Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 7 No. 2.June, 2016 - www.cisdijournal.net

Comparative Analysis of Some Selected Cryptographic Algorithms

Afolabi, A.O. & Atanda, O.G.
Department of Computer Science and Engineering
Ladoke Akintola University of Technology
Ogbomoso, Nigeria.
E-mail: adefolabius@yahoo.com, dayo.oladayoo@gmail.com
Phone: 08163099965

ABSTRACT

Encryption is the technique used to convert a plain text message into cipher text which is unreadable to human or machine. Encryption is of two types, namely: symmetric key encryption and asymmetric key encryption. Encryption scheme in which both the sender and receiver share the same key is referred to as symmetric key encryption scheme. Encryption scheme in which encryption and decryption are performed using different keys, i.e. a public key and a private key is referred to as asymmetric key encryption scheme. This paper presents a performance comparison between four popular and commonly used encryption algorithms: Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA). DES, 3DES, and AES are symmetric key encryption algorithms while RSA is an asymmetric key encryption algorithm. The comparative analysis is carried out based on their Architecture, Scalability, Flexibility, Reliability, Security and Limitation that are essential for secured communication (Wired or Wireless).The results achieved form a baseline in choosing an encryption algorithm that is more efficient and that have strength against cryptanalysis.

Keywords: Encryption, Decryption, Cryptography, Cipher, Cryptanalysis, key etc.

CISDI Journal Reference Format
Allenotor, D. (2016): Comparative Analysis of Some Selected Cryptographic Algorithms. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 7 No 2. Pp 41-52 Available online at www.cisdijournal.met

1. INTRODUCTION

In this era of universal electronic connectivity, the possibility of theft of information by hackers and eavesdroppers is very high. There is indeed no time at which security does not matter. The tremendous growth in computer systems and their interconnections via networks have increased the dependence of organizations and individuals on the information stored and communicated using these systems. There is a need to protect data and resources from disclosure and to protect systems from network based attacks. For secure communication over public network data can be protected by the method of encryption. Encryption converts that data by any encryption algorithm using the 'key' in scrambled form. Only user having access to the key can decrypt the encrypted data.

Encryption is a fundamental tool for the protection of sensitive information. The purpose of using encryption is privacy (preventing disclosure or confidentiality) in communications. The main goal of cryptography is keeping data secure from unauthorized users. Original data that is readable and understandable either by a person or by a computer is called plain text whereas the data which is unreadable to human or machine is called cipher text. The technique to convert a plain text message into cipher text is called encryption (Paar and Pelzi, 2010).

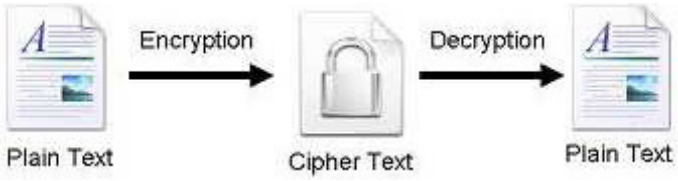

Figure 1: Encryption-Decryption Flow

Encryption is a way of talking to someone while other people are listening, but such that other people cannot understand what you are saying. Encryption algorithms play a big role in providing data security against malicious attacks. In mobile devices security is very important and different types of algorithms are used to prevent malicious attack on the transmitted data. Encryption algorithm can be categorized into symmetric key (private) and asymmetric (public) key.

In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys (Davis, 2003). Public key is used for encryption and private key is used for decryption (e.g. Rivest-Shamir-Adleman). According to (Elminaam *et al.*, 2008), asymmetric encryption techniques are about 1000 times slower than Symmetric encryption which makes it impractical when trying to encrypt large amounts of data. Also to get the same security strength as symmetric, asymmetric must use a stronger key than symmetric encryption technique Public key encryption is based on mathematical function, computationally intensive and is not very efficient for small mobile devices (Alexandre *et al.,* 2006). The present scenario uses encryption which includes mobile phones, passwords, smart cards and DVDs. It has permeated everyday life and is heavily used by much web application.

According to (Jeeva *et al.*, 2012), Encryption algorithms play a vital role in information systems. The study discovers the progress of Encryption algorithms in terms of their diversity of applications. Some of the Encryption algorithms have been developed to make transmission and storage of data more secured and confidential. Different levels of securities are offered by different algorithms depending on how difficult it is to break them (Elminaam *et al., 2010)*. If it is difficult to recover the plain text in spite of having substantial amount of cipher text then an algorithm is unconditionally secured. Dhawan (2002) compared the performance of the different encryption algorithms by conducting experiments inside .NET framework. This study provides evaluation of four of the most common encryption algorithms namely: Data Encryption Standard (DES), Triple Data Encryption Standard (3-DES), Advanced Encryption Standard (AES or Rijndael), and Rivest-Shamir-Adleman (RSA). The rest of this paper has been organized as follows: section 2 presents the research focus, section 3 presents the methodology, section 4 presents the results and discussion and section 5 presents the conclusion.

2. REVIEW OF RELATED WORKS

This paper presents a detailed study of the popular Encryption Algorithms such as RSA, DES, 3DES and AES. The use of internet and network is growing rapidly, so there are more requirements to secure the data transmitted over different networks using different services. To provide the security to the network and data different encryption methods are used (Nadeem, 2006). In this paper, a survey on the existing works on the Encryption techniques has been done. 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 and has its own significance. According to research done and literature survey it can be found that AES algorithm is most efficient in terms of speed, time, throughput, and avalanche effect. The security provided by these algorithms can be enhanced further, if more than one algorithm is applied to data. Our future work will explore this concept and a combination of algorithms will be applied either sequentially or parallel, to setup a more secure environment for data storage and retrieval.

