International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 21
October 2018

A New and Novel Study of Comparison on Cryptographic Algorithms using AES, DES and RSA for Network Security

V. Subhashini[1], Dr. N. Geethanjali[2]
[1]Research Scholar, Department of Computer Science & Technology, Sri Krishnadevaraya University, Ananthapuramu, Andhra Pradesh, India.
[2] Professor, Department of Computer Science & Technology, Sri Krishnadevaraya University, Ananthapuramu, Andhra Pradesh, India.

Abstract:

Security measures must be incorporated into computer systems whenever they are potential targets for malicious or mischievous attacks. This is especially for systems which handle financial transactions or confidential, classified or other information whose secrecy and integrity are critical. With the need to protect the integrity and privacy of information belonging to individuals and organizations. In recent years network security has become an important issue. Encryption has come up as a solution, and plays an important role in information security system. Many techniques are needed to protect the shared data. The present work focus on cryptography to secure the data while transmitting in the network. Firstly the data which is to be transmitted from sender to receiver in the network must be encrypted using the encryption algorithm in cryptography. Secondly, by using decryption technique the receiver can view the original data. In this paper we implemented three encrypted techniques like AES, DES and RSA algorithms and compared their performance of encrypt techniques based on the analysis of evaluation parameters like encryption time, decryption time, memory used throughput of cpu utilization and entropy effect. Experiments results are given to analyses the effectiveness of each algorithm.

Keywords: Encryption,Decryption,Advanced Encryption algorithm(AES),Data Encryption Standard (DES),RSA Algorithm

1.INTRODUCTION

Security plays an important role to store information and transmit it across the undefined networks with secure manner. Hence, the secure communication is the basic requirement of every transaction over networks. Cryptography is an essential component for secure communication and transmission of information through security services like confidentiality, data integrity, access control, authentication and non-repudiation. It provides a way to protect sensitive information by transferring it into unintelligible and only the authorized receiver can be able to access this information by converting into the original text. The process to convert the plaintext into ciphertext with the key is called encryption process and to reverse the process of encryption is called decryption process. The design of cryptographic algorithms is secure and efficient, low cost, require small memory footprint, easy to implement and utilized on multiple platforms. The vast range of applications is developed to secure cryptographic algorithms using different mathematical process. It is quite difficult to develop fully secure encryption algorithm due to the challenges from cryptanalysts who continuously trying to access any available cryptographic systems [1]-[5]. The right selection of algorithms is important to achieve

high-security requirements which protect the cryptographic components to cryptanalysis [6]. Cryptographic systems can be divided into deterministic and probabilistic encryption scheme [7]. Deterministic encryption scheme allows the plaintext is encrypted by using keys that always provide the same ciphertext, but the encryption process is repeated many times. In this scheme, every plaintext has one to one relationship with the keys and ciphertext otherwise it will produce more than one output of particular plaintext during the decryption process. Probabilistic Encryption Scheme shows the plaintext has different ciphertext with the different keys. The probabilistic encryption scheme is significantly secure than the deterministic encryption scheme because it makes difficult for a cryptanalyst to access any sensitive information regarding plaintext that is taken from ciphertext and corresponding key. Furthermore, the cryptographic algorithms can be further divided into two main categories like keyless cryptosystem and key-based cryptosystem as shown in Fig. 1. In the keyless cryptosystem, the relationship between the plaintext and ciphertext having a different version of the message is exclusively depend on the encryption algorithm [8]. The keyless cryptosystem is generally less secure than key-based systems because anyone can gain access to the algorithm will be able to decrypt every message that was encoded using keyless cryptosystem such as Caesar cipher [9]. The keybased cryptosystem can be further categories into symmetric key (secret key) encryption and asymmetric key (public key) encryption based on the type of security keys utilized for the encryption or decryption process [10]-[13]. The detail of the cryptosystems is explained as follows: A. Symmetric Key Encryption The symmetric key (secret key) encryption is employed similar key for the encryption and decryption of a message. Encryption and decryption keys are keeping secret and only known by authorized sender and recipient who want to communicate. The allocation of different keys to the different parties increases the overall message security. The strength of the symmetric key encryption is depending on the secrecy of encryption and decryption keys. The symmetric encryption algorithms can be classified into block and stream cipher on This paper was partly sponsored by the Centre for Graduate Studies UTHM (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 11, 2017 334 | P a g e www.ijacsa.thesai.org the basis of the grouping of message bits [14], [15]. In a block cipher, a group of messages characters of a fixed size (a block) is encrypted all at once and sent to the receiver. Moreover, the block cipher can be further divided into binary and non-binary block cipher based on the final results of the message, keys and ciphertext. The message bit size for the binary block cipher is 64, 128, 192, and 256 and the non-binary block cipher has not defined the standard that depends on the cipher implementation.

