International Journal of Current Research and Applied Studies, (IJCRAS)

ISSN: 2583-6781

available at https://ijcras.com/

Volume 2 Issue 4 July-August 2023

Page 103-126

A SURVEY AND APPLICATION ON SECURED DATA COMMUNICATION NETWORK USING FOUR CRYPTOGRAPHIC ALGORITHMS

Uyoo, Stephen Yavenga[1] Francis, Akogwu Alu[2] and James, Mark Ukwejeh[3]

[1]Computer Science Department, Joseph Sarwuan Tarka University, Makurdi, Nigeria
[2]Information Security Analyst, USA
[3]Directorate of Information & Communication Technology, Joseph Sarwuan Tarka University, Makurdi, Nigeria
Corresponding Author: Osai, Doris

ABSTRACT

Data Communication Networks are facing a very high threat of information security issue from hackers. Data Encryption is now a solution to close the gap and plays an important role in Data Communication Security Systems. The applied security mechanism will use some algorithms to scramble any transmitted data into unreadable text which can only be decrypted by the recipient who will have the associate key for decryption. Cryptographic algorithms involves a significant amount of computing resources such as the CPU time, Memory, Power and Computation time that may not be readily available for the expected output task. Here we will compare four cryptographic algorithms, RSA (Rivest-Shamir-Adleman), 3DES (Triple Data Encryption Standard), DES (Data Encryption Standard), and AES (Advanced Encryption Standard) algorithms. Based on the analysis of its stimulated time at the time of encryption and decryption considering parameters such as computation time and buffer size usages to determine the amount of computer resource that is utilized and how long it takes each algorithm to complete its task. Experiments results are given to analyse the effectiveness of each algorithm. In this paper we developed an application based on an Android platform which the user can encrypt the message before it is transmitted over the network. The platform's architecture is a client/server one; the server side is designed using PHP programming language and HTML, while the client side is designed using Android Technology, JSON, and MySQL at the backend and other necessary tools.

Keywords: Information Security, Encryption, decryption, private key encryption, public key encryption, cryptography, DES, 3DES, AES and RSA.

INTRODUCTION

The possibility of data damage or stolen is very high in this era of universal electronic connectivity, a tremendous escalation in computer systems and inter connectivity with networks have increased depending on company or individual base of information or data stored and communicated using this system. This calls for the need to protect the data from disclosure and to protect systems from network based hackers. The word "crypto" means secret and "graphy" means writing. Thus, the basic meaning of Cryptography is secret writing by which we can protect our confidential data in an effective manner. Cryptography is a secured scheme engaged to guard data from intruders and also save or send data in coded form (Ijaz *et al*. 2011). Cryptography is a technique deployed to transform data and also provide various security related concepts such as confidentiality, data integrity, authentication, authorization and non-repudiation. (Faiqa, et al 2017). This security mechanism usually involves encryption and decryption as well as generation of sub-keys to convert plain text into cipher text. For secure communication over public network, data can be protected by the method of encryption. Encryption converts that data using encryption algorithm with the 'key' in scrambled form. Only a user having access to the key that can decrypt the encrypted data, it is an essential tool for the protection of sensitive information (Shashi and Rajan, 2011). The purpose of using encryption is privacy (preventing disclosure) while carrying out transfer of data.

There are many techniques and tools which are used to reduce network threats. Basically encryption/decryption is the fundamental function of cryptography, which is used to hide the information from the unauthorized users so that chances of threats will be reduced. The aim of many cryptosystems is to make their data computationally infeasible to crack by intruders. It provides integrity as well as detect changes which may have occurred to the data, and offers accountability for verification of data origin.

In encryption, a simple message (the plaintext) is converted into unreadable form called cipher text (scrambled message after encryption). While decryption the cipher text is converted into plain text (original form). Many encryption algorithms are widely available and used in information security (Faiqa, et al 2017). Encryption algorithm can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. 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 (Idrizi, et al., 2013). Public key is used for encryption and private key is used for decryption (e.g. RSA). Public key encryption is based on mathematical functions, computationally intensive. There are many examples of strong and weak keys of cryptography algorithms like DES, AES. DES uses one 64-bits key while AES uses various 128,192, 256 bits keys (Abdul et al., 2014).

Cryptosystems are used to encrypt data using a cipher, and can be classified into the following broad categories:

- Symmetric encryption: Symmetric key cryptosystems are much faster than the asymmetric key

cryptosystems (Ritu and Sanjay, 2014).

- Asymmetric encryption: It is a mechanism that uses private key and public key. Public key is used for encryption while private key is used for decryption. Asymmetric encryption techniques are almost 1000 times slower than symmetric techniques because they require more computational processing power for example, RSA algorithm.
- Physical encryption: *the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage.*
- Hashing encryption: a function that meets the encrypted demands needed to secure information. Hashes are of a fixed length, making it nearly impossible to guess the hash if someone was trying to crack a blockchain.
- Quantum encryption: also known as quantum cryptography is the practice of harnessing the principles of quantum mechanics to bolster security and to detect whether a third party is eavesdropping on communications.

These methods are specifically designed to meet some of the goals of cryptography such as confidentiality, integrity and accountability.

Here we have some of the ciphers used by cryptosystems to encode data with different kind of calculation;

- Substitution cipher
- Transposition cipher
- Stegano graphic cipher
- Block cipher
- Stream cipher

The selection of key in Cryptography algorithm is core issue because the security of encryption algorithm depends directly on it.

This study evaluates four different encryption algorithms namely; AES, DES, 3DES and RSA. The performance measure of encryption schemes will be conducted in terms of encryption and decryption time such as text or document (Elminaam, et al., 2010).

This research is limited to comparing cryptographic algorithms AES, DES, 3DES and RSA to encrypt the text files for selecting which one algorithm takes lower encryption time and detecting limitation among AES, DES, 3DES and RSA algorithms. An analysis of algorithms according to their memory usage and computation time is carried out.

Related Works

This subsection describes and examines previous work done in field of data encryption. securing encryption algorithms performance, the metrics taken into consideration are processing speed, security,

block size, rounds, key length and cipher type. It also discusses the results obtained for some of the algorithms.