2.1 Overview of Various Encryption Algorithms

Thakur *et al.* (2011) discussed a fair comparison between three most common symmetric key cryptography algorithms: DES, AES and Blowfish. The main concern was the performance of the algorithms under different settings, the presented comparisons takes into consideration the behavior and performance of the algorithms when different data loads are used. The comparison was made on the basis of these parameters: speed, block size, and key size. Simulation program was implemented using java programming. It was concluded that blowfish has better performance than other common encryption algorithms used. Marwaha *et al.* (2013) discussed three algorithms DES, 3DES and RSA. DES and 3DES are symmetric key cryptographic algorithms and RSA is an asymmetric key cryptographic algorithm. Algorithms have been analyzed on their ability to secure data, time taken to encrypt data and throughput the algorithm requires. Performance of different algorithms was different according to the inputs. It was concluded that confidentiality and scalability provided by 3DES over DES and RSA is much higher and makes it suitable even through DES consumes less power memory and time to encrypt and decrypt the data but on security from DES can be easily broken by brute force technique as compared to 3DES and RSA, making it the last secure algorithm.

Alam *et al.* (2013) discussed performance and efficiency analysis of different block cipher algorithms (DES, 3DES, CAST-128, BLOWFISH, IDEA and RC2) of symmetric key cryptography. Block cipher algorithms has been compared based on the factors: input size of data(in the form of text, audio and video), encryption time, decryption time, throughput of encryption and decryption of each block cipher and power consumption. It was concluded that 3DES has more power consumption and less throughput than the DES due to its triple phase characteristics. Saini (2014) make a performance analysis of various algorithms-DES, AES, RC2, Blowfish, 3DES and RC6. It was concluded from the simulation outcomes that best algorithm are those that are well known and well documented because they are well tested and well-studied. A good cryptographic system strikes a balance between what is possible and what is acceptable. Alanazi *et al.* (2010) has done the comparative analysis of three Encryption Algorithms (DES, 3DES and AES) within nine factors such as Key Length, Cipher Type, Block Size, Security, Possible Keys, Possible ASCII printable character keys and Time required to check all possible keys at 50 billion keys per second etc. Study shows that AES is better than DES and 3DES.

Arora *et al.* (2012) studied about the performance of different security algorithms on a cloud network and also on a single processor for different input sizes. This paper aims to find in quantitative terms like Speed-Up Ratio that benefits of using cloud resources for implementing security algorithms (RSA, MD5 and AES) which are used by businesses to encrypt large volumes of data. Three different kinds of algorithms are used – RSA (an asymmetric encryption algorithm), MD5 (a hashing algorithm) and AES (a symmetric encryption algorithm). The results reported in this paper conclude that the algorithms implemented on cloud environment (i.e. Google App) are more efficient than using them on single system. For both uni-processor (local) as well as cloud (Appengine) environment, RSA is the most time consuming and MD5 is the least. Highest Speed-Up Ratio is obtained in AES for low input file sizes and the Speed up Ratio falls sharply as the input file size is increased. For each input size, the Speed-Up Ratio is highest for AES, followed by MD5 and least for RSA algorithm. In the following sub-sections, we shall discuss four major cryptographic algorithms to be analyzed for their performance evaluation:

2.1.1 DES Algorithm

It was developed in the early 1975 at IBM labs by Horst Fiestel. The DES was approved by the NBS (National Bureau of Standards, now called NIST –National Institute of Standards and Technology) in 1978. The DES was standardized by the ANSI (American National Standard Institute) under the name of ANSI X3.92, better known as DEA (Data Encryption Algorithm). The DES was once a predominant symmetric-key algorithm for the encryption of electronic data. But now it is an outdated symmetric key data encryption method. DES uses 56 bits key for encryption and decryption. It completes the 16 rounds of encryption on each 64 bits block of data. Data encryption standard works on a particular principle. Huang (2008) explains that Data encryption standard is a symmetric encryption system that uses 64-bit blocks, 8 bits (one octet) of which are used for parity checks (to verify the key's integrity). Each of the key's parity bits (1 every 8 bits) is used to check one of the key's octets by odd parity, that is, each of the parity bits is adjusted to have an odd number of '1's in the octet it belongs to. The key therefore has a real useful length of 56 3bits, which means that only 56 bits are actually used in the algorithm. So it would take a maximum of 2^{56} or 72,057,594,037,927,936 attempts to find the correct key (Coppersmith, 1994). DES uses 16 rounds of a Feistel like encryption method to encrypt plain text. A key schedule is used to derive 16 keys for the successive rounds of encryption from the original key. The block diagram of one round of DES is shown in Figure 2. Even so, DES remained a trusted and widely used encryption algorithm through the mid1990s (Islam *et al.*, 2008).