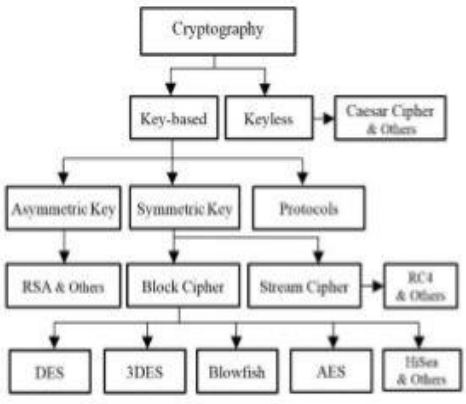


Fig. 1. Overview of the cryptographic encryption algorithms.

International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 21
October 2018

2. Background

Cryptographic Encryption Algorithms

A.Symmetric Key

Symmetric key block cipher comprises the five main components: plaintext, encryption and decryption algorithm, ciphertext and key schedule algorithm as shown in Fig. 2.There are several symmetric key encryption algorithms such as DES [16], [17], 3DES [9], AES [18], [19], BLOWFISH [20], HiSea [21], RC4 [22], etc. The encryption process in symmetric block cipher converts the plaintext into ciphertext with the secret key that is generated from the key schedule algorithm. Similarly, the ciphertext is transferred to the appropriate recipient is decrypted using decryption process with the same key. The block size for the stream cipher is one character and it is not more appropriate for software processing due to the key length as long the message [23], [24]. The working of the stream cipher is presented in following steps: 1) A single character of plaintext is combined with a single character from key stream to produce the single character of ciphertext. 2) The ciphertext character from Step 1 sent to the receiver. 3) Step 1 and Step 2 is repeated until the entire message has been sent.

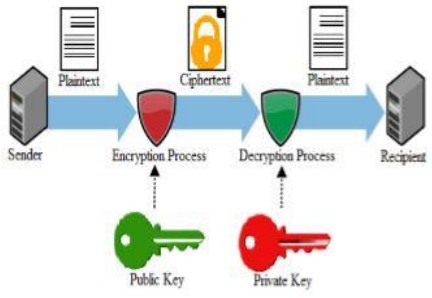


Fig. 2. Components of symmetric block cipher.

B. Asymmetric Key Encryption

The asymmetric key encryption is commonly referred to as public key encryption in which different keys are employed for the encryption and decryption of the message. The encryption key is also said as the public key and can be utilized to encrypt the message with the key. The decryption key is said to as secret or private key and can be used to decrypt the message. The strength of the asymmetric key encryption is utilized with digital signature then it can provide to the users through message authentication detection. The asymmetric encryption algorithm includes RSA [25], DiffieHellman algorithm [26], etc. The component of an asymmetric block cipher is shown in Fig. 3.

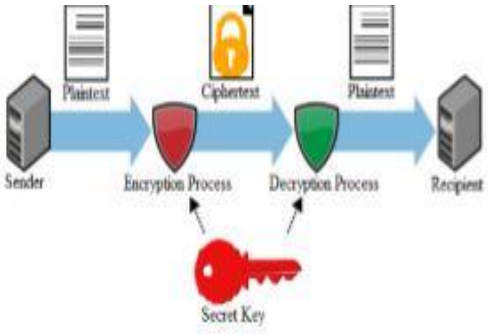


Fig. 3. Components of asymmetric block cipher.

