A Survey on the Cryptographic Algorithms

Mr. K. Vijay Anand[*], Dr. D. Binu[**]

[*] Associate Professor, Department of Computer Science, SNMV College of Arts and Science, Coimbatore.
[**] Assistant Professor (Sl. Gr.), Department of ECE, Sri Ramakrishna Institute of Technology, Coimbatore.

Abstract- With the growth in the use of Internet in various fields like medical, education and private sector, the security and privacy of the data has become very important. Internet does most of the data handling and electronic transactions today. When the sender transfers the information to the receiver on the Internet, it may be eavesdropped by an intruder and thus is a continuous threat to the secrecy or confidentiality of the data. Cryptography is the popular technique that protects the confidentiality of the data. Cryptography converts the plain text into a form which can not be understood and then receiver applies reverse mechanism to decrypt the unreadable form of data to readable form. This mechanism is called as encryption-decryption process. Thus, for a secured transfer of data over the Internet, it is important to find out which algorithm performs better than the other algorithms. In this paper, the different symmetric encryption algorithms like AES, Blowfish, DES, RC4 and RSA have been analyzed with respect to different parameters.

Index Terms- Cryptography, AES, Blowfish, DES, RC4 and RSA

I. INTRODUCTION

Encryption is a process of converting in formation in "hidden" form, so that it can be understood only by someone who knows how to decrypt it. There are two aspects for encryption and decryption: algorithm and key used. Key is like one time pad used in vernal cipher. If the keys used for encryption and decryption, are the same, then this is called secret key cryptography. And if dissimilar keys are used for encryption and decryption, we call this public key cryptography. In secret key cryptography, only a single key is used. Hence before distributing the data between the sender and receiver, the key must be transferred. DES, AES, 3DES, IDEA, Blowfish algorithms, etc. are listed under secret key cryptography and RSA, Digital Signature and Message Digest algorithms are categorized under public key cryptography.

There are two key aspects used for each algorithm. They are algorithm type (define size of plain text should be encrypted per step) and algorithm mode (define cryptographic algorithm mode). The combination of series of the basic algorithms and some block ciphers and some feedbacks from previous steps makes algorithm mode.

A. Basic Terms Used in Cryptography

- *Plain Text*

Plain Text is nothing but the original message that the person wishes to communicate with the other person. In cryptography the actual message that has to be sent to the other end is given a special name as Plain Text. For instance, person A wishes to send "Hello Friend how are you" message to the person B. Here "Hello Friend how are you" is a plain text message.

- *Cipher Text*

Cipher Text is the message that can not be understood by anyone or meaningless message. In Cryptography the original message is transformed into non readable message before the actual message is transmitted. For example, "Ajd672#@91ukl8*^5%" is the Cipher Text produced for the Plain Text "Hello Friend how are you".

- *Encryption*

When the original text is converted into Cipher Text, it is called encryption. Cryptography uses the encryption technique to send secret messages through an insecure channel. Two things are required by the process of encryption. They are an encryption algorithm and a key. An encryption algorithm is the technique that has been used in encryption. Sender side does the encryption.

- *Decryption*

Decryption is the reverse process of encryption. The process of converting Cipher Text into Plain Text or original text is called decryption. Decryption technique is used at the receiver side to obtain the original message from unreadable message (Cipher Text). The process of decryption requires two things. They are the Decryption algorithm and a key. A Decryption algorithm is the technique that has been used in Decryption.

- *Key*

Numeric or alpha numeric text or a special symbol can be a Key. The Key is used when the encryption takes place on the Plain Text and when decryption takes place on the Cipher Text. The selection of key in Cryptography is very significant because the security of encryption algorithm depends directly on it. For example, if the Alice uses a key of 4 to encrypt the Plain Text "President" then Cipher Text produced will be "Tviwmhirx".

B. Purpose of Cryptography

A number of security goals to ensure the privacy of data, non alteration of data and so on are provided by cryptography. Today, cryptography is widely used because of the great security advantages of cryptography. Following are the various goals of cryptography.