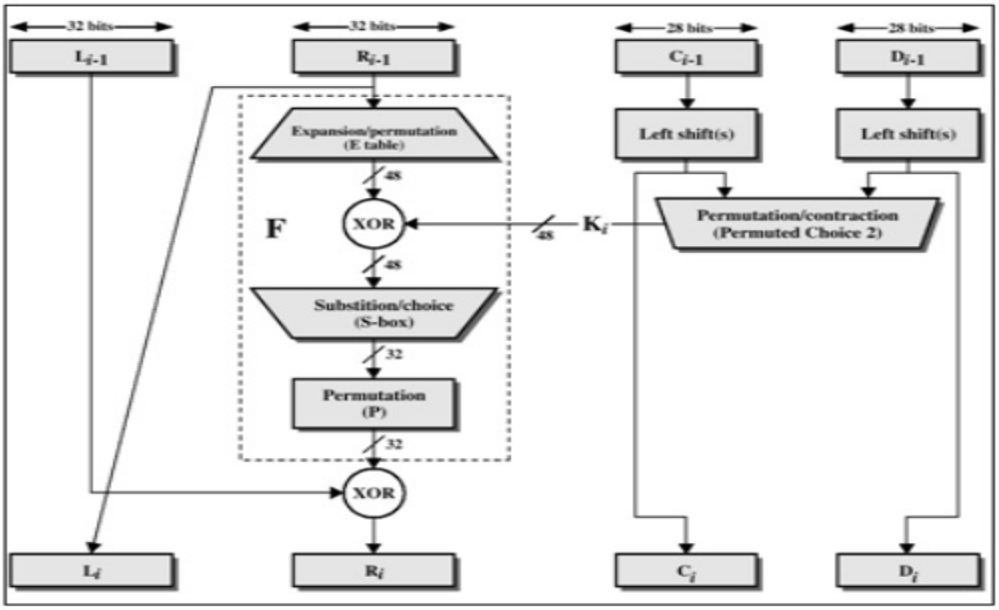

Figure 2: Depiction of One Round of DES

2.1.2 3-DES Algorithm

In cryptography techniques, Triple Data Encryption Standard (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) encryption algorithm three times to each data block. Triple-DES is also proposed by IBM in 1978 as a substitute to DES. So, 3DES is simply the DES symmetric encryption algorithm, used three times on the same data. Three DES is also called as T-DES. It uses the simple DES encryption algorithm three times to enhance the security of encrypted text (Stallings, 1999).

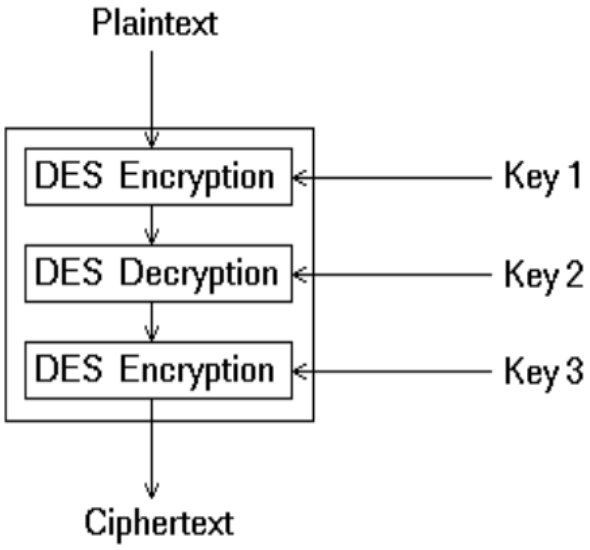

Figure 3: 3-DES Structure

In this, same data is encrypted two times more using DES. Hence, this makes the encryption stronger and more difficult to break. Triple DES is basically a Block cipher which uses 48 rounds (Three times the DES) in its computation, and has a key length of 168 bits. 3-DES also uses the Block size of 64 bits for encryption (Stallings, 1999). 3DES is a trick to reuse DES encryption algorithm but with three distinct keys. 3DES is believed to be secure up to at least 2^{112} security, but it is slow, especially in software computations (Stallings, 2005).

2.1.3 RSA Algorithm

The RSA (Rivest-Shamir-Adleman) algorithm is the most important public-key cryptosystem. It is best known and widely used public key scheme. It uses large integers like 1,024 bits in size. It has only one round of encryption. It is asymmetric block cipher. RSA is an algorithm used by modern computers to encrypt and decrypt messages. RSA is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys are used in encryption and decryption process (Kakkar and Singh, 2012). This is also called public key cryptography, because one of them can be shared with everyone and another key must be kept private.

It is based on the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who developed and publicly described it in 1978. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. Following algorithm is used in RSA; (i) Choose p and q (ii) Compute n = p * q (iii) Compute $\varphi(n) = (p - 1) * (q - 1)$ (iv) Choose e such that $1 < e < \varphi(n)$ and e and n are co-prime. (v) Compute a value for d such that $(d * e) \% \varphi(n) = 1$. (vi) Public key is (e, n) (vii) Private key is (d, n) (viii) For encryption C=me(mod n) and decryption m =cd(mod n). Hence, by following above algorithm the plain text in encrypted form or cipher text and then decrypted from cipher text to plain text.

2.1.4 AES Algorithm

In 1997, the National Institute of Standards and Technology (NIST) announced an initiative to choose a successor to DES; in 2001, it selected the Advanced Encryption Standard as a replacement to DES and 3DES. AES (Advanced Encryption standard) is developed by (Rijmen and Daeman, 2001). The Advanced Encryption Standard (AES) is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world for sensitive data encryption. AES is actually, three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128 bits, 192 bits and 256 bits, respectively. In Advanced encryption standard there are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys (Shanta, 2012).

