Comparative Analysis of Cryptographic Algorithms in Securing Data

[1]Taylor, Onate E.[2]Emmah, Victor T.
Department of Computer Science, Rivers State University, Port Harcourt, Nigeria

Abstract—*Despite the numerous cryptographic algorithms being implemented in our world today, we still encounter issues of their usage. While some are very efficient in communication across networks, others are better in file encryption such as images, text files etc. The efficiency of these algorithms varies based on the purpose of encryption. This paper focuses on the comparative analysis of modern cryptographic algorithm. In this paper, we analyzedthe Advance Encryption Algorithm (AES), Data Encryption Algorithm (DES), and Rivest Shamir Alderman (RSA) and compare them based on the following parameters namely: computation time, memory utilization and security level. A simulation program was developed to make the comparisons and result obtained shows that AES is a better solution based on computation time, memory utilization and security level.*

Key Words— *Cipher Text, Decryption, Encryption, Plain Text.*

I. INTRODUCTION

One essential aspect for secure communications is that of Cryptography. The concept of securing messages through cryptography has a long history. The history of Cryptography dates back to about 2000 B.C. Cryptography is considered as one of the oldest methods employed by ancient civilizations for secret communications.Cryptography - a word with Greek origin mean "secret writing". It refers to the science and art of transforming messages to make them secure and immune to attacks. It is the art of protecting the information by transforming it into an unreadable format in which a message can be concealed from the casual reader and only the intended recipient will be able to convert it into original text. The main goal of cryptography is to keep the data secure from unauthorized access.

II. PROBLEM STATEMENT

The problem to be solved in this work is to evaluate the cryptographic algorithms (AES, DES and RSA) using the specified parameter (computation time, memory space and security level), as to enable an optimum choice. The analysis of the project is going to cover text files of different sizes, consisting of alphabets, numbers and special characters.

III. LITERATURE REVIEW

[1] presented a paper titled Comparative analysis on different parameters of encryption algorithms (AES, RC6, IDEA, BLOWFISH).Their main aim was to analyze the performance of the most popular symmetric key algorithm. They compared the algorithm in terms of architecture, flexibility, reliability, security and limitation where *architecture* defines the structure and operation that an algorithm can perform, its characteristics and how they are implemented. *Security* of an encryption algorithm depends on the key size used to execute the encryption: generally, greater the key size, stronger the encryption. *Flexibility* defines whether the algorithm is able to endure minor modifications according to the requirements. *Limitation* defines how fine the algorithm works by making use of the computer resources available to it. After analyzing the most popular symmetric algorithm, it was observed that AES (Rijndael) was the best among all in terms of security, flexibility, memory usage and encryption performance. Although other algorithms were also competent but most of them have tradeoff between memory usage and encryption performance with few algorithms been compromised.

[2] studied about the performance of encryption algorithms (RSA, DES, 3DES, and AES) for information security and the parameters used are: key length, Round(s), Block size, Cipher Type, speed and security [3].

Table 1:Comparison table of RSA, DES, 3DES and AES.

Factors	RSA	DES	3DES	AES
Created by	Ron Rivest, Adi Shamir, and Leonard Adleman in 1978	IBM in 1975	IBM in 1978	Vincent Rijmen, Joan Daemen in 2001

Key length	Depends on number of bits in the modulus n where n=p*q	56 bits	168 bits (k1, k2 and k3) 112 bits (k1 and k2)	128,192 or 256 bits
Round(s)	1	16	48	10-128 bits key, 12-192 bits key, 14-256 bits key
Block size	Variable	64 bits	64 bits	128 bits
Cipher Type	Asymmetric Block cipher	Symmetric Block cipher	Symmetric Block cipher	Symmetric Block cipher
Speed	Slowest	Slow	Very slow	Fast
Security	Least secure	Not secure enough	Adequate security	Excellent security

The table above shows that Asymmetric Algorithms such as RSA etc. are slower than that of Symmetric Algorithms and RSA is least secure algorithm as compared to DES, 3DES and AES. In their research, they found that AES algorithm is most efficient in terms of key length, round(s), block size, cipher type, speed and security.

