Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Review on Comparative Study of Various Cryptography Algorithm

[1] Yousif Elfatih Yousif, [2]Dr.Amin Babiker A/Nabi Mustafa, [3]Dr.Gasm Elseed Ibrahim Mohammed
[1, 2] Department of Communications, Faculty of Engineering, AL-Neelain University, Khartoum, Sudan
[3] Faculty of Engineering, International University of Africa, Khartoum, Sudan

Abstract— Cryptography refers to the tools and techniques used to make messages secure for communication between the participants and make messages immune to attacks by hackers. For private communication through public network, cryptography plays a very crucial role. Cryptography is a method to provide information confidentiality, authenticity and integrity .Cryptography can be categorized into symmetric or asymmetric. In this paper we have defined and analyzed various cryptographic symmetric algorithms like DES, Triple DES, AES and asymmetric key cryptographic algorithms like RSA.

Keywords— Encryption, Decryption, Cryptography, DES, Triple DES, AES , RSA

I. INTRODUCTION

Cryptography is usually referred to as "the study of secret". Encryption is the process of converting normal text to unreadable form; while decryption is the process of converting encrypted text to normal text in the readable form.
Important aspects of encryption and decryption are privacy, authentication, identification, trust and verification. As the security demand increases thecost of cryptography algorithm increases [1]. There are two types of cryptosystems; symmetric cryptosystems and asymmetric cryptosystems. Symmetric cryptosystems use the same key for encryption and decryption. On the other hand, asymmetric cryptosystems use two different keys; a public key for encryption and a private key for decryption.
Furthermore, symmetric encryption algorithms are very efficient at processing large amounts of information and computationally less intensive than asymmetric encryption algorithms. There are two types of symmetric encryption algorithms: stream ciphers and block ciphers which provide bit-by-bit and block encryption respectively.

II. METHODOLOGY

- Comparing and analyzing the performance of various cryptography algorithms (DES, Blowfish, AES, RSA etc.) in terms of throughput, execution time, power consumption and key size.
- Analyzing the performance of the algorithm when different types of data isused.
- Comparingthe four most common symmetric key cryptography algorithms: RC2, RC4, RC5, and RC6.

III. RESULTS

No	Researchers	Topic	Contribution	Advantages	Disadvantages
1	Sombir Singh, Sunil K Maakar and Dr. Sudesh Kumar June 2013	A Performance Analysis of DES and RSA Cryptography	Comparison between the DES private key based Algorithm and RSA public key based algorithm. The main feature that specifies and differentiate one algorithm from another are the ability to the speed of encryption and decryption of the input plain text. It also includes several computational issues as well as the analysis of DES algorithm and RSA algorithm like the encryption throughput and decryption throughput.	• studied that the encryption and decryption execution time • comparison between ASE and RSA • The performance of DES is very good as compared to RSA	• Studied that the encryption and decryption execution time in one case
2	Sumitra January 2013	Comparative Analysis of AES and DES security	Comparison between AES, DES ,It is shown that both algorithms consume different times at different machines. Different machines take different times for same algorithm over same data packet, two symmetric key security algorithms AES and DES	• AES, DES analyzing time based on different file and different case • AES is more secure as	• Only studied execution time (without throughput) .