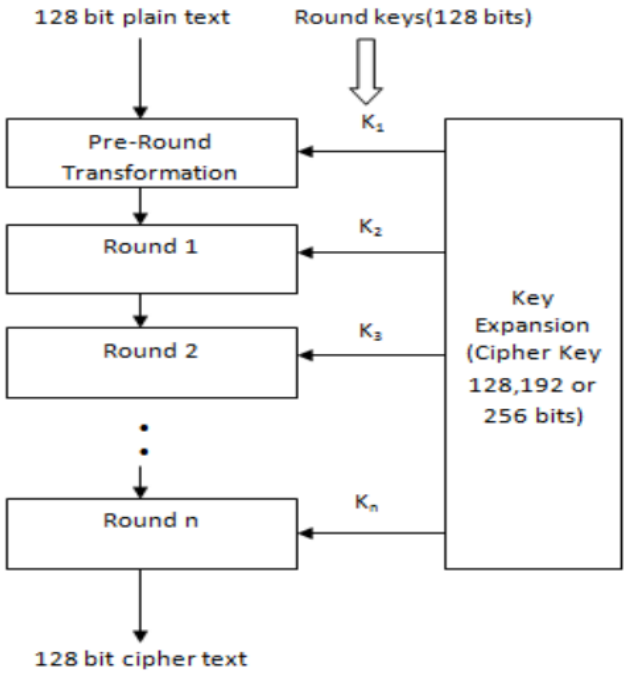

Figure 4: AES Algorithm

In each case, all other rounds are identical, except for the last round. Each round in encryption process further follows some steps to complete each round till n. Each round possess four rounds i.e. Substitute byte, Shift rows, Mix Column and Add round key. In AES encryption process, it uses different round keys. These keys are applied along with other mathematical operations on an array of data. This data is present in blocks of particular size. This array is called state array. This encryption process includes following process:

1. First derive the different round keys from cipher key.
2. Initialize the state array with block data or plaintext.
3. Start with initial state array by adding round key.
4. Perform the process of state manipulation in nine rounds.
5. After tenth round of manipulation, we will get the final output as cipher text.

By following above process we get the final encrypted text or cipher text.

3. METHODOLOGY

In this section, an exploratory research design was considered the most suitable approach in view of the nature of the problem being investigated. The purpose of the case study and the methodology to answer the study questions were also reviewed. The methodological procedures are also described. Data analysis procedures are reviewed with expected results as a representation of the study.

3.1 Simulation Setup

This simulation setup uses the provided classes in .NET environment to simulate the performance of DES, 3DES, RSA and AES (Rijndael). This implementation is thoroughly tested and is optimized to give the maximum performance for the algorithms. System is coded using C# programming language, and compiled Visual Studio as the IDE.

3.2 Experimental Design

We used a Laptop Pentium®IV CPU B980 @ 2.40 GHz processor under Windows 8 environment, in which performance data is collected. In the experiments, the laptop encrypts different file sizes ranging from 321KByte to 7.139MegaByte.

The following tasks that will be performed are shown as follows:

- A comparison is conducted between the results of the selected different encryption schemes in terms of the encryption time at two different encoding.
- A study is performed on the effect of changing packet size at power consumption during throughput for each selected cryptography algorithm.

- A study is performed on the effect of changing data types -such as text or document and images- for each cryptography selected algorithm on power consumption.
- A study is performed on the effect of changing key size for cryptography selected algorithm on power consumption.

Here, our goal is to measure the Encryption speed of each algorithm for different packet sizes. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted by the total encryption time for each algorithm. As the throughput value is increased, the power consumption of this encryption technique is decreased.By considering different sizes of data blocks (0.5MB to 20MB) the algorithms were evaluated in terms of the time required to encrypt the data block. All the implementations were exact to make sure that the results will be relatively fair and accurate.

The Simulation program shown in Figure 5 displays three outputs: Algorithm Time difference, Cipher Mode and Output byte size. After a successful execution, the data generated, encrypted and decrypted are shown. Another comparison is made after the successful encryption/decryption process to make sure that all the data are processed in the right way by comparing the generated data (the original data blocks) and the decrypted data block generated from the process.