Neetesh and Ashish (2016) proposed an end-to-end encryption approach by proposing a terminal for sending/receiving a secure message. An asymmetric key exchange algorithm is used in order to transmit secret shared key securely to the recipient. The proposed approach with terminal device provides authentication, confidentiality, Integrity and non-repudiation. Symmetric algorithms are faster than asymmetric algorithms, thus they implemented DES, 3DES with 2 keys, 3DES with 3 keys and AES. Out of these algorithms, AES is the best algorithm to provide ciphering to the SMS during transmission. The author also proposed a GSM terminal device for providing authentication, confidentiality, integrity, and non-repudiation services for a secure communication.

Paritosh (2014) presented a new encryption technique for secure SMS transmission that was based on 3D-AES block cipher symmetric cryptography algorithm to enhance security strength on SMS for mobile communication on Android message application. The application of SMS Encryption of 3D-AES block cipher on android application has been designed and implemented. From the experiment, 3D-AES block cipher has a high decryption time when the cipher text size between 32 bit to 128 bits while it has low encryption and decryption time when message size is more than 256 bits. It was indicated that SMS encryption application using the 3D-AES block cipher will be proposed running after 256 bits.

Gurpreet (2013) integrated AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security. The study of the three popular modern encryption Algorithms such as AES, DES and 3DES were compared in this research work. Results show that AES algorithm takes less time to encrypt and decrypt the file as compared to DES and 3DES. Also, when the encryption algorithms are applied parallel to the same file then time taken to produce output file is less. Although, application of multiple algorithms increases time and space complexity of the system, but security of the system has become manifolds.

Diaa et al. (2010) presented a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are AES, DES, and 3DES, RC6, Blowfish and RC2. Several points can be concluded from the simulation results. First, in the case of changing packet size, it was concluded that Blowfish has better performance than other common encryption algorithms used, followed by RC6. Secondly, 3DES still has low performance compared to algorithm DES. Thirdly, RC2 has disadvantage over all other algorithms in terms of time consumption. Fourthly, Diaa et al. (2010) concluded AES has better performance than RC2, DES, and 3DES. In the case of audio and video files they found that the result is the same as in text and document. Finally, in the case of changing key size they found that that higher key size leads to clear change in the battery and time consumption.

Advanced encryption standard (AES)

After looking up the vulnerabilities in DES and 3DES, the National Institute of Standard and Technology (NIST) developed a new algorithm called Advanced Encryption Standard (AES) as a replacement to the

two algorithms. The AES algorithm is comparatively more secure and has a strong avalanche effect. Attackers cannot easily decrypt the encrypted text by the brute force attack; therefore, AES has been used in many applications (Oh et al., 2010). AES algorithm can support any combination of data (128 bits) and key length of 128, 192, and 256 bits. The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length. During encryption-decryption process, AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys in order to deliver final cipher-text or to retrieve the original plain-text (Gurjeevan et al., 2011). AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a matrix of the order of 4×4 that is called the state. For both encryption and decryption, the cipher begins with an Add Round Key stage. However, before reaching the final round, this output goes through nine main rounds, during each of those rounds four transformations are performed; 1) Sub-bytes, 2) Shift-rows, 3) Mix-columns, 4) Add round Key. In the final (10th) round, there is no mix-column transformation. Decryption is the reverse process of encryption and using inverse functions: Inverse Substitute Bytes, Inverse Shift Rows and Inverse Mix Columns (Gurpreet, 2013).

Alanazi et al. (2010) presented 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. The study also shows that AES is better than DES and 3DES.

Rivest-shamir-adleman (RSA) encryption algorithm is the most important public-key cryptosystem. It is the 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 has an 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 two different keys are used in encryption and decryption process. 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 (Kakkar and Singh, 2012). A user of RSA creates and then publishes the product of two large prime numbers (P*Q), along with an auxiliary value (I), as their public key. The prime factors (P*Q) must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. 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 (Kakkar and Singh, 2012).

In RSA cryptographic algorithm the main disadvantage is its encryption speed. It consumes lot of time to encrypt data. Actually, this is the disadvantage of asymmetric key algorithms because of the use of two asymmetric keys. It provides good level of security but it is slow for encrypting files. Another threat in this algorithm is fake key insertion at decryption level so the secret key should be private and correct to achieve the encryption in successful manner (Rajdeep and Rahul, 2015).

Kumar and Singh (2012) proposed a new method for node's authentication in wireless sensor networks using RSA. RSA algorithm is applied into source node, intermediate and destination node. The proposed algorithm generates private and public keys. The cipher text is created, which is encrypted using public key and a private key is sent to the receiver. After encryption, a packet is sent to intermediate node, which sends it to the destination node. The destination node will finally decrypt it using private key. Analysis of scheme is conducted in MATLAB, and results show that the technique is effective in terms of energy efficiency and data transfer.

Seth and Ranja (2011) performed a comparative analysis of three algorithms; RSA, DES and AES while considering certain parameters such as computation time, memory usage and output byte. These parameters are the major issue of concern in any encryption algorithm. Experimental results show that DES algorithm consumes least encryption time and AES algorithm has least memory usage while encryption time difference is very minor in case of AES and DES algorithm. RSA consumes longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm (Seth and Ranja, 2011).

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. Their aim is to provide the comparative analysis of the different algorithm such as AES, DES and 3DES which are used by businesses to encrypt large volumes of data. Cyber security and protection is one of the most important issue. As relation between user and internet is increasing rapidly the chances of theft also increase, so there are more requirements to secure the data transmitted over different network using different services. To provide the security to the network and data different encryption methods are used. In this paper, a survey on the existing algorithms on the encryption techniques are useful for real time encryption. Each technique is unique in its own way , which might be suitable for different applications and services and has its own significance. According to research done and literature survey it can be found that the AES algorithm is most efficient in terms of speed, time, throughput, and etc. These parameters are vital for any Encryption Algorithm to measure the standard. Experimental results show that DES algorithm consumes least encryption time and AES algorithm has least memory usage while encryption time difference is very minor in case of AES and DES algorithm. RSA consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm.