C. Key Schedule Algorithm

Key schedule algorithm is employed to generate secret keys and plays an important role in the development of encryption and decryption key. The insignificant key generation algorithm generates weak keys that are used for encryption process can easily attack using brute force attack because cryptanalyst continuously trying all possible combinations to get original text using this attack [27]-[29]. All cryptographic algorithms follow the consideration of Advanced Encryption Standard (AES) that must support the key lengths include 128 bits, 192 bits and 256 bits [19]. The number of the round for that key length is 10, 12, 14 respectively and the round keys are taken from the cipher key using

key schedule algorithm and utilized in the construction of block cipher. For the development of fully secure block cipher, the multiple numbers of rounds ensure the high diffusion and employed invertible transformation.

3.Existing System

At present, the Elgamal encryption algorithm works by sending data to the receiver who has just one private key to decrypt the data .

The entire process is as follows : [30]

Key generation : The receiver who wishes to get message, chooses a large prime number p, a random number g which is also prime and less than the prime number initially chosen and a random integer x from 0 to (p-1). He then calculates y=gx mod p The public key of the sender is (p , g , y) and his private key is x. Encryption by the sender : The sender generates an integer k lying between 0 to (p-1). He then calculates r = g k mod p xiv and t = (yk . M) mod p and transmits (r , t) as the encrypted message .

Decryption of the ciphertext : The receiver with his private key calculates t. r-x which gives the plaintext .But in this algorithm , as there is just one private key , it can be gessed by any intruder and is thus not reliable.

In Elgamal encryption algorithm by dividing the private key and assigning them to 2n+1 authorized receivers individually. The persons will be able to decrypt the message received from the sender only if they are together, separately this operation being impossible for them. It has the following operations :

Key generation : A large prime number p and a random number g which is prime and less than the initially chosen prime number is chosen.

Then after from {0,…,p-1} there are chosen the elements x1,x2,…,x2n+1, preferably distinct , then there are being calculated y1=g x1 mod p,y2=g x2 mod p,…, y2n+1=g x2n+1 mod p .

The public key is {p,g,y1,y2,…….,y2n+1} and the private key consists of {x1,x2,…,x2n+1}.

Encryption of a message : The sender encrypts message m knowing the public key as follows: He chooses a random element k from {0 ,…, p-1} and calculates c1=g k mod p,c21=m.x1 k mod p, c22=m.x2 k mod p,… , c22n+1=m.x2n+1 k mod p, c2= c21. c23. c25. c27…./c22. c24. c26…. then sends the encrypted message (c1, c2) to the recipient.

Decryption of the message : In order to decrypt the message (c1, c2),the receiver use p and the private keys {x1}, {x2},…..,{x2n+1} respectively, computing together c2. c1 x2 . c1 x4 . c1 x6 …/ c1 x1 . c1 x3. c1 x5. c1 x7…= (c21. c23. c25. c27…/ c22. c24. c26…)(c1 x2 . c1 x4 . c1 x6…/ c1 x1. c1 x3.c1 x5. c1 x7…) = (m .y1 k . m . y3 k . m . y5 k . m . y7 k…/ m .y2 k . m . y4 k . m . y6 k…)(c1 x2. c1 x4 . c1 x6…/ c1 x1 . c1 x3 . c1 x5 . c1 x7…) = m.

4. Proposed System:

In this paper, we are modifying the existing Elgamal encryption algorithm by dividing the key 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. This study evaluates

three different encryption algorithms namely; AES, DES and RSA. The performance measure of encryption schemes will be conducted in terms of encryption and decryption time such as text or document

4.1 Data Encryption Standard (DES)

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.

DES is one of the most widely accepted, publicly available cryptographic systems. The Data Encryption Standard (DES) is a block Cipher which is designed to encrypt anddecrypt blocks of data consisting of 64 bits by using a 64-bit key.

Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. The algorithm goes through 16 iterations that interlace blocks of plaintext with values obtained from the key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key are used for decryption. There are many attacks and methods recorded till now those exploit the weaknesses of DES, which made it an insecure block cipher. Despite the growing concerns about its vulnerability, DES is still widely used by financial services and other industries worldwide to protect sensitive on-line applications. The flow of DES Encryption algorithm is shown in Fig4.