- *Confidentiality*

The transmitted information has to be accessed only by the authorized party and not by anyone else.

- *Authentication*

The system which receives the information has to check the identity of the sender whether the information has arrived from an authorized person or from a false identity.

- *Integrity*

The transmitted information can be modified only by the party who is authorized. The given message can not be altered by anyone in between the sender and receiver.

- *Non-Repudiation*

The sender or the receiver is not able to deny the transmission.

- *Access Control*

The given information can be accessed only by the authorized parties.

C. Classification of Cryptography

Encryption algorithms have two broad categories. They are called symmetric and asymmetric key encryption.

- *Symmetric Encryption*

The same key used for encryption is used for decryption in symmetric cryptography. Thus, the key distribution has to be carried out before the transmission of information. The key plays a very vital role in symmetric cryptography because the security directly depends on the nature of key like the key length and etc. Few examples of symmetric key algorithms are DES, TRIPLE DES, AES, RC4, RC6, BLOWFISH.

- *Asymmetric Encryption*

When two different keys are used, that is one key for encryption and another key for decryption, then that mechanism is known asymmetric encryption. E.g., RSA algorithm.

II. LITERATURE SURVEY

Shraddha Dadhich explained that as security is one of the major issues in today's era, to enhance security we have cryptographic algorithms. In this paper, implementation of AES and DES cryptographic algorithms on two different platforms like WINDOWS and UBUNTU using JAVA has been taken into consideration. By this implementation, performance analysis of these two algorithms has been completed. Performance of these two algorithms depends upon various factors like number of rounds, key size and etc. But in this experimental analysis performance is evaluated considering two parameters.

1. Encryption Time
2. Decryption Time

Encryption time is the time taken by the algorithm to produce the cipher text and Decryption time is the time taken by algorithm to produce plain text from cipher text.

Experimental results for cryptographic algorithms AES and DES show, the comparison of speed of these two algorithms i.e., AES and DES, using same input string.

By analyzing the results, time taken by DES algorithm for encryption and decryption is more than AES algorithm for the same input. So, AES algorithm is fast compared to DES algorithm.

On the basis of these results the performance of AES and DES are analyzed on various operating systems also. For example, when comparing WINDOWS and UBUNTU, both the algorithms execute much faster in Ubuntu than Windows.

International Journal of Computer Trends and Technology (IJCTT), Volume 35, Number 4, May 2016.

Pooja Patil and Dr. Rajesh Bansode analyzed the limitations of various cryptographic techniques and proposed a hybrid system with hash function which is the combination of the AES, ECC and SHA256. This methodology was implemented for secure sharing of healthcare data. Text and images with different file size were taken as input. Encryption was performed on original file and it was sent to the intended receiver. Receiver decrypted that file using secret key and then matching of hash was performed. The successful hash matching indicates that data was not altered. This system performed encryption and decryption for better security of confidential data. It protected the sensitive data from unauthorized access and attacks. It provided authentication, enhanced time and validation of data integrity. So, sharing and accessing the data can be secured using this hybrid approach.

International Research Journal of Engineering and Technology (IRJET), Volume 07, Issue: 09, September 2020.

Mohsin Khan et.al. presented a survey on the Symmetric Encryption Algorithms. In the symmetric encryption algorithms one secret key is used. Since the symmetric key algorithms are more prone to attacks, they provide less security than asymmetric algorithms. But the processing time, throughput, and memory usage of this algorithms are very less. The DES, AES, Blowfish, Modified Blowfish, and Fused DES Algorithms were discussed in this paper. The more secure algorithm was blowfish. In modified blowfish the security had been increased while the processing was decreased through random numbers. 56 bits key was used by DES and hence it is a less secure algorithm and key is regenerated easily using 2^56 imaginations using a brute force. Fused DES through GA Technique and Blowfish key generation solved this drawback.

