the encryption algorithm, and the decryption algorithm.

## II. RELATED WORK:

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

Jawahar Thakur et al. [2011], provides a fair comparison between three most common symmetric key cryptography algorithms: DES, AES, and Blowfish. Since main concern here is the performance of algorithms under different settings, the presented comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used. The comparison is made on the basis of these parameters: speed, block size, and key size. [7]

Shashi Mehrotra Seth et al. [2011], performs comparative analysis of three algorithm; DES, AES an RSA considering certain parameters such as computation time, memory usages and output byte. A cryptographic tool is used for conducting experiments. Experiments results are given to analyses the effectiveness of each algorithm. [14]

G. RAMESH et al [2012] performs comparative analysis of five algorithm; DES, 3DES, AES, UMARAM and UR5 Algorithm, considering certain parameters such as throughput, encryption time and power consumption. A cryptographic tool is used for conducting experiments. The experimental results show the superiority of our UR5 encryption algorithm over other algorithms in terms of the power consumption, processing time, and throughput .[16]





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)

Shaina Arora et al [2015] design an algorithm to merge both enhanced RSA algorithm and El-Gamal algorithm to provide user with a higher level of data security. The enhanced RSA algorithm enables faster encryption and decryption process and generating public and private key faster than the original RSA.[9]

Harshala B. Pethe et al [2015] present this paper deals with the implementation of Data Encryption Standard algorithm, which is one of the symmetric key cryptography algorithm. The m file DES.m is created and the two functions encrypt() and decrypt() are called into this file. This m file DES.m gives the time required for encryption and decryption in seconds for the entered text.[1]

Jitendra Singh Chauhan et al. [2105], focuses on the comparative study of various cryptographic algorithms like AES, DES, RSA, Blow Fish, Elliptic Curve, SHA and MD5 and give a proper direction to the users for use of proper algorithm for securing of data. MD5 algorithm takes least encryption time whereas, RSA takes largest encryption time. [11]

Arti Devi et al [2015] provides the comparison between three symmetric key cryptographic techniques namely as DES, AES and Blowfish algorithms in terms of time and security by using image simulation. Based on the image files used and the experimental result it was concluded that Blowfish algorithm consumes least encryption time and DES consume maximum encryption time. We also observed that Decryption of Blowfish and AES algorithms is better than DES algorithm.[14]

Jitendra Singh Laser et al. [2016], surveyed the conventional algorithms, based on their benefits and drawbacks. We additionally have in comparison the significance of each these cryptographic techniques. This paper also offer an appropriate future opportunity related to these cryptographic techniques. [11]

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]

V. Kapoor et al. [2016], a hybrid cryptographic technique for improving data security during network transmission is proposed and their implementation and results are reported. The proposed secure cryptographic technique promises to provide the highly secure cipher generation technique using the RSA, DES and SHA1 technique. [12]

Dr. D. Vimal Kumar et al. [2016], some well-known cryptographic algorithms have been analyzed in this paper to demonstrate the basic differences between the existing encryption techniques. Regardless of the mathematical theory behind an algorithm, the best algorithm are those that are well-known and well-documented because they are well-tested and well studied. [13]

## III. PROBLEM FORMULATION

Cryptography is a technology, which is essential for network security. There are two ways of sending such data in the secret form using the Asymmetric and Symmetric key cryptography .

From the literature survey, it is reviewed that all cryptography algorithms have their own advantages and disadvantages. There are many algorithms available for network security and they require more time for encryption and decryption process and the ones which require less encryption and decryption time are easy to crack and have low output. To remove the drawbacks of existing systems for increase the security, a hybrid encryption model using AES and ElGamal algorithms can be designed and compared with existing algorithm AES.

## IV. PROPOSED WORK

To design a hybrid model using AES and Elgamal algorithms for enhancing the security, to reduce encryption time and decryption time, data size, space complexity, and to increase throughput following are some points as a proposals to implement .

1. To combine AES and Elgamal algorithms.
2. To implement AES algorithms.
3. To compare the algorithm AES with Hybrid AES and Elgamal

## V. CONCLUSION

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. Cryptographic algorithms play a very important role in Network security. We studied the various cryptographic algorithms and majorly deals the encryption and decryption process for protecting the data on the network. Cryptographic algorithms play a very important role in network security. Our research work surveyed the performance of existing cryptographic methods such as symmetric and asymmetric algorithms. . In the review of literature survey there are many drawbacks. To overcome them, if we implement proposed technique the results may be better than the existing one.

## REFERENCES

[1] Harshala B. Pethe, Dr. Subhash. R. Pande, “Implementation Of Data Encryption Standard Algorithm” International Journal Of Computer & Mathematical Sciences Ijcms Volume 4, Issue 9 September 2015.