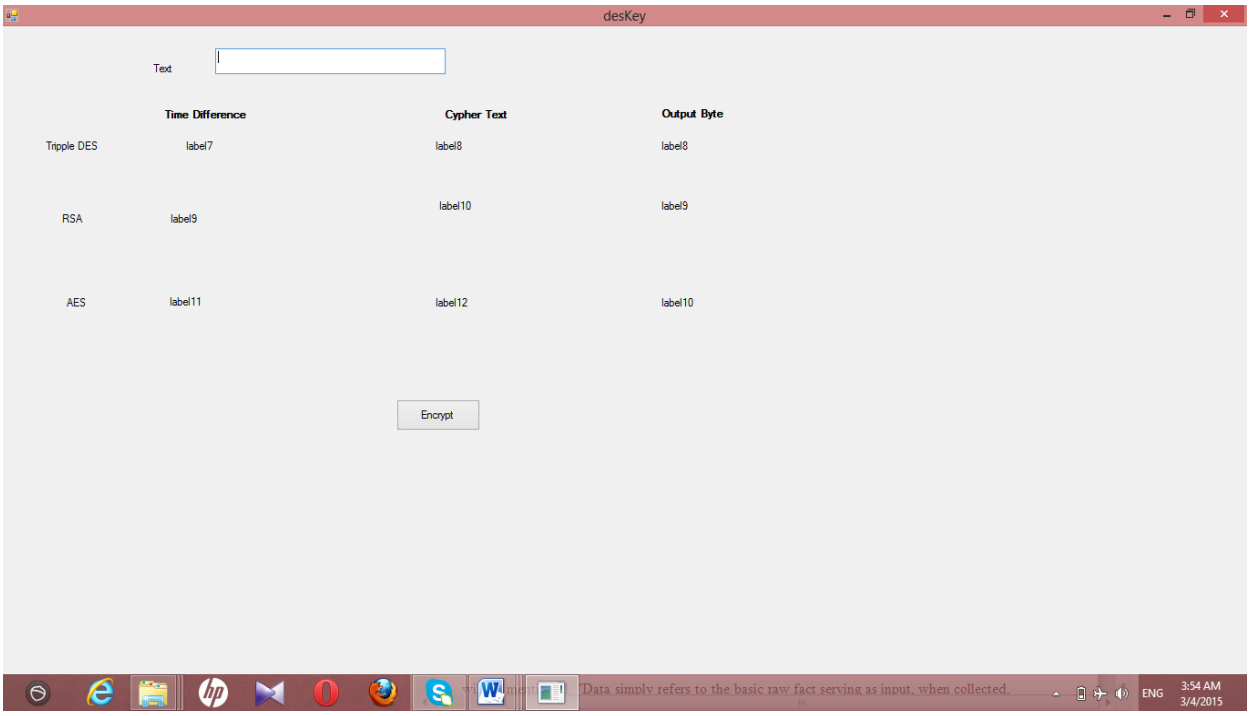

Figure 5: Simulation Program Screenshot

3.3 Evaluation Parameters

Performance of encryption algorithm is evaluated considering the following parameters.

(i) Encryption Time
(ii) Memory Usage
(iii) Output Bytes
(iv) Power Consumption rate
(v) Level of Security
(vi) Flexibility
(vii) Scalability, etc.

The Encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. The CPU process time is the time that a CPU is committed only to the particular process of calculations. It reflects the load of the CPU. The more CPU time is used in the encryption process, the higher is the load of the CPU. The CPU clock cycles are a metric, reflecting the energy consumption of the CPU while operating on encryption operations. Each cycle of CPU will consume a small amount of energy.

4. RESULT AND DISCUSSION

We have used Java and ASP.net for simulation. We have taken two parameters time and memory for the simulation setup and calculated throughput by dividing the total plaintext encrypted on total encryption time for each algorithm. We have calculated time taken by each algorithm in milliseconds and calculated memory by subtracting size of original data from encrypted data. The Tables below represents the speed of RSA, Triple DES and DES algorithm to encrypt the data of same length. Throughput of the encryption algorithms is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm. Thus, if the throughput increased than power consumption decreased. So, as speed of the DES encryption is twice the speed of RSA encryption speed. And DES also consumes small power as comparison to RSA power.

Finally, Triple DES still requires more time than DES because DES encrypts the data once and Triple DES encrypts the data three times. Triple DES has more power consumption and fewer throughputs than the DES due to its triple phase characteristics. It had been also observed that decryption of DES algorithm is better than other algorithms in throughput and less power consumption. But the aspect the DES and RSA lacks that make 3DES as our choice of algorithm is security.

4.1 Simulation Results

This section shows the results obtained from running the simulation program using different data loads. The results show the impact of changing data load on each algorithm and the impact of Cipher Mode (Encryption Mode) used. The five text files of different sizes are used to conduct five experiments, where a comparison of three algorithms DES, 3DES and RSA is performed. A cryptography too is use to conduct experiments.

Table 1: Experimental Results of five different text files

DATA	ALGORITHM	TIME (MILISEC)	MEMORY (KB)	OUTPUT BYTE
FILE 1 (68KB)	AES	02344	81,912	24
	3DES	32325	85,261	348
	RSA	23115	95,435	344
FILE 2 (105KB)	AES	04221	62,512	48
	3DES	46733	69,678	348
	RSA	52441	77,453	344
FILE 3 (124KB)	AES	06001	53,213	72
	3DES	51332	55,423	348
	RSA	45221	57,890	344
FILE 4 (235KB)	AES	07991	16,122	96
	3DES	66331	21,342	348
	RSA	75331	26,775	344
FILE 5 (435KB)	AES	09223	14,234	128
	3DES	81113	18,456	348
	RSA	66232	20,543	344

Experimental result for Encryption algorithm AES, DES and RSA are shown in Table 1, which shows the comparison of three algorithm AES, DES and RSA using same text file for five experiment, output byte for AES and DES is same for different sizes of files. By analyzing the Table 1, we noticed the AES has very smaller output byte compare to AES and DES algorithm. Time taken by RSA algorithm is much higher compare to the time taken by AES and DES algorithm. Variation in memory usage is noticed. It does not increase according to size of file in all algorithms. By analyzing Figure 6 which shows time taken for encryption on various size of text file by three algorithms i.e. AES, DES and RSA, it is noticed that RSA algorithm takes much longer time compare to time taken by AES and DES algorithm. DES algorithm consumes least time for encryption. AES and DES algorithm show very minor difference in time taken for encryption.

Figure 9 which show Memory usages and Encryption performance by DES, AES, 3DES and RSA algorithm. It is noticed that RSA algorithm memory usages are highest for all sizes of text file while memory usage is least. Figure 7 shows the size of Output Byte for each algorithm used in experiment. The result of Figure 7 shows same size of output byte for different size of text file in case of all three algorithms.