The algorithm processes with an initial permutation, sixteen rounds block cipher and a final permutation (i.e. reverse initial permutation)

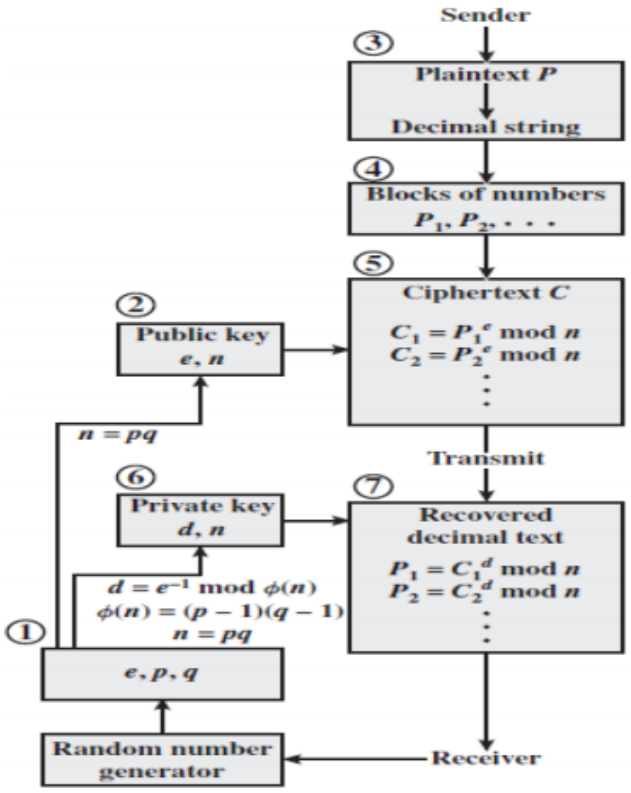


Fig4. Flow Of DES Algorithm

4.2 Rivest-Shamir-Adleman (RSA)

RSA is widely used Public-Key algorithm. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. RSA algorithm involves these steps:

Public key cryptosystems for key exchange or digital signatures or encryption of blocks of data. RSA uses a variable size encryption block and a variable size key. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. It uses two prime numbers to generate the public and private keys. These two different keys are used for encryption

and decryption purpose. Sender encrypts the message using Receiver public key and when the message gets transmit to receiver, then receiver can decrypt it using his own private key.

RSA operations can be decomposed in three broad steps key generation, encryption and decryption. RSA have many flaws in its design therefore not preferred for the commercial use. When the small values of p & q are selected for the designing of key then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. On the other hand if large p & q lengths are selected then it consumes more time and the performance gets degraded in comparison with DES. Further, the algorithm also requires of similar lengths for p & q, practically this is very tough conditions to satisfy. Padding techniques are required in such cases increases the system's overheads by taking more processing time.

1. **Key Generation Procedure**

1. Choose two distinct large random prime numbers p & q such that $p \neq q$.

2. Compute $n = p \times q$.

3. Calculate: phi (n) = (p-1) (q-1).

4. Choose an integer e such that $1<e< n$

5. Compute d to satisfy the congruence relation $d \times e = 1 \bmod \text{phi}(n)$; d is kept as private key exponent.

6. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

. **Encryption Plaintext:**

$P < n$ Cipher text: $C = P^e \bmod n$.

Decryption Cipher text:

C Plaintext: $P = C^d \bmod n$

4.3 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size.

AES is the new encryption standard recommended by NIST to replace DES[31]. 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 . 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.

The Final round, there is no Mix-column transformation Fig5. shows the overall process. Decryption is the reverse process of encryption and using inverse functions: Inverse Substitute Bytes, Inverse Shift Rows and Inverse Mix Columns.

Each round of AES is governed by the following transformations.

1. Substitute Byte transformation

AES contains 128 bit data block, which means each of the data blocks has 16 bytes. In sub-byte transformation, each byte (8-bit) of a data block is transformed into another block using an 8-bit .

2. Shift Rows transformation

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.