[2] Depavath Harinath, M V Ramana Murthy, B Chitra, “Cryptographic Methods And Performance Analysis Of Data Encryption Algorithms In Network Security” International Journal Of Advanced Research In Computer Science And Software Engineering, Volume 5, Issue 7, July 2015.

[3] Manju Rani, Dr. Sudesh Kumar, “Analysis On Different Parameters Of Encryption Algorithms For Information Security” International Journal Of Advanced Research In Computer Science And Software Engineering, Volume 5, Issue 8, August 2015.

[4] 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



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)

Of Advancement In Engineering And Technology" Voume3 /Issue1, June 2015.

[5] S. Pavithra , Mrs. E. Ramadevi , " Study And Performance Analysis Of Cryptography Algorithms " International Journal Of Advanced Research In Computer Engineering & Technology, Volume 1, Issue 5, July 2012.

[6] 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.

[7] Jawahar Thakur, Nagesh Kumar, "Des, Aes And Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis" International Journal Of Emerging Technology And Advanced Engineering, Volume 1, Issue 1, November 2011.

[8] 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.

[9] Shaina Arora, Pooja, "Enhancing Cryptographic Security Using Novel Approach Based On. Enhanced – Rsa And Elgamal : Analysis And Comparison " International Journal Of Computer Applications (0975 – 8887) Volume 112 – No 13, February 2015.

[10] B.Nithya, Dr.P.Sripriya, "A Review Of Cryptographic Algorithms In Network Security" International Journal Of Engineering And Technology (Ijet) Vol 8 No 1 Feb-Mar 2016.

[11] Jitendra Singh Laser, Viny Jain, "A Comparative Survey Of Various Cryptographic Techniques" International Research Journal Of Engineering And Technology (Irjet), Volume: 03 Issue: 03 | Mar-2016.

[12] V. Kapoor, Rahul Yadav, "A Hybrid Cryptography Technique For Improving Network Security" International Journal Of Computer Applications (0975 – 8887) Volume 141 – No.11, May 2016.

[13] Dr. D. Vimal Kumar, Mrs. J. Divya Jose, "Over View Of Cryptographic Algorithms For Information Security" International Journal Of Advanced Research In Computer And Communication Engineering Vol. 5, Issue 5, May 2016.

[14] Aarti Devi, Ankush Sharma, Anamika Rangra, "Performance Analysis Of Symmetric Key Algorithms: Des, Aes And Blowfish For Image Encryption And Decryption" International Journal Of Engineering And Computer Science Volume 4 Issue 6 June 2015.

[15] Shashi Mehrotra Seth, Rajan Mishra, "Comparative Analysis Of Encryption Algorithms For Data Communication" Ijcst Vol. 2, Issue 2, June 2011.

[16] G. Ramesh1 Dr. R. Umarani, "Performance Analysis Of Most Common Symmetrical Encryption Algorithms" International Journal Of Power Control Signal And Computation (Ijpcsc) Vol3. No1. Jan-Mar 2012.

[17] Jitendra Singh Chauhan, S. K. Sharma, "A Comparative Study Of Cryptographic Algorithms" International Journal For Innovative Research In Multidisciplinary Field, Volume - 1, Issue - 2, Sept – 2015.

[18] 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.

[19] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, And Mohiy Mohamed Hadhoud, "Evaluating The Performance Of Symmetric Encryption Algorithms" International Journal Of Network Security, Vol.10, No.3, Pp.213-219, May 2010.

[20] Pratap Chandra Mandal, "Evaluation Of Performance Of The Symmetric Key Algorithms: Des, 3des, Aes And Blowfish" Journal Of Global Research In Computer Science Volume 3, No. 8, August 2012.

[21] Lalit Singh Dr. R.K. Bharti, "Comparative Performance Analysis Of Cryptographic Algorithms" International Journal Of Advanced Research In Computer Science And Software Engineering, Volume 3, Issue 11, November 2013.

[22] Mini Malhotra, "A New Encryption Scheme Based On Enhanced Rsa And Elgamal" International Journal Of Emerging Technologies In Computational And Applied Sciences, 8(2), March-May, 2014, Pp. 138- 142,2014..

[23] Shaina Arora, 2pooja To Do Comparative Study By Implementing Cryptography Algorithms On The Bases Of Rsa And El-Gamal International Journal Of Computer Science And Technology Vol. 5, Issue 4, Oct - Dec 2014.

[24] 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.

[25] Kalyani Ganesh Kadam, Prof. Vaishali Khairnar, "Hybrid Rsa-Aes Encryption For Web Services" International Journal Of Technical Research And Applications, September, 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)