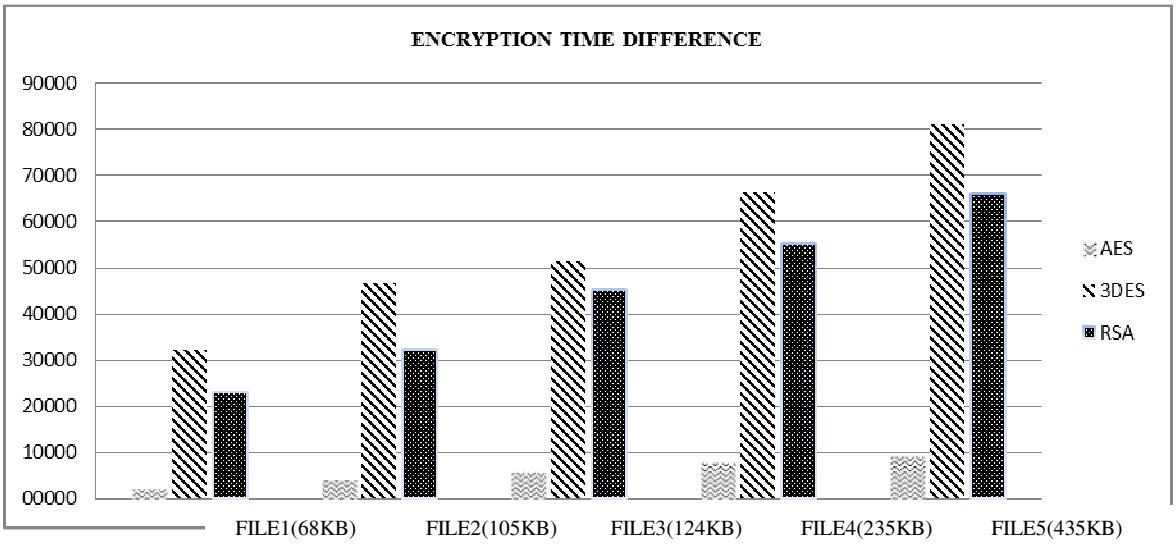

Figure 6: Comparison of Encryption Time among AES, 3DES and RSA

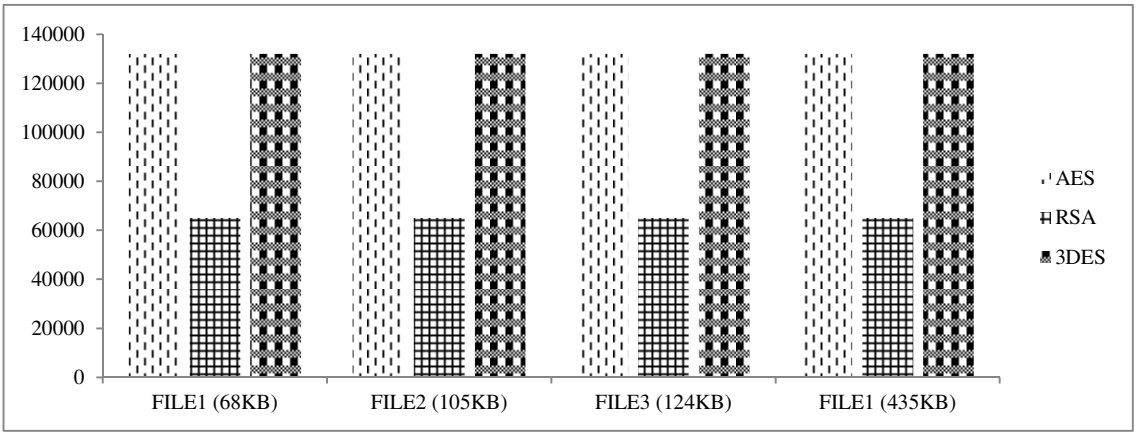

Figure 7: Comparison of Output Byte used by AES, DES and RSA

4.1.1 Level of Security

The security provided by algorithm is more dependent on the length of key being used. Greater the keys size, stronger the encryption.

Table 2: Level of security among the algorithms

Encryption Algorithms	Plain Text/Cipher Text Length	Key Length (bits)	# of Rounds (bits)
DES	64 bits	56	16
3DES	64 bits	168	48
AES	128 bits	128, 192, or 256; default 256	10, 12, 14
RSA	64bits	Variable	variable

4.1.2 Power Performance Analysis

In variable key size algorithm the power requirement can be analyzed and compared with other algorithms by varying the key size under certain limit for same logic to generate the same condition that other algorithm follows in terms of key size.