[4] presented a paper titled Comparative analysis of AES and RC4 algorithm for better utilization, and the performance metrics were throughput, CPU process time, memory utilization encryption and decryption time at different settings like variable key size and variable data packet size, were *encryption time* is the time that an encryption algorithm takes to produce a cipher text from a plaintext; decryption time is the time that a decryption algorithm takes to produce a plain text from a cipher text; throughput of an encryption scheme defines the speed of encryption; CPU process time is the time that a CPU is dedicated only to the particular process for calculation; memory utilization defines how much memory is being consumed while doing the encryption or decryption. After the analysis was done based on the above mentioned metrics, their experiments show that RC4 is fast and energy efficient for encryption and decryption, and they concluded that RC4 is better than AES.

IV. METHODOLOGY

The design methodology to be used in this project is the waterfall model. This model emphasis planning in early stages, it ensures design flaws are corrected before developing the code. In waterfall model, any phase in the development process begins only if the previous phase is completed. The waterfall model is chosen in this project because each phase is processed and completed one at a time.

V. AES ALGORITHM

Rijndael was developed by Joan Daemen and Vincent Rijmen, becomes U.S.'s new Advanced Encryption Standard in October 2000 declared by the National Institute of Standards and Technology. (Advanced Encryption Standard), also known as the Rijndael (pronounced as Rain Doll) algorithm, is a symmetric block cipher that can encrypt data blocks of 128 bits. It uses 10,12 or 14 rounds. The key size that can be 128, 192 or 256 bits depends on the number of rounds, but the round keys are always 128 bits. AES uses several rounds in which each round is made of several stages. At the beginning and end of cipher, AES uses term data block; before and after each stage, the data block is referred as state. States, like blocks are made of 16 bytes but normally are treated as matrices of 4X4 bytes. The entries are denoted by;

S0,0, S0,1, S0,2, S0,3,
S1,0, S1,1, S1,2, S1,3,
S2, 0, S2,1, S2,2, S2,3,
S3,0 , S3,1, S3,2, S3,3

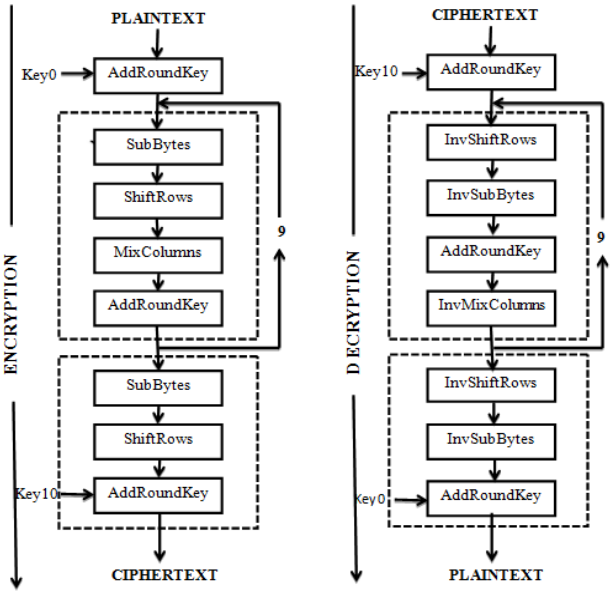

Fig 1: AES Encryption and Decryption

VI. DES ALGORITHM

Data Encryption Standard (1974), designed by IBM based on their Lucifer cipher was the first encryption standard to be published by NIST (National Institute of Standards and Technology). The DES was initially considered as a strong algorithm, but today the large amount of data and short key length of DES limits its use. DES encrypts and decrypts data in 64-bit blocks, using a 64-bit key (although the effective key strength is only 56 bits). It takes a 64-bit block of plaintext as input and outputs a 64-bit block of cipher text. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm, DES is both a block cipher and a product cipher. DES (Data Encryption Standard) algorithm purpose is to provide a standard method for protecting sensitive commercial and unclassified data. In this same key used for encryption and decryption process.