3. Mix columns transformation

This round is equivalent to a matrix multiplication of each Column of the states. A fix matrix is multiplied to each column vector. In this operation the bytes are taken as polynomials rather than numbers.

4. Add round key transformation

It is a bitwise XOR between the 128 bits of present state and 128 bits of the round key. This transformation is its own inverse.

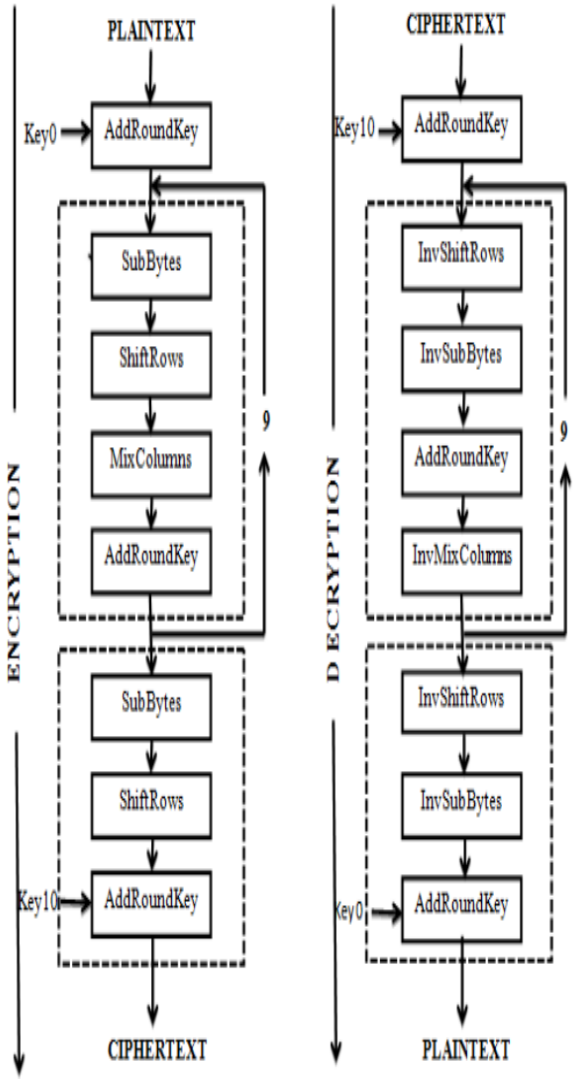


Fig5.Overall Process of AES algorithm

5. Implementation Process

The Proposed work is implemented and categorized on four modules.

5.1 Symmetric-key Encryption and Decryption Module:

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key.Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as

opposed to individual characters, the input form used by a stream cipher.

The data Encryption Standard(DES) and the Advanced Encryption Standard(AES) are block cipher designs which have been designated cryptography Stream ciphers will create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character –by-character

5.2 Asymmetric key Encryption and Decryption Module:

Public-key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. Although different, the two parts of the key pair are mathematically linked. One key locks or encrypts the plaintext, and the other unlocks or decrypts the cipher text. Neither key can perform both functions by itself. The public key may be published without compromising security, while the private key must not be revealed to anyone not authorized to read the messages. Public-key cryptography uses asymmetric key algorithms (such as RSA), and can also be referred to by the more generic term "asymmetric key cryptography."

The algorithms used for public key cryptography are based on mathematical relationships that presumably have no efficient solution. Although it is computationally easy for the intended recipient to generate the public and private keys, to decrypt the message using the private key, and easy for the sender to encrypt the message using the public key, it is extremely difficult (or effectively impossible) for anyone to derive the private key, based only on their knowledge of the public key. This is why, unlike symmetric key algorithms, a public key algorithm does not require a secure initial exchange of one (or more) secret keys between the sender and receiver.

.

5.3 KEY PAIRS

In an asymmetric system the encryption and decryption keys are different but related. The encryption key is known as the public key and the decryption key is known as the private key. The public and private keys are known as a key pair. Where a certification authority is used, remember that it is the public key that is certified and not the private key. This may seem obvious, but it is not unknown for a user to insist on having his private key certified!