Journal of Information Technology & Electrical Engineering (ITEE), Volume2, Issue 2, April 2013.

U. Thirupalu and Dr. E. Kesavulu Reddy discussed the weakness and strength of asymmetric key algorithms and symmetric key algorithms. Based on survey, security of RC5 and RC4 was questionable but RC4 was faster than RC5. Of all these encryption algorithms, AES was more secure, efficient and faster than the other algorithms allowing 256-bit key sizes and protected against future attacks. Blowfish was replaced by Twofish. RSA is best Asymmetric key algorithm but it consumed more time for encryption and had factorization problem for large Integers in the decryption process.

International Journal of Engineering Research & Technology (IJERT), Volume 8, Issue 02, 2019.

III. EXPERIMENTAL METHODOLOGY AND ENVIRONMENT

In this experimental performance, analysis of the given algorithms on the basis of the following parameters on local system at different input size was done. Experimental parameters, platforms and key management of experimental algorithms are described in this section.

A. Evaluation Parameters

The following parameters evaluate the performance of encryption algorithm.

1. Encryption Time: The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plain text.
2. Decryption Time: The decryption time is considered as the time that a decryption algorithm takes to produce a plain text from a cipher text.

B. Evaluation Platforms

The system configuration following evaluates the performance of encryption algorithm.

1. Software Specification: Experimental evaluation on Eclipse Jee Mars with Java Development Kit 8 Update 65, Matlab version 2014, Windows 8.1 Pro 64 bit Operating System.
2. Hardware Specification: All the algorithms are tested on Intel Core i5 (2.40 GHz) fourth generation processor with 4GB of RAM with 1 TB-HDD.

C. Key Management of algorithms

Key management is the central and more important aspect for security data in cryptosystem. If the key is strong and secure from unauthorized access the cryptography algorithms will be more effective. In our experiment, we used the key size of AES is 256 bit, Blowfish is 128 bit, DES is 56 bit, RC4 is 64 bit, RSA 1024 bit.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results for encryption algorithm AES, BLOWFISH, DES, RC4, RSA are shown in table-1 which have been implemented for several input file sizes: 329 bytes, 778 bytes and 2048 bytes. Key size of each algorithm that is used in this experiment is also mentioned in the table. Good care had been given to get the results for getting higher accuracy. Hundred (100) samples of total execution time were taken. Then an average of hundred samples was taken for the measurement and comparative analysis among algorithms and for the graph plotting as well. Encryption and Decryption time are calculated in milliseconds and the input size is taken in kilobytes. All the respective observation readings are specified in Table-1 and the corresponding graphs are shown in fig.-1, fig.-2, fig.-3 and fig.-4 for all the analyzed algorithms on single system.

Table-1: Performance Comparison of Different Algorithms

S. No.	Algorithm	Key Size (bit)	File Size (bytes)	Average (100 Times) Encryption Time (Milliseconds)	Average (100 Times) Decryption Time (Milliseconds)
1	AES	256	329	287	293
			778	299	304
			2048	300	297
2	Blow-fish	128	329	293	290
			778	287	278
			2048	283	279
3	DES	56	329	284	280
			778	292	282
			2048	303	317
4	RC4	64	329	282	286
			778	283	280
			2048	313	292
5	RSA	1024	329	462	499
			778	541	450
			2048	488	491