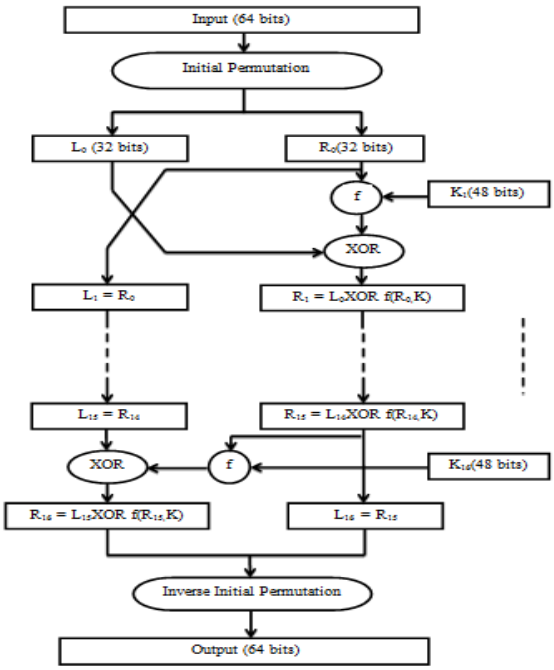

Fig 2: Diagram of DES Algorithm

VII. RSA ALGORITHM

RSA Algorithm is a Public key algorithm invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman (RSA). It supports encryption and Digital Signatures. It is the most widely used public key algorithm which gets its security from integer factorization Problem. It is relatively easy to understand and implement. RSA computation occurs with integers modulo n = p*q. It requires keys of at least 1024 bits for good security. Keys of size 2048 bit provide best security. Widely used for secure communication

Channel and for authentication to identity service provider. RSA algorithm is used to encrypt the data to provide security so that only the concerned user can access it. The diagram below shows how to generate a public and a private key.

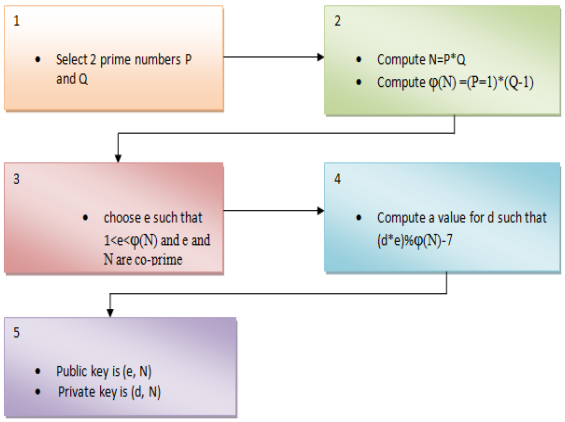

Fig 3: Generation of public and private key in RSA

After getting the public and private key, the main thing is how to encrypt and decrypt using RSA.

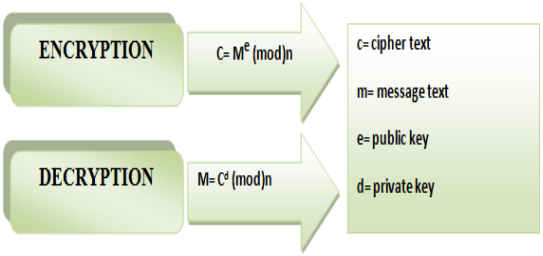

Fig 4: Encryption and decryption in RSA

VIII. RESULTS/FINDINGS

The three algorithms have been thoroughly analyzed based on the way they run, their complexities and the way they work. The program has been developed and different file size has been tested. After taking an average of the three algorithms, it was discovered that AES is the better solution based on computation time, memory utilization and security level.

1. Computational Time

The Computational time is considered the time that an encryption algorithm takes to produces a cipher text from a plain text. The analysis of this parameter led to understanding of the complexity of each of the algorithm. The complexity of AES and DES is constant time while that of RSA is dependent on the file size. We compare the execution time of each algorithm on different file sizes like text file.