Table 3: Power consumption Analysis for different Key Size

S. No.	**Algorithms**	**Key Size**	Power Consumption(mW)
1	DES	128	89.86
2	RSA	128	1450
3	3DES	128	309.56
4	AES	128	82

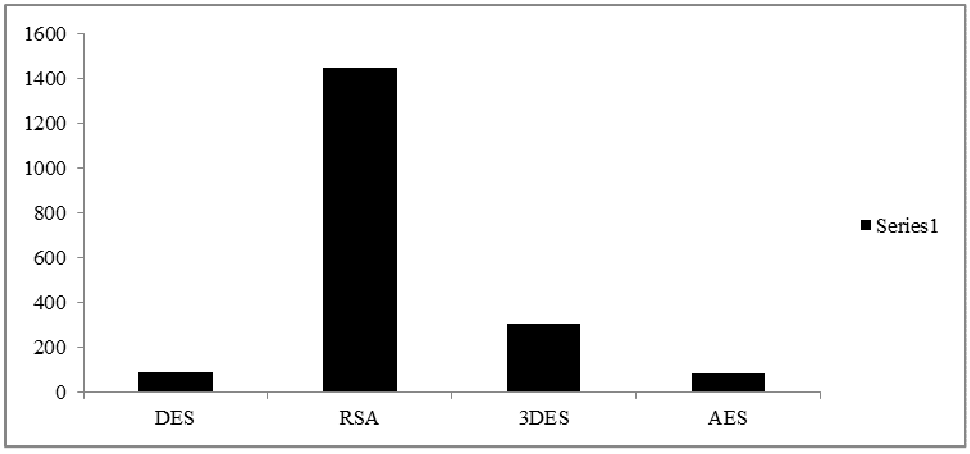

Figure 8: Power consumption chart of DES, AES, 3DEA and RSA Algorithm

Figure 8 demonstrates the Power Comparison analysis of DES, AES, 3DEA and RSA Algorithm. From figure it is clear that AES consumes negligible amount of power as compared to other algorithm. Among of these RSA consumes most amount of power; 3DEA and RSA consume more power than AES.

4.1.3 Flexibility

In Table 4, different algorithms are analyzed on the bases of their flexibility i.e. the ability of an algorithm to accept modifications according to the requirements.

Table 4: Summary of Symmetric Algorithms Flexibility

Algorithms	Flexible	Modification	Comments
DES	No	none	The structure of DES doesn't support any modifications.
3DES	Yes	168	The structure of 3DES is same as DES ,it doesn't support any changes but as it iterates DES 3 times so the key size is extended to 168 bits.
AES	Yes	128,192,256	The structure of AES(R) was extendable to the multiple of 64 bits, have same sub key size as the size of the key
RSA	Yes	128-2048	RSA has a variable key length and can be extended to 2048 bits however the key lengths must be a multiple of 32 bits

In this section scalability of different algorithms are analyzed on the basis of memory usage and encryption performance (encryption and key scheduling). The memory usage can be defined as the number of functions performed by the algorithm. The smaller the memory usage the greater will be the efficiency. Encryption rate is the processing time required by the algorithm for certain data size. Encryption rate is dependent on the processor speed, and algorithm complexity etc. The smallest value of encryption rate is desired. The hardware and software must be in accordance with the algorithm for better performance.

The graph in Figure 9 shows generic scalability (memory usage & encryption performance) of the encryption algorithms. The analyses were derived from different researches. Bruce (2000) provides a comprehensive analysis of the performance of the five AES finalist showing approximated algorithm speed against on a variety of common software and hardware platforms. So, it is concluded that for most operational systems scalability is simply another parameter that must be incorporated in to a design and must be trade off with other features (Security, architecture, flexibility and robustness). It is very difficult to compare cipher designs for scalability and even more difficult to design cipher that are scalable among all platforms.

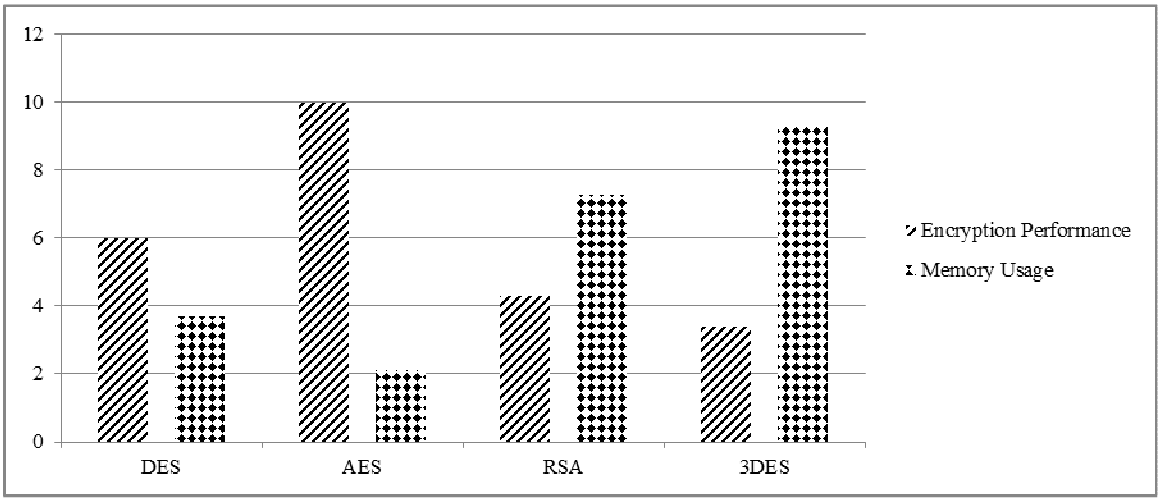

Figure 9: Generic Scalability (Memory Usage & Encryption Performance) of the Encryption Algorithms

4.2 Comparative analysis of Encryption Algorithms

We have studied different techniques used for fulfillment of data encryption purpose. There are some comparisons generated on different important features such as:

Input data size-

Different algorithm required different memory space to perform the operation. The memory space required by any algorithm is determined on the basis of input data size, number of rounds etc. The algorithm is considered best which use small memory and perform best task.

Time-

The time required by algorithm to complete the operation depends on processor speed, algorithm complexity. The less the time algorithm takes to complete its operation the better it is.