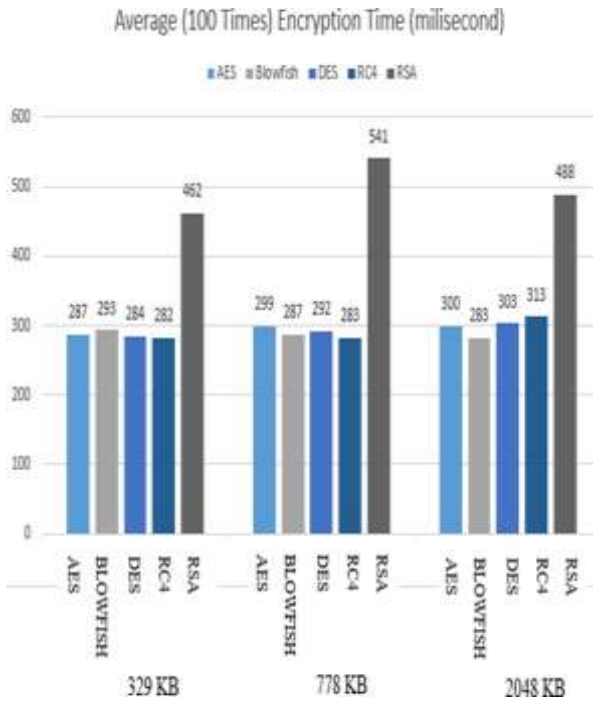

Fig.-1: Encryption Time of different Algorithms (Column Based)

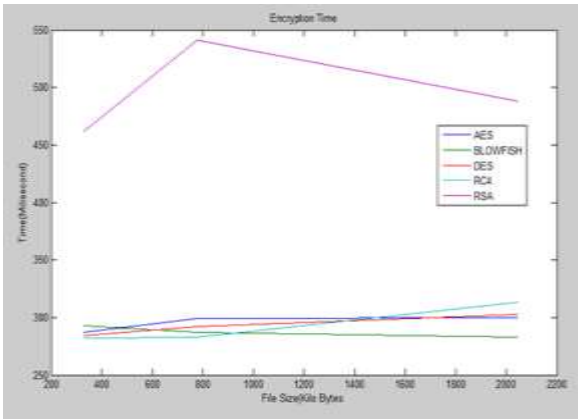

Fig-2: Encryption Time of different Algorithm (Line Based)

The encryption time is represented by fig.-1 and 2 and decryption time is represented by fig.-3 and 4 for both symmetric algorithms (AES, BLOFISH, DES and RC4) and asymmetric

algorithms (RSA). On the basis of the above figures, symmetric algorithms are better than the asymmetric algorithms. Apart from this, the proportion relation between the running time and input file size are enjoyed by all algorithms in both categories (symmetric and asymmetric), except the DES and RSA algorithms. When the file size is increased, the running time of the DES and RSA changes slightly. By analyzing table-1, time taken by RSA algorithm for both encryption and decryption process is much higher, compared to the time taken by AES, BLOWFISH, DES and RC4 algorithms.

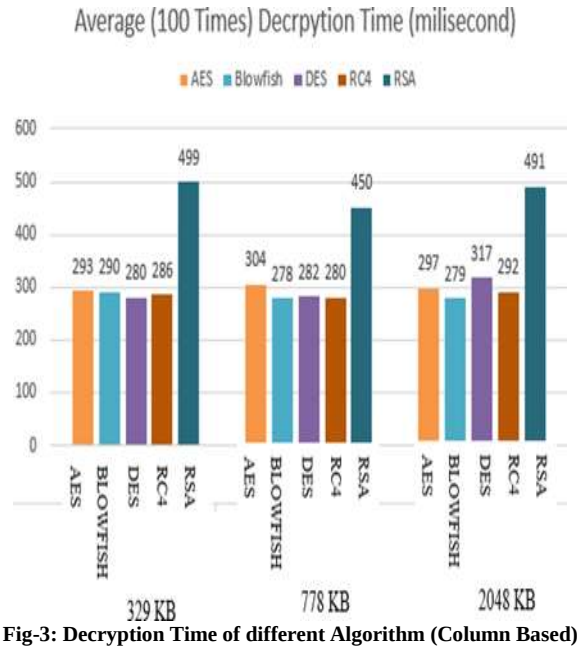

Fig-3: Decryption Time of different Algorithm (Column Based)