			are compared.	compare to DES. All algorithms have different speed	
3	Apoorva Yogesh Kumar July 2013	Comparative Study of Different Symmetric Key Cryptography Algorithms	This thesis provides a fair comparison between three most common symmetric key cryptography algorithms: AES, Twofish, CAST-256 and Blowfish. The comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used, as our main concern here is to study the performance of algorithms under different settings,.	• The comparison between these algorithms is based on encryption time and decryption time. • The comparison is made on the basis of three parameters speed, block size, and key size • It can be clearly seen in the graph that the blowfish is superior to other algorithms as it takes less time..	• Although when the data size is very small this difference is not clearly visible. But for file having size greater 100KB it is very clearly visible. • studied one case for comparison
4	Gunjan Gupta Rama Chawla July 2012	Review on Encryption Ciphers of Cryptography in Network Security	This paper covers the various cipher generation algorithms of cryptography which are helpful in network security This paper presents an overview of various block and stream ciphers and their algorithms, which are used in cryptography for Network security purpose. With the help of these cipher's algorithms one can generates its own cipher text algorithms by making modification into existing cipher text algorithms.	• performance evaluation of various ciphers can be done with the help of the cipher's algorithms discussed in this paper. • overview of encryption block and stream ciphers for data security.	• This paper discussed DES algorithm more than other algorithms
5	Rajinder Kaur Er. Kanwalpreet Singh April 2013	Comparative Analysis and Implementation of Image Encryption Algorithms	Due to the rapid growth of digital communication and multimedia application, security becomes an important issue of communication and storage of images. Image security has found a great need in many applications where the information (in the form of image) is to be protected from unauthorized access Encryption is one of the ways to ensure high security , In recent years, encryption technology has been developed and many image encryption methods have been used Encryption and decryption consume a considerable amount of time. This paper proposed three different image encryption techniques for color image.	• This paper describes the concept of selective encryption technique and full encryption Technique. • The proposed algorithm will expect in the best performance • Selective encryption is faster as compared to the full encryption of the data.	• All result displaying by interface of Matlab but necessary show graphs

6	Shrikant Mane Prof.R. Sathynarayana Prof.Moresh. Mukhedkar January 2014	A Survey on Various Cryptographic Algorithms	There is need to develop system which can protect data from hackers. Cryptography plays important role in the field of internet security. Now a day's many encryption algorithms are available . Such as DES, Blowfish, AES and MARS etc. Each one has their own benefit. User need to choose encryption algorithm according to their need. Every algorithm has their own strength and weakness. This paper present analysis of above algorithms with various parameters such as time required for encryption and decryption, encryption key size, power consumption, and most important security provided by algorithm.	• comparative study of different encryption algorithm were presented. • advanced encryption standard is faster than the Data encryption standard. • Blowfish good for text encryption when compare to AES but AES can be used when high security is needed.	
7	T.Gunasundari Dr. K.Elangovan February 2014	A Comparative Survey on Symmetric Key Encryption Algorithms	Cryptography is the one of the main categories of computer security that converts information from its normal form into an unreadable form. The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so. There are basically two techniques of cryptography-Symmetric and Asymmetric .This paper provides a fair comparison between four most common symmetric key cryptography algorithms: RC2, RC4, RC5, and RC6.	• detailed study of the symmetric key encryption algorithms like RC2, RC4, RC5 and RC6. • Among those algorithms the RC6 algorithm uses a variable number of bits ranging from 8 to 1024 bits and encryptsthe data 16 times. So it is impossible for a hacker to decrypt it.	• Compare between four algorithms using same technique • Symmetric key algorithms contains other algorithms not study
8	Vanya Diwan Shubhra Malhotra Rachna Jain April 2014	Cloud Security Solutions: Comparison among Various Cryptographic Algorithms	Cloud computing is emerging as a new thing and many of the organizations are moving toward the cloud but lacking due to security reasons. So secure the cloud to put the data safely without any intervention by any intruder. Cloud security implementation using various cryptographic algorithms, DES, AES, RSA and ECC.This paper describes the comparison among these algorithms**.**	• There are significant security concerns that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments. • compare various algorithms as described cloud security	• compare various algorithms but no implementation • this paper no specify the best algorithm for cloud
9	Vikas Agrawal	Analysis and Review of	Cryptography prior to the modern age was effectively synonymous with	• MREA algorithm	• In this paper