Zaran et al. (2016) studied about the performance of Symmetric Encryption and Asymmetric Algorithms. Their work provides evaluation of Symmetric key algorithms: AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6, TEA, MARS, IDEA, SERPENT, TWO FISH, BLOW FISH and Asymmetric key algorithms: DH, SSL, RSA, SSH. A comparison has been conducted at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. Experimental simulation shows results. The analysis is based on the architecture of algorithm, the security aspects and the limitation they have. The comparison clearly states that though asymmetric algorithms are superior in security, they take more time for

processing and requires more memory.

Faiqa et al. (2017) compare some of the symmetric algorithm such as DES, AES, RC5,Two fish and some asymmetric algorithm such as ECC and RSA, they observed AES works with less complexity and has high security level while compare to DES it taken time very less. Prerna et al. (2013) compares the performance evaluation of various cryptographic algorithms. On the basis of parameter such as scalability, inherent vulnerability, power consumption and deposit keys. Study shows that AES is better than DES and 3DES.

Rajadeep et al. (2015) compared two most widely used symmetric encryption techniques i.e. data encryption standard (DES) and advanced encryption standard (AES) on the basis of key length, number of rounds, block size(bits), attack found, level of security and encryption speed, memory required for implementation and simulation time required for encryption. 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, DES is highly susceptible to linear crypto analysis attacks. It is exposed to brute force attack because of weak keys, 3DES is vulnerable certain variation of meeting on the middle attacks. It is also exposed to differential and related key attacks.

Zaran et al. (2016) AES is ideal for encrypting messages sent between objects via chat-channels, and is useful for objects that involve monetary transactions. Studied the various techniques and algorithms used for the data security in MN (Multinode Network). It has been observed that the strength of system depends upon the key management, type of cryptography (public or private keys), number of keys, number of bits used in a key. Longer key length and data length consumes more power and results in more heat dissipation. Larger the number of bits used in a key, the more secure the transmission. All the keys are based upon the mathematical properties and their strength decreases with respect to time. The keys having more number of bits requires more computation time which simply indicates that the system takes more time to encrypt the data. To secure the communication key size is the most important parameter in symmetric and asymmetric cryptography. The key size of symmetric cryptography is less than the asymmetric cryptography which makes symmetric cryptography less secure for more sensitive data. Faiqa et al (2017).

Communication Security

Cryptography provides a number of security goals to avoid a security issue. Due to the security advantages of cryptography widely used today. The following are the different goals of cryptography (Srinivas et al., 2014):

i. **Confidentiality:** Nobody can read the message not including the future receiver. Information in computer information is transmitted and has to be contacted only by the authorized party and not by unauthorized person.

ii. **Authentication:** This process is proving one's identity. The information received by system then checks the identity of the sender that whether the information is incoming from an authorized person or unauthorized person or wrong identity.
iii. **Integrity:** Only the authorized party is modifying the transmitted information or message. Nobody can change the given message.
iv. **Non-Repudiation:** This is a mechanism to prove that the sender really sent this message. So if any sender denies that he doesn't send the message; this method does not allow doing such type of action to sender.
v. **Access Control:** Only the authorized parties are capable to contact the given information.

(II). Algorithms in this Survey

Encryption is a well-known technology for protecting sensitive data. Use of the combination of Public and Private Key encryption to hide the sensitive data of users, and cipher text retrieval. Arora et al., (2012)
a) Data Encryption Standard (DES)

Shashi and Rajan (2011), DES algorithm is the most widely used encryption technique which was developed in the early 1995 at IM labs by Horst Fiestel. 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, (Pavithra S. and Ramadevi E., 2012). The DES was once a predominant symmetric-key algorithm for the encryption of electronic data. But now it is an out-dated symmetric key data encryption method. DES algorithm does not provide the strong security, because of the many attacks bombarded on the DES.

Steps Involved in DES Algorithm

Encryption

1. DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64-bit block. (Rajdeep and Rahul, 2015).
2. The plaintext block has to shift the bits around.
3. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
4. The plaintext and key are processed by following.
   i. The key is split into two 28 halves
   ii. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
   iii. The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed key used to encrypt this round's plaintext block.
   iv. The rotated key halves from step 2 are used in next round.
   v. The data block is split into two 32-bit halves.
   vi. One half is subject to an expansion permutation to increase its size to 48 bits.
   vii. Output of step 6 is exclusive-OR'ed with the 48-itcompressed key from step 3.
   viii. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.

ix. Output of step 8 is subject to a P-box to permute the bits.

x. The output from the P-box is exclusive-OR'ed with other half of the data block. k. The two data halves are swapped and become the next round's input.