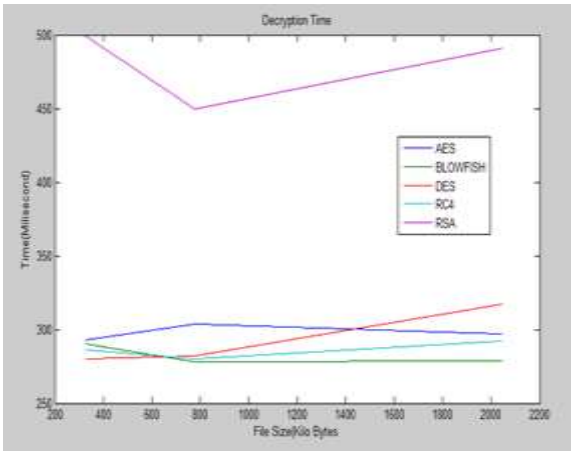

Fig-4: Decryption Time of different Algorithm (Line Based)

V. CONCLUSION

Communication security is given a good contribution by the encryption algorithms. The performance of widely used encryption techniques like AES, DES RSA algorithms were shown in this research work. Based on the text files used and the experimental result, it was decided that least encryption time is consumed by AES algorithm and longest encryption time is taken by RSA algorithm. It also showed that AES algorithm encrypts better than other algorithms. From the analytical result, AES algorithm performs better than DES and RSA algorithm. Based on the above study, this research analyzes that there is a need to develop a hybrid encryption algorithm which combines different encryption algorithms based on all suitable parameters that are used to enhance the overall security of the encryption techniques.

REFERENCES

[1] National Bureau of Standards, "Data Encryption Standard," FIPS Publication 46, 1977.

[2] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

[3] Ramesh G, Umarani. R, " Data Security In Local Area Network Based On Fast Encryption Algorithm", International Journal of Computing Communication and Information System (JCCIS) Journal Page 85-90. 2010.

[4] Shraddha Dadhich, "Performance Analysis of AES and DES Cryptographic Algorithms on Windows & Ubuntu using Java", International Journal of Computer Trends and Technology (IJCTT), Volume 35, Issue 4, pp. 179-183, May 2016.

[5] Pooja Patil and Dr. Rajesh Bansode, "Performance Evaluation of Hybrid Cryptography Algorithm for Secure Sharing of Text & Images", International Research Journal of Engineering and Technology (IRJET), Volume 7, Issue 9, pp. 3773-3778, September 2020

[6] Mohsin Khan, Sadaf Hussain and Malik Imran, "Performance Evaluation of Symmetric Cryptography Algorithms: A Survey", International Journal of Information Technology and Electrical Engineering (ITEE), Volume 2, Issue 2, pp. 1-8, April 2013.

[7] U. Thirupalu and Dr. E. Kesavalu Reddy, "Performance Analysis of Cryptographic Algorithms in the Information Security", International Journal of Engineering Research & Technology (IJERT), Volume 8, Issue 2, pp. 64-69, 2019.

[8] Iram Ahmad and Archana Khandekar, "Homomorphic Encryption Method Applied to Cloud Computing", International Journal of Information & Computation Technology (IJICT), Volume 4, Issue 15, pp. 1519-1530, 2014.

[9] A. Dharini, R.M. Saranya Devi, and I. Chandrasekar, "Data Security for Cloud Computing Using RSA with Magic Square Algorithm", International Journal of Innovation and Scientific Research (IJISR), Volume 11, Issue 2, pp. 439-444, November 2014.

[10] Vijay. G.R, A.Rama Mohan Reddy, "Data Security in Cloud based on Trusted Computing Environment", International Journal of Soft Computing and Engineering (IJSCE), Volume 3, Issue 1, pp. 2231-2307, March 2013.

[11] J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," *IEEE J. Quantum Electron.*, submitted for publication.

AUTHORS

First Author – Mr. K. Vijay Anand, MCA, M.Phil., SNMV College of Arts and Science

Second Author – Dr. D. Binu, ME, Ph.D., Sri Ramakrishna Institute of Technology

Correspondence Author – Mr. K. Vijay Anand,