Throughput-

Throughput of the encryption algorithms is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm. Thus, if throughput increased the power consumption is decreased. Based on the reviews and research performed over the four encryption algorithm, the following is the brief outcome of this study.

Table 5: Comparison of Cryptographic Algorithms on various parameters

Parameters	DES	3DES	AES	RSA
Full Meaning	Data Encryption Standard	Triple Data Encryption Standard	Advanced Encryption Algorithm	Rivest, shamir, Adleman
Developed By and Year	IBM (1972)	IBM	Rijmen and Daemen	R. Rivest, A Shamir, L.Adleman
Type	Symmetric	Symmetric	Symmetric	Asymmetric
Key size	56 bits	192 bits	128, 192 or 256- bits	Variable
Block size	64 bits	64 bits	128, 192, 224, 256-bit	Variable
Security	Proven insecure	Secure than DES	Secure	Secure

5. CONCLUSION

Encryption algorithms play an important role in communication security where encryption time, memory usage, output byte and battery power are the major issues of concern. The performance evaluation of the selected AES, DES, 3DES and RSA encryption algorithms were carried out based on the encryption time, memory usage, output byte, power consumption rate, flexibility and security. Based on the text files used and the experimental results, it was concluded that AES algorithm consumes least encryption time and AES algorithm has least memory usage. While encryption time difference is very minor in case of AES algorithm and DES algorithm, RSA consumes large encryption time and memory space that is very high. During this analysis it was observed that AES (Rijndael) was the best among all the encryption algorithms in terms of Security, Flexibility, Memory usage, Encryption performance, and power consumption rate. Although the other algorithms were also effective but most of them have a tradeoff between memory usage and encryption performance.

REFERENCES

1. Alam M. and Khan M. (2013): "Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3(10), pp. 713-720.
2. Alanazi H., Zaidan B., Zaidan A., Jalab H., Shabbir M. and Al-Nabhani Y. (2010): "New Comparative Study Between DES, 3DES and AES within Nine Factors", *Journal of Computing*, vol. 2(3), pp. 152-157.
3. Alexandre B., Jean-Guillaume D. and Louis G. (2009): "Fault attacks in RSA public key", *Proceeding CT-RSA '09 Proceedings of the Cryptographers' Track at the RSA Conference,* pp. 414 – 428.
4. Arora P., Singh A. and Tiyagi H. (2012): "Evaluation and Comparison of Security Issues on Cloud Computing Environment", *World of Computer Science and Information Technology Journal (WCSIT)*, vol. 2(5), pp. 179-183.
5. Coppersmith D. (1994): "The data encryption standard (DES) and its strength against attacks", *IBM Journal Research Develop*ment, vol. 38(3), pp. 243 -250.
6. Davis R. (2003): "The data encryption standard in perspective", *Communications Society Magazine, IEEE,* pp. 5 – 9.
7. Dhawan P. (2002): "Performance Comparison: Security Design Choices", *Microsoft Developer Network.*
8. Elminaam D., Abdul Kader H. and Hadhoud M. (2008): "Performance Evaluation of Symmetric Encryption Algorithms", *IJCSNS International Journal of Computer Science and Network Security*, vol. 8(12), pp. 280-286.
9. Elminaam D., Kader H, Hadhoud M. (2010): "Evaluation of the Performance of Symmetric Encryption Algorithms", *International Journal of Network Security*, vol.10 (3), pp. 216–222
10. Huang Y. (2008): "Algorihtm for elliptic curve diffie-Hellman key exchange based on DNA title self-assembly", *Proceedings of 46th IEEE Theories and Applications*.
11. Islam N., Mia M., Chowdhury M. and Matin M. (2008): "Effect of Security Increment to Symmetric Data Encryption through AES Methodology", *Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*.
12. Jeeva A., Palanisamy V. and Kanagaram K. (2012): "Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms", *International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622*, Vol. 2(3), pp.3033-3037.
13. Kakkar A. and Singh M. (2012): "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network", *Published in International Journal of Engineering, and Technology (IJET)*, vol. 2(1).
14. Marwaha M., Bedi R., Singh A. and Singh T. (2013): "Comparative Analysis of Cryptographic Algorithms", *International Journal of Advanced Engineering Technology*, pp.16-18.
15. Nadeem A. (2006): "A performance comparison of data encryption algorithms", *IEEE information and communication technologies*, pp.84-89.
16. Paar C. and Pelzi, J. (2010): "Understanding Cryptography: A Textbook for Students and Practioners", *ISBN 978-3-642- 04 101-3*.
17. Rijmen, V. and Daemen, J. (2001): "AES Proposal: Rijndael" *National Institute of Standards and Technology*.
18. Saini B. (2014): "Survey on Performance Analysis of Various Cryptographic Algorithms", *International Journal of advanced Research in Computer Science and Software Engineering,* vol. 4(4), pp. 1-4.
19. Shanta J. (2012): "Evaluating the performance of Symmetric Key Algorithms: AES (Advanced Encryption Standard) and DES (Data Encryption Standard)", *published in IJCEM International Journal of Computational Engineering & Management*, vol. 15(4), pp.43-49.
20. Stallings W. (1999): "Cryptography and Network Security: Principles and Practice", *Prentice-Hall, New Jersey.*
21. Stallings W. (2005): "Data and Computer Communications", *6eWilliam 6e.*
22. Thakur J. and Kumar N. (2011): "DES, AES and Blowfish Symmetric Key Cryptography algorithm Simulation Based Performance Analysis", *IJETAE*, vol. 1(2), pp. 6-12.