DES Data Encryption Standard

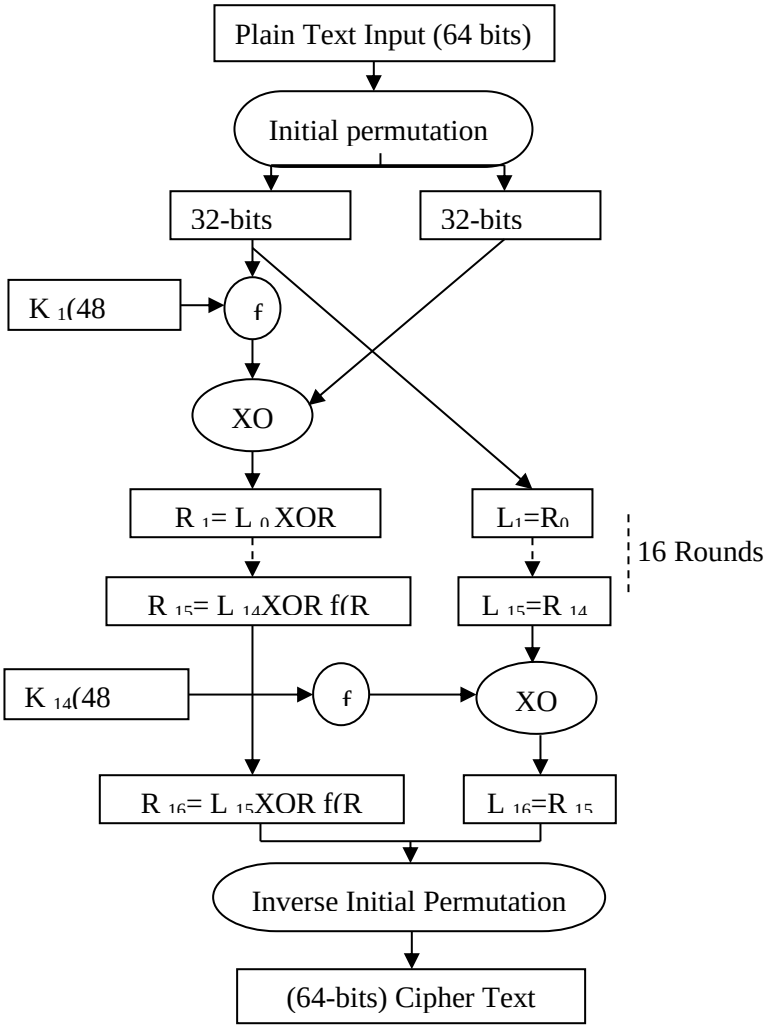


Figure 1: Diagram of DES Algorithm

b) Triple DES (3-DES)

3DES is a symmetric-key block cipher, derived from the DES and it uses three different key that means which applies the Data Encryption Standard (DES) three times to each data block. Uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. 3-DES simply increases the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits

because of 56 bit with three times. 3-DES involves using three 64-bit DES keys (Key1, Key2, Key3) in Encrypt-Decrypt- Encrypt (EDE) mode, which means, the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3. The 3-DES is a trick to reuse DES encryption algorithm but with three distinct keys. (Rajadeep et al., 2015).

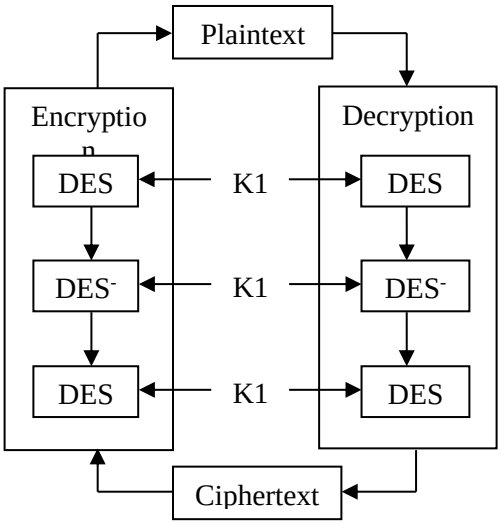


Fig 2: General Depiction of 3DES

c) Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) AES algorithm is not only security but also for great speed. Both hardware and software implementation are faster. AES is also block cipher algorithm based on fiestel network, to replace DES in 2001. AES is actually, three block ciphers AES-128, AES-192, AES-256.Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128 bits, 192 bits, 256 bits respectively The 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. Rajadeep et al[13].. During encryption-decryption process, AES system involves 10 rounds for 128-bit keys, 12 round for 192-bit keys, and 14 round for 256-bits in order to deliver final cipher-text or to retrieve the original plain-text. It can be implemented on various platforms specially in small devices. It is carefully tested for many security applications.

Algorithm Steps:

These steps are used to encrypt 128-bit block of an AES

1. The set of round keys from the cipher key.
2. Initialize state array and add the initial round key to the starting state array.
3. Perform round = 1 to 9: Execute Usual Round.
4. Execute Final Round.
5. Corresponding cipher text chunk output of Final Round Step

Usual Round: Execute the following operations which are 1).Sub Bytes 2).Shift Rows 3).Mix Columns 4).Add Round Key. Different type of attack to crack AES like square attack, key attack, differential attack were tried, but none of them cracked AES algorithm, and also consider as impervious to all attacks.

Each round consists of following four steps:

i) **Substitute Byte:** The first transformation, sub bytes is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.
ii) **Shift Rows:** It is a simple byte transposition, the bytes in the last three rows of the state, depending upon the row location, are cyclically shifted. For 2nd row, 1 byte circular left shift is performed. For the 3rd and 4th row 2-byte and 3-byte left circular left shifts are performed respectively.
iii) **Mixcolumns :** This mix columns transformation operates at the column level; it transforms each column of the state to a new column.
iv) **Addroundkey:** Add Round Key. Proceeds one column at a time. Add key round adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition

Final Round:

Final Rounds execute the operations described in algorithm steps above.

i) Sub Bytes
ii) Shift Rows
iii) Add Round Key, using K(10)

(AES) Encryption:

Each round consists of the following steps:

i. **Sub Bytes:** The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.
ii. **Shift Rows:** In the encryption, the transformation is called Shift Rows.
iii. **Mix Columns:** The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.
iv. **Add Round Key:** Add Round Key proceeds one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition.

The last step consists of XO Ring the output of the previous three steps with four words from the key schedule. And the last round for encryption does not involve the “Mix columns” step. (Hamdan et al., 2010).

(AES) Decryption

Decryption involves reversing all the steps taken in encryption using inverse functions like

i) Inverse shift rows,
ii) Inverse substitute bytes,
iii) Add round key, and
iv) Inverse mix columns.

The third step consists of XO Ring the output of the previous two steps with four words from the key schedule. And the last round for decryption does not involve the “Inversemix columns” step.