5.4 KEY COMPONENTS

Keys should whenever possible be distributed by electronic means, enciphered under previously established higher-level keys. There comes a point, of course when no higher-level key exists and it is necessary to establish the key manually. A common way of doing this is to split the key into several parts (components) and entrust the parts to a number of key management personnel. The idea is that none of the key parts should contain enough information to reveal anything about the key itself. Usually, the key is combined by means of the exclusive-OR operation within a secure environment. In the case of DES keys, there should be an odd number of components, each component having odd parity. Odd parity is preserved when all the components are combined.

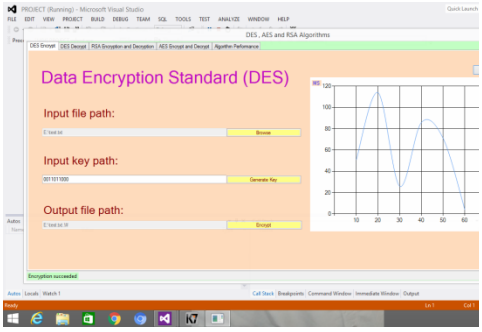
Further, each component should be accompanied by a key check value to guard against keying errors when the component is entered into the system. A key check value for the combined components should also be available as a final check when the last

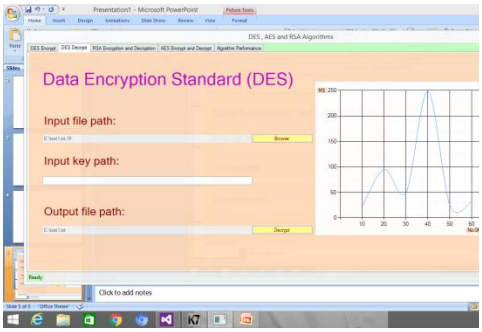
International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 21
October 2018

component is entered. A problem that occurs with depressing regularity in the real world is when it is necessary to re-enter a key from its components. This is always an emergency situation, and it is usually found that one or more of the key component holders cannot be found. For this reason it is prudent to arrange matters so that the components are distributed among the key holders in such a way that not all of them need to be present.

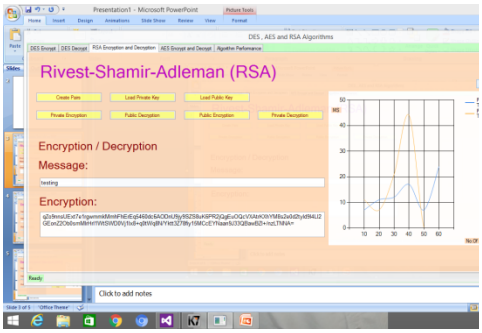
6. Experimental Results

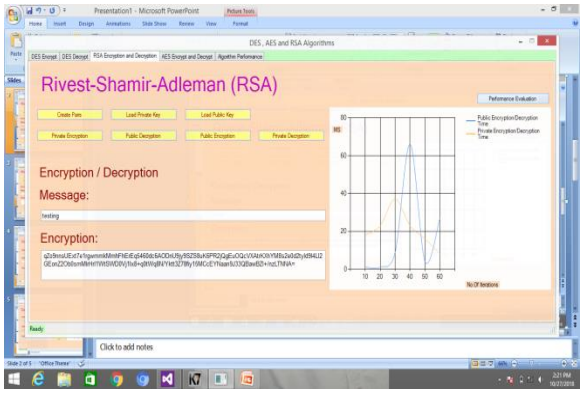
6.1 Performance Analysis of DES Algorithms