Table 2: Computation time values

File sizes (bytes)	AES	DES	RSA

4.72	800	1098	367
	1703	1606	4370
5.18	634	1174	483
	1576	1677	5201
7.97	710	1524	523
	1883	2146	4098
10.1	746	1825	376
	2133	2547	5796
16.3	903	2637	510
	2797	3560	5934

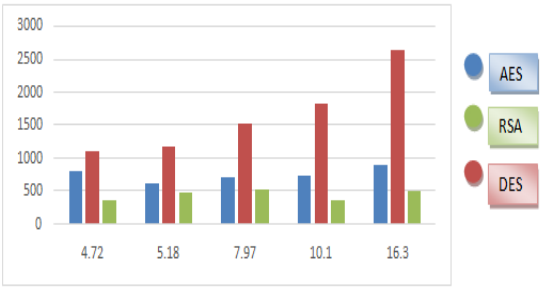

Fig 5: Comparative status of Encryption time among AES, DES and RSA

By analyzing Fig 5 which shows time taken for encryption on various size of file by three algorithms. DES algorithm takes longer time compare to time taken by AES and RSA algorithm. AES and RSA algorithm show very minor difference in time taken for encryption process.

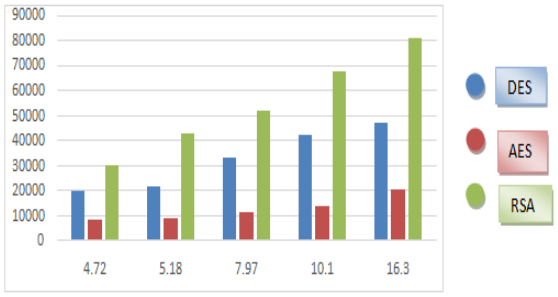

Fig 6: Comparative status of Decryption time among AES, DES and RSA

By analyzing Fig 6. which shows time taken for decryption on various size of file by three algorithms. RSA algorithm takes longer time compare to time taken by AES and DES algorithm. AES takes the least time to decrypt.

2. Memory Utilization

Table 3: Memory Utilization values

File sizes (bytes)	AES	DES	RSA
4.72	20316	14800	668
	19732	8388	30405
5.18	21592	13920	548
	21592	8868	843146
7.97	33020	13856	768
	33020	11724	52187
10.1	42068	21984	845
	42068	13988	67890
16.3	67320	38368	1078
	67320	20316	81241

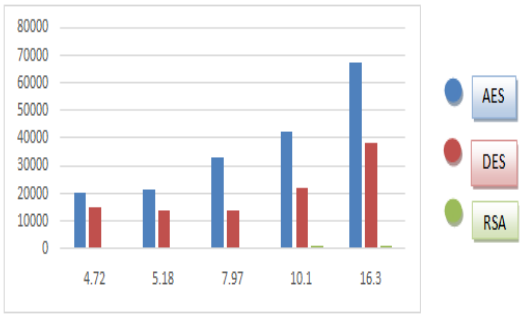

Fig 7: Comparative status of Memory utilization (Encryption) among AES, DES and RSA

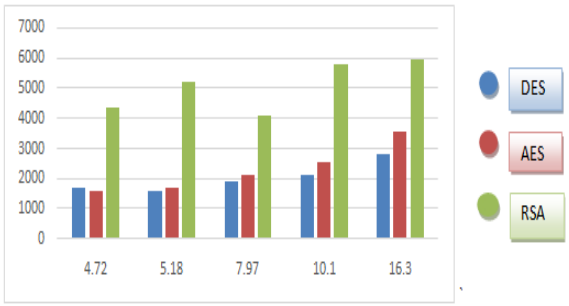

Fig 8: Comparative status of Memory utilization (Decryption) among AES, DES and RSA.

To evaluate the efficiency of a cryptographic algorithm based on memory utilization, Big*O*analysis is used to check the complexity based on the efficiency of the algorithm i.e. it checks for space and time. AES and DES are normally only working on a fixed block size and takes approximately the same time independently of the input. Thus, they operate on *O*(1) because it doesn't matter the size of the file but runs based on the key size. RSA on the other hand,

encrypt and decrypt with *O*(n) because it encrypt and decrypt based on the size of the file.