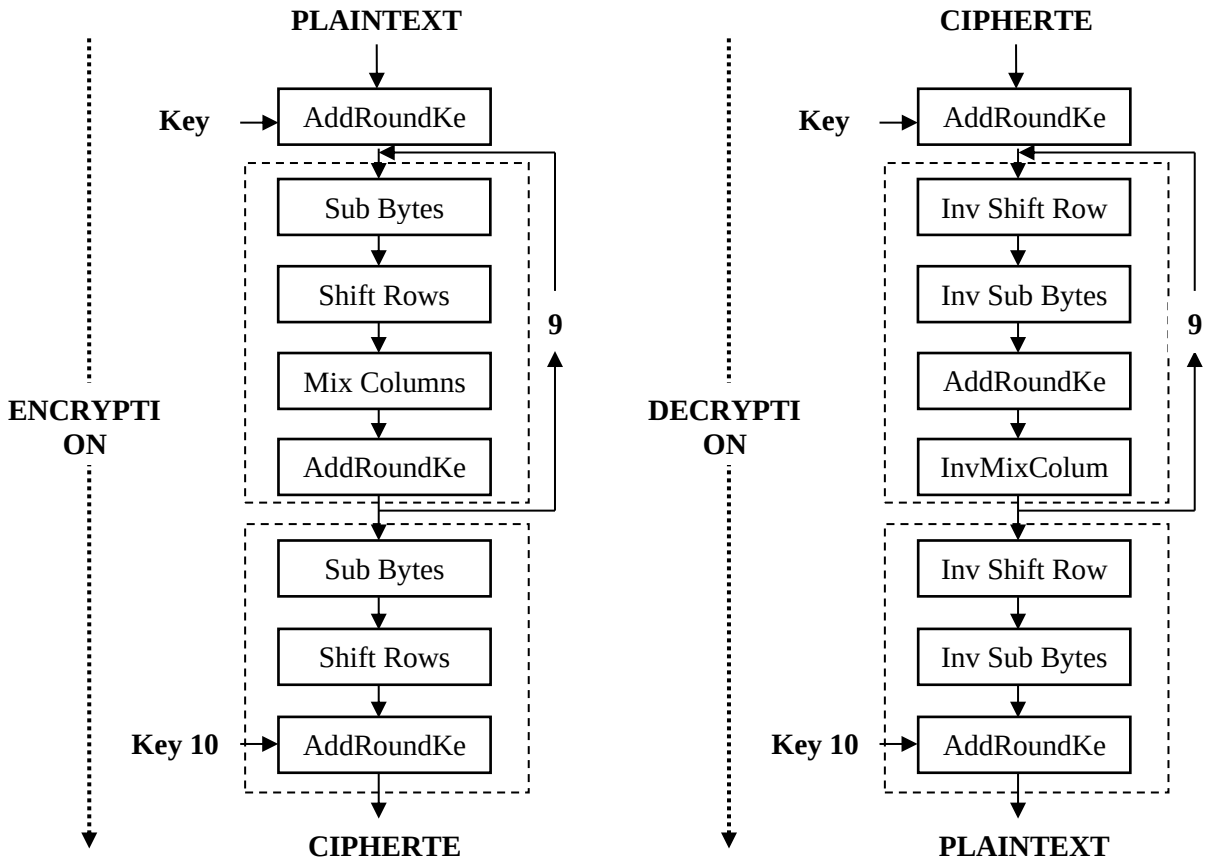


Figure 3: AES Encryption and Decryption Diagrammatic Algorithm

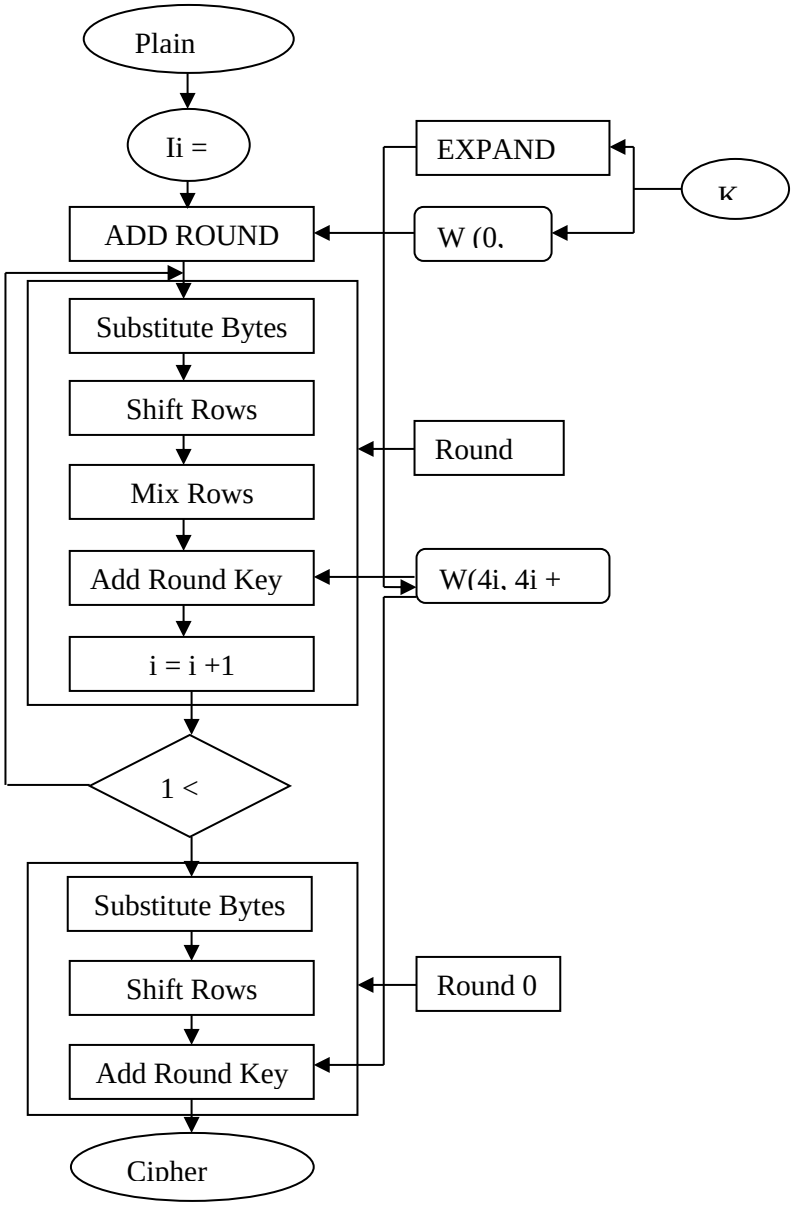


Fig 4: AES (Advanced Encryption Standard) process

d) Rivest-Shamir-Adleman (RSA)

RSA is a widely used Public-Key algorithm. It is an algorithm that encrypts data to provide security so that only the concerned user can access it. RSA algorithm involves these steps:

1. Key Generation
2. Encryption
3. Decryption

(i) Key Generation

Before the data is encrypted, Key generation should be done using the following Steps: (Kumar et al., 2012).