	Shruti Agrawal Rajesh Deshmukh February 2014	Encryption and Decryption for Secure Communication	encryption, the conversion of information from a readable state to apparent nonsense. The Process of Encryption and Decryption is performed by using Symmetric key cryptography and public key cryptography for Secure Communication. In this paper, we studied that how the process of Encryption and Decryption is perform in case of Symmetric key and public key cryptography using AES and DES algorithms and modified RSA algorithm.	is used to encrypt files and transmit encrypted files to other end where it is decrypted. • Main feature of this method is that it satisfies the properties of Confusion and diffusion and also has a perfect guess of encryption key makes decryption impossible.	we analyze that the process of encryption and decryption is perform by using DES, AES and RSA algorithms. But not apply and implement these processes for secure and better communication.
10	Anjula Gupta Navpreet Kaur Walia 2014	Cryptography Algorithms: A Review	Cryptography is such a way that make sure of integrity, availability and identification, confidentiality, authentication of user and as well as security and privacy of data can be provided to the user. In this paper we have defined and analyzed various cryptographic symmetric algorithms like DES, Triple DES, Blowfish, AES and IDEA and asymmetric key cryptographic algorithms like RSA. They have been analyzed on their ability to secure data, key size, block size, features.	• By Surveying many papers found that throughput value of BLOWFISH is greater than all symmetric algorithms. • Power Consumption value of BLOWFISH is least. • The next technique that is widely used to protect our information is RSA.	• This paper covers symmetric Key Algorithms more than asymmetric Key Algorithms

IV. CONCLUSIONS

This paper studied and analyzed the performance of different encryption techniques. It can be concluded that:

- The encryption/decryption speed for DES algorithms is faster than RSA.
- AES is more secure compared to DES.
- The throughput rates for BLOWFISH are greater than all symmetric algorithms.
- While the power consumption of BLOWFISH is the least among all algorithms.
- RC6 algorithm uses a variable number of bits ranging from 8 to 1024 bits and encrypts the data 16 times, therefore making it difficult for a hacker to decrypt it.

REFERENCES

[1] M. Anand Kumar and Dr. S. Karthikeyan "Investigating the efficiency of blowfish and rejindael (AES) algorithms." Published online March 2012 in MECS.

[2] Gabriela Moise "A survey on the usage of substitution Tables in DES and AES algorithms" Vol.LXI No.2/2009

[3] Shraddha Soni, Himani Agrawal,Dr.(Mrs.) Monisha Sharma "Analysis and comparison between AES and DES cryptographic algorithm" IJEIT, volume 2, Issue 6, December 2012.

[4] Sombir Singh, Sunil K Maakar and Dr. Sudesh Kumar "A Performance Analysis of DES and RSA Cryptography" IJETTCS ,Volume 2, Issue 3, May – June 2013

[5] Sumitra " Comparative Analysis of AES and DES security" International Journal of Scientific and Research Publications, Volume 3, Issue 1, January 2013

[6] Apoorva , Yogesh Kumar"Comparative Study of Different Symmetric KeyCryptography Algorithms " , IJAIEM, Volume 2, Issue 7, July 2013

[7] Gunjan Gupta , Rama Chawla " Review on Encryption Ciphers of Cryptography in Network Security" , International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 7, July 2012

[8] Rajinder Kaur, Er. Kanwalpreet Singh" Comparative Analysis and Implementationof Image Encryption Algorithms " IJCSMC, Vol. 2, Issue. 4, April 2013

[9] Shrikant Mane ,Prof.R. Sathynarayana , Prof.Moresh. Mukhedkar " A Survey on Various Cryptographic Algorithms" , IJLTET , Vol. 3, Issue 3 , January 2014

[10] T.Gunasundari, Dr. K.Elangovan "A Comparative Survey on SymmetricKey Encryption Algorithms " ,IJCSMA , Vol.2 , Issue. 2, February- 2014

[11] Vanya Diwan, Shubhra Malhotra,Rachna Jain "Cloud Security Solutions : Comparison among Various Cryptographic Algorithms " , International Journal of Advanced Research in Computer Science and Software Engineering , Volume 4, Issue 4, April 2014

[12] Vikas Agrawal, Shruti Agrawal, Rajesh Deshmukh" Analysis and Review of Encryption and Decryption for Secure Communication " , IJSER, Volume 2 Issue 2, February 2014

[13] Anjula Gupta, Navpreet Kaur Walia "Cryptography Algorithms: A Review", IJEDR , Volume 2, Issue 2 , 2014