3. *Security Level*

The rate at which a particular algorithm encrypts the data is an essential parameter in analyzing the performance of encryption algorithm. An algorithm is considered to be better if it provides strong security level. This section analyzes the security levels of various cryptographic algorithms.

i. **AES:** AES provides a high security level since uses variable length key bits. It uses operations similar to the RSA modulo arithmetic operations but it can be mathematically inverted. Security of the encryption depends on how long it takes to crack and how high cost will it take an attacker to find a key. Different types of attack to crack AES like Square attack, Key attack, and Differential attack were tried, but none of them cracked AES algorithm.

ii. **DES:** Security in DES is of major concern because of the 56 bit key length. Brute force attack becomes possible with a massively parallel machine of more than 2000 nodes with each node, capable of a key search rate of 50 million keys/sec. Cryptanalysis is possible by exploiting the characteristics of DES. The weak S-boxes provide a possible mean for a cryptanalytic attack.

iii. **RSA**: The security of RSA cryptosystem is based on factoring large numbers and taking the eth root modulus of a composite n, finding a value m such that C=m^e(mod n) where (n, e) is a public key and C is the cipher text. If the attacker computes the secret exponent d from a public key (n, e) ,C can be decrypted using the standard procedure. But naturally it is time consuming to find the integer factorization in a polynomial time, which still proves RSA to be a strong algorithm.

Table 4: Comparison table between AES, DES and RSA

	Parameters	**AES**	**DES**	**RSA**
i.	Computation Time	Faster	Moderate	Slower
ii.	Memory Utilization	Requires moderate memory space	Requires least memory space	Requires more memory space
iii.	Security Level	Excellent Security	Adequate	Least Secure

IX. FUTURE WORKS

For encryption of multimedia files, Subsequent research will focus on comparative analysis of modern cryptographic algorithm that handles multimedia files.

X. REFERENCES

[1] S.Kumari and J. Chawla, Comparative Analysis on Different Parameters of Encryption Algorithms for Information Security, International Journal of Innovations & Advancement in Computer Science (IJIACS), Volume 4, Special Issue, pp. 123-129, 2015.

[2] S. Gurpreet and Supriya,A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information SecurityInternational Journal of Computer Applications, Volume6, Issue 19, pp. 33-38, 2013.

[3] H.O.Alanazi, B.B.Zaidan, A.A.Zaidan, H.A.Jalab, M.Shabbir and Y.Al-Nabhani,New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal of Computing, Volume 2, Issue 3, pp.152-157, 2010.

[4]N.Singhaland J.P.S.Raina,Comparative Analysis of AES and RC4 Algorithms for Better Utilization, International Journal of Computer Trends and Technology, 177-181, 2011.

[5] K.Ajah, M.Singh and P. Bansel, Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network. International Journal of Engineering and Technology, Volume 2, Issue 1, pp.87-92, 2012.

[6] K.Aman, J. Sudesh and M.Sunil, Comparative Analysis between DES and RSA Algorithm's: International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7,pp. 386-391,2012.

[7] DiaaSalama A. Elminaam, M.Hatem and Mohi M.Hadhoud, Performance Evaluation of Symmetric Encryption Algorithms: IJCSNS International Journal of Computer Science and Network Security, Volume 8, Issue 12, pp.280-286, 2008.

[8] S.Lalit and R.Bharti, Comparison among different Cryptographic Algorithms: Neighborhood-Generated Keys InternationalJournal of Computer Applications (0975 – 8887), Volume 73, Issue 5, pp. 144-153, 2013.

[9] S. Neetu, Cryptanalysis of Modern Cryptographic Algorithms: International Journal of Computer Science and Technology,Volume 1, Issue 2, pp.166-169, 2012.

[10] M. Mini and S.Aman,Study of Various Cryptographic Algorithms. International Journal of Scientific Engineering and Research (IJSER) www.ijser.in ISSN (Online): 2347- 3878, 1 (3): pp.1667-1672, 2013.

[11] S. Pavithra, and E.Ramadevi, (2012). Performance Evaluation of Symmetric Algorithms: Journal of Global Research in Computer Science, 3 (8): 43-45.

[12] Pasmavathi B. and Ranjitha S.A Survey Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique: International Journal of Science and Research (IJSR) Volume 2, Issue 4, pp. 170-174,2013.