Generate a Public/Private Key Pair:

1. Generate two large distinct primes p and q
2. Compute n = pq and φ = (p − 1)(q − 1)
3. Select an e, 1 < e < φ, relatively prime to φ.
4. Compute the unique integer d, 1 < d < φ where ed ≡φ 1.
5. Return public key (n, e) and private key d

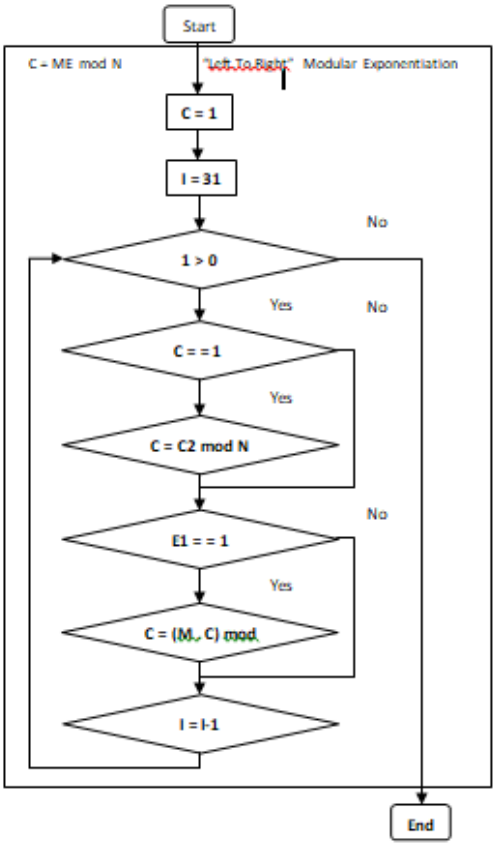
(ii)Encryption

Encryption is the process of converting original plain text (data) into cipher text (data). Encryption with key (n,e)

1. Represent the message as an integer m € {0, . . . , n − 1}
2. Compute c = me

(iii) Decryption mod n

Decryption is the process of converting the cipher text (data) to the original plain text (data). (Kakkar, A. and Singh, M. 2012).



Decryption with key d: compute m = cd mod n

Figure 5: RSA Encryption and Decryption Flowchart

Over time lots of algorithms have been studied considering the weakness and strength of the current methods to secure data. These algorithms are classified under the symmetric and asymmetric algorithms. Some of the results obtained from published papers give more insight about the performance of the compared algorithms such as AES, DES, 3DES, RSA, Blowfish algorithms etc. In the table below a comparative study between AES, DES, 3DES and RSA is presented in to different parameters, which are Algorithm, key size, Block size, Number of Rounds, Encryption, Decryption, Power consumption, Hardware and Software implementation, and the security of data against attacks are discussed.

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

Parameters Analysed	**AES**	**DES**	**3DES**	**RSA**
Developed By	Vincent Rijmen, Joan Daemen in 2001	IBM In early 1970 and published in 1977.	IBM in 1978	Ron Rivest, Shamir and Leonard Adleman in 1978
Key Size or length	128, 192, and 256 bits	56 bits	168 bits (k1, k2 and k3) 112 bits (k1 and k2)	Greater than 1024
Rounds	10-128 bit key, 12-192 bit key 14-256 bit key	16	48	1
Block size	128 bits	64 bits	64bits	Minimum of 512 bits
Type of algorithm	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Asymmetric Block Cipher
Key used	Same key used for Encryption	Same key used for Encryption and	Same key used for Encryption	Different key used for Encryption and

	and Decryption process	Decryption process	and Decryption process	Decryption process
Speed	Fast	Slow	Very slow	Slow
Encryption	Faster	Moderate (less than AES)	Moderate (greater than DES)	Slower
Decryption	Faster	Moderate	Moderate	Slower
Power consumption	low	Low	Low	High
Hardware and Software implementation	Faster and efficient	Better in hardware than in software	Moderate in hardware than in software	Not very efficient
Security attack	Excellent security	Inadequate, (not secured enough)	Adequate security	Timing attack (least secured)
Ciphering and deciphering key	Same	Same	Same	Different
Scalability	Not scalable	It is scalable a algorithm due to its varying key size and block size	Scalable algorithm	Not scalable
Deposit of keys	Needed	Needed	Needed	Needed
Inherent vulnerabilities	Brute forced attack	Brute forced, linear and differential cryptanalysis attack	Brute forced, linear and differential cryptanalysis attack	Brute forced and oracle attack
Simulation speed	Faster	Faster	Faster	Faster
Trojan horse	Not approved	No	No	Not
Ciphering and Deciphering algorithm	Different	Different	Different	Same

DISCUSSION

Analysis of Cryptographic Algorithms and Transmission of Exam Results

An Android application is developed and technologies used include PHP, JSON, XML, REST and MySQL. The Server-side application that is responsible for storing Student's result and sending it to the desired Student is designed using PHP codes and the data entry and exit point is designed using JSON codes. REST Service is created to convert and manage data leaving the PC platform for the phone platform and vice versa. The mobile application is designed using Android and XML to support modern day gadgets while all data is stored and managed using the MySQL database. Also, the compared cryptography algorithms are implemented using java. The front end is developed using Net beans IDE 8.1 and the back end is implemented using MySQL. This data communication uses Advanced Encryption Standard algorithm for both encryption and decryption of messages and provides a highly secured communication over public network proven by the experiments carried out.

Experiments indicate the evaluation of four algorithms RSA, DES 3DES and AES using same text file for the tests, RSA, DES 3DES and AES algorithms are tested on three parameters; encryption/decryption, time and buffer size usage for the same file. We found that RSA algorithm takes much longer time compared to time taken by DES, 3DES and AES algorithms. AES algorithm consumes least time for encryption. However, DES has the lowest decryption time**.** DES and AES algorithm show very minor difference in time taken for encryption and decryption process. Buffer size usages by RSA, DES, 3DES and AES algorithm shows that RSA algorithm buffer size usage is the highest for all sizes of document files.

Based on the simplicity and ease of administration, the designed system for both the administrator and student/client, this model is useful for authentication, confidentiality, integrity and efficiency of a students' results transmission system in the Nigerian Education system.

Evaluation of the System

For certainty of the developed model to achieve its set objective, the selected encryption AES, DES, 3DES and RSA algorithms are evaluated for performance. The encryption algorithms are tested on three parameters; encryption time, decryption time and buffer size usage to determine the amount of computer resource that is utilized and how long it takes to complete certain tasks using same text file for the experiments carried out. The encryption time is considered to be the time that an encryption algorithm takes to generate a cipher text from a plain text, which is calculated by the throughput of an encryption scheme; **[Total plaintext in bytes encrypted divided by the encryption time]. [Decryption time is the time taken to produce a plain text from cipher text].** The results of the experiments are presented in Tables 2, 3, 4, and 5. Experimental results obtained show the effectiveness of each algorithm towards proposing an efficient system for a secure communication.

Analysis for encryption and decryption time shows that, RSA algorithm takes much longer time compared to time taken by DES, 3DES and AES algorithm. AES algorithm consumes least time for encryption followed by DES and 3DES. DES and AES algorithm show very minor difference in time taken for encryption and decryption process as compared to 3DES.

The buffer size which is the variation in memory usage is also evaluated as shown in Table 4 with respect to AES, DES, 3DES and RSA algorithms. It was suggested that RSA algorithm buffer size usages are highest for all sizes of text files and the DES has very smaller buffer size usage compared to RSA, 3DES and AES algorithms. The summary of the result presented in Table 5 based on the average computation time indicate that AES is faster and more efficient than DES, 3DES and RSA for a secured communication.

Table 2: Encryption Time of the System

No of Experiments	Algorithms	Data length	Encryption time(s)
1	AES	723	0.0028
	DES	723	0.0066
	3DES	723	0.0069
	RSA	723	0.0353
2	AES	577	0.0018
	DES	577	0.0020
	3DES	577	0.0023
	RSA	577	0.0130
3	AES	428	0.0015
	DES	428	0.0014
	3DES	428	0.0015
	RSA	428	0.0060

4	AES	306	0.0012
	DES	306	0.0013
	3DES	306	0.0014
	RSA	306	0.0045

Table 3: Decryption Time of the System

No of Experiment	Algorithms	Data length	Decryption time(s)
1	AES	723	0.0057
	DES	723	0.0045
	3DES	723	0.0048
	RSA	723	0,0196
2	AES	577	0.0024
	DES	577	0.0020
	3DES	577	0.0017
	RSA	577	0.0067
3	AES	428	0.0015
	DES	428	0.0016
	3DES	428	0.0019
	RSA	428	0.0048
4	AES	306	0.0010
	DES	306	0.0013

	3DES	306	0.0016
	RSA	306	0.0031

Table 4: Buffer Size Usage of the System

No of Experiment	Algorithms	Data length	Decryption time(s)
1	AES	723	1008
	DES	723	728
	3DES	723	731
	RSA	723	4059
2	AES	577	812
	DES	577	584
	3DES	577	587
	RSA	577	3257
3	AES	428	590
	DES	428	432
	3DES	428	435
	RSA	428	2472
4	AES	306	438
	DES	306	312
	3DES	306	315
	RSA	306	1755

Table 5: Summary of Result for the Average Computation Time for AES, DES, 3DES and RSA

No of Experiments	Algorithms	Data Length	Encryption Time(s)	Decryption Time(s)	Buffer Size Usage	Average Computation Time
1	AES	723	0.0028	0.0057	1008	0.0043
	DES	723	0.0066	0.0045	728	0.0056
	3DES	723	0.0069	0.0048	731	0.0059
	RSA	723	0.0353	0.0196	4059	0.0275
2	AES	577	0.0018	0.0024	812	0.0021
	DES	577	0.0020	0.0020	584	0.0020
	3DES	577	0.0023	0.0017	587	0.0023
	RSA	577	0.0130	0.0067	3257	0.0099
3	AES	428	0.0015	0.0015	590	0.0015
	DES	428	0.0014	0.0016	432	0.0015
	3DES	428	0.0015	0.0019	435	0.0016
	RSA	428	0.0060	0.0048	2472	0.0054
4	AES	306	0.0012	0.0010	438	0.0011
	DES	306	0.0013	0.0013	312	0.0013
	3DES	306	0.0014	0.0016	315	0.0016
	RSA	306	0.0045	0.0031	1755	0.0038

Review sources show that cryptographic algorithms have been effectively used towards secure communication over public network as data can be protected by the method of encryption. it has secured mobile banking, governance, business, military, power, health and so on. AES, DES, 3DES, RC2, Blowfish, and RC6 algorithms have been compared based on different sizes of data blocks, varied data types, battery power usage, varied key size and finally encryption/decryption speed. A comparative analysis of AES, DES, 3DES and RSA in relation to stimulation time and memory usage. Results from the analysis shows that AES algorithm consumes least encryption and decryption time and memory usage compared to DES algorithm. However, this survey compares AES, DES, 3DES and RSA considering parameters such as computation time and buffer size usages to determine the amount of computer resource that is utilized and how long it takes each algorithm to complete its task. In addition, this survey proves the current security strength on our educational system towards securing transmission of student's results in universities by applying cryptographic technology in securing students result transmission.

CONCLUSION

Encryption algorithm plays an important role in communication security where encryption/decryption time, memory usages and battery power are the major issue of concern. This paper surveyed the performance of existing encryption techniques of RSA, DES, 3DES and AES algorithms towards securing transmission of students' results. Based on the text files used and the experimental results, the model indicates that AES algorithm consumes least encryption time; DES algorithm has the least memory usage while encryption time difference is very minor in the case of AES algorithm and DES algorithm. RSA consumes the longest encryption time and memory usage is also very high. From the evaluated results, AES algorithm is much better than DES, 3DES and RSA algorithm since DES is highly vulnerable to linear cryptanalysis attacks due to Weak keys which remain an issue of serious concern resulting in exposure to brute force attacks. AES was more efficient and secured than DES, 3DES and RSA for the transmission of students' results, thus, proposed as a model for results transmission. The android application has been designed and implemented using Advanced Encryption Standard algorithm for both encryption and decryption of messages and provides a highly secured communication over public network. The data encryption application runs using a mobile phone which does not require any additional encryption device, thus, making it user friendly and commonly available for users. The experimental test also showed that the AES algorithm is suitable and easy to implement in mobile devices. Thus, it is found to be secure, reliable and efficient. Solutions such as encrypted data should be considered if there is a need to send sensitive information.

In this review, we compared four existing cryptographic algorithms for efficiency, which includes AES, DES, 3DES and RSA and also an application for secure data transmission. Therefore, AES algorithm is recommended as the best for implementation.

REFERENCES

Alanazi, O., Zaidan, B., Zaidan, A., Hamid, A., Shabbir, M. and Al-Nabhani, Y. (2010).New Comparative

Study between Data Encryption Standard, Triple Data Encryption Standad and Advanced Encryption Standard. *Journal of Computing***,** 2(3): 152-157.

Diaa, S., Elminaam, H. and Mohie, M. (2010). Evaluating the Effects of Symmetric Cryptography Algorithm on Power Consumption for Different Data Types. *International Journal of Network Security*, 11(2): 78-87.

Diaa, S., Elminaam, H. and Mohie, M. (2010). Evaluating the Effects of Symmetric Cryptography Algorithm on Power Consumption for Different Data Types. *International Journal of Network Security*, 11(2): 78-87.

Ijaz, A., Kamalrulnizam, B. and Mohsin, I. (2011). A Survey about the Latest Trends and Research Issues of Cryptographic Elements. *International Journal of Computer Science*, 8(2): 140- 149.

Kakkar, A. and Singh, M. (2012). Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Networks. *International Journal of Engineering and Technology (IJET)*, 2 (1): 87-93.

Kakkar, A. and Singh, M. (2012). Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Networks. *International Journal of Engineering and Technology (IJET)*, 2 (1): 87-93.

Oh, J., Yang, D. and Chon, K. (2010). A Selective Encryption Algorithm Based on Advanced Encryption Standard for Medical Information. *Healthcare Informatics Research*, 16(1): 22-29.

Rajdeep, B. and Rahul, H. (2015). A Review and Comparative Analysis of Various Encryption Algorithms. *International Journal of Security and Its Applications*, 9(4): 289-306.

Ritu T. and Sanjay, A. I. (2014). Comparative Study of Symmetric and Asymmetric Cryptography Techniques. *International Journal of Advance Foundation and Research in Computer (IJAFRC)*, 1(6): 2348 – 4853.

Seth, S. and Rajan, M. (2011). Comparative Analysis of Encryption Algorithms for Data Communication. *International Journal of Computer Science and Technology*, 2(2): 292- 294.

Shashi, M. and Rajan, M. (2011). Comparative Analysis of Encryption Algorithms for Data Communication. *International Journal of Computer Science and Technology*, 2(2): 292-294.

Srinivas, B., Anish, S. and Austin, S. (2014). A Comparative Performance Analysis of Data Encryption Standard and Blowfish Symmetric Algorithm. *International Journal of Innovative Research in Computer and Communication Engineering*, 2(5): 77-88.

Neetesh, S. and Ashish, P. (2016). Enhancing Security System of Short Message Service for M-Commerce in GSM. *International Journal of Computer and Engineering Technology,* 2(4): 126- 133.

Rajdeep, B. and Rahul, H. (2015). A Review and Comparative Analysis of Various Encryption Algorithms. *International Journal of Security and Its Applications*, 9(4): 289-306.

Gurjeevan, S., Ashwani, S. and Sandha, K. (2011). Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System. *International Journal of Multidisciplinary Research*, 1(4): 143-151.

Gurpreet, S. (2013). A Study of Encryption Algorithm for Information Security. *International Journal of Computer Application*, 67(19): 33- 38.

Paritosh, S. (2014). New Encryption Technique for Secure Short Message Service Transmission. *International Journal of Advanced Computer Technology*, 3(11): 1265- 1269.

Idrizi, Florim, Dalipi, Fisnik & Rustemi, Ejup. (2013), "Analyzing the speed of combined cryptographic algorithms with secret and public key". International Journal of Engineering Research and Development, e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 8, Issue 2 pp. 45.

Elminaam, Diaa Salama Abd, Abdual Kader, Hatem Mohamed & Hadhoud, Mohiy Mohamed.(2010) "Evaluating The Performance of Symmetric Encryption Algorithms". International Journal of Network Security, Vol.10, No.3, pp. 216.

Faiqa M, Muhammad A, Muhammad M A, Munam A, (2017)" Cryptography: A Comparative Analysis for Modern Techniques", International journal of Advanced Computer Science and Applications, volume 8, issue 6,

Zaran H, Durga V & Croatia, (2016) " Comparative Analysis of Cryptographic Algorithms", International Journal of Digital Technology and Economy, volume 1, issue 2,

Prerna M, Abhishek S, (2013)" A study of Encryption Algorithms AES,DES ans RSA for Security" Global Journal of Computer Science and Technology Network and Web Security, Volume 13 issue 15.

Hamdan.O.A, Zaidan B.B., Zaidan A.A., Hamid A.Jalab, Shabbir M. and Al-Nabhani Y., (2010) "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal Of Computing, Volume 2,ISSUE 3, pp. 152-157.

Pavithra S. and Ramadevi E., (2012) "Performance Evaluation of Symmetric Algorithms", Journal of Global Research in Computer Science, Volume 3, No. 8, pp. 43-45.

Kumar A. M, Chandra P and Archana T, (2012) "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5.

Gurpreet, Singh, & Kinger, Supriya. (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. International Journal of Computer Applications. 67. 33-38. 10.5120/11507-7224.

Arora P, Arun S and Himanshu T, (2012) "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal (WCSIT), Vol. 2, No. 5, pp. 179-183.

Rajadeep B, Rahul H, (2015) "A review and Comparative Analysis of various Encryption Algorithms", International Journal of Security and its Applications, volume 9, issue 4.