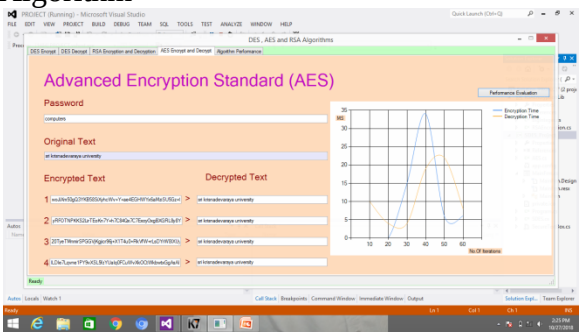


6.2 Performance Analysis of RSA Algorithm



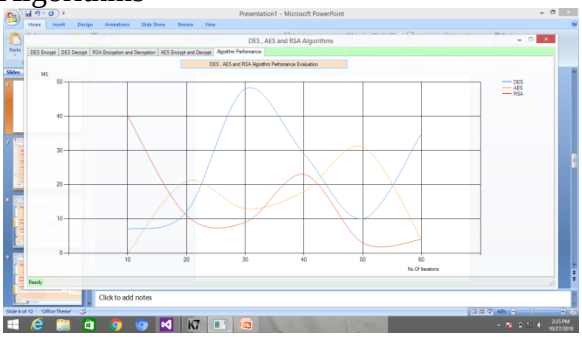


6.3 Performance Analysis of AES Algorithm



After Comparing DES,RSA and AES algorithm ,we conclude that AES Algorithm is more efficient comparing to DES and RSA Algorithm.

6.4 Comparision of DES,RSA and AES Algorithms



7. Conclusion and Future Work

I have studied of the popular Encryption Algorithms such as RSA, DES 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. 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 .According to research done and literature survey it can be found that AES algorithm is most efficient in terms of speed, time, and throughput and 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.

8. References

[1] K. Mandal, C. Parakash, and A. Tiwari, "Performance evaluation of cryptographic algorithms: DES and AES," in Proceeding of the IEEE Students' Conference on Electrical, Electronics and Computer Science: Innovation for Humanity (SCEECS), 2012.

[2] M. Ebrahim, S. Khan, and U. bin Khalid, "Symmetric algorithm survey: A comparative analysis," International Journal of Computer Applications, vol. 61, no. 20, pp. 12–19, 2013.

[3] N. Kumar and P. Chaudhary, "Performance evaluation of encryption/decryption mechanisms to enhance data security," Indian Journal of Science and Technology, vol. 9, no. 20, 2016.

[4] Disina, A. H., Pindar, Z. A., & Jamel, S., "Enhanced caeser cipher to exclude repetition and withstand frequency cryptanalysis," Journal of Network and Information Security, 2015.

[5] V. V Palagushin and A. D. Khomonenko, "Evaluation of cryptographic primitives security based on proximity to the latin square," in Proceeding of the IEEE 18th conference of fruct association, pp. 266– 271, 2016.

[6] S. H. Jamel and M. M. Deris, "Diffusive primitives in the design of modern cryptographic algorithms," in proceedings of the International Conference on Computer and Communication Engineering (ICCCE08): Global Links for Human Development, pp. 707–710, 2008.

[7] S. Goldwasser and M. Bellare, Lecture Notes on Cryptography, Cambridge, Massachusetts, 2008.

[8] A. Kaushik, M. Barnela, and A. Kumar, "Keyless user defined optimal security encryption," International Journal of Computer and Electrical Engineering, vol. 4, no. 2, pp. 2–6, 2012.

[9] W. Stallings, Cryptography and network security: principles and practices. Prentice Hall, 2005.

[10] M. Stamp, Information Security: Principles and Practice. John Wiley & Sons, 2011.

[11] F. Maqsood, M. M. Ali, M. Ahmed, and M. A. Shah, "Cryptography: A comparative analysis for modern techniques," International Journal of Advanced Computer Science and Applications, vol. 8, no. 6, pp. 442– 448, 2017.

[12] S. Ahmad, K. M. R. Alam, H. Rahman, and S. Tamura, "A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets," in Proceedings of the IEEE International Conference on Networking Systems and Security, 2015.

[13] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," Journal of Cryptology, vol. 26, no. 1, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 11, 2017 344 | P a g e www.ijacsa.thesai.org pp. 80–101, 2013.

[14] A. M. Alshahrani and S. Walker, "Implement a novel symmetric block cipher

algorithm," International Journal on Cryptography and Information Security, vol. 4, no. 4, pp. 1–11, 2014.
[15] M. Dworkin, "Recommendation for block cipher modes of operation," NIST Spec. Publ. 800-38B, 2005. [16] T. Nie and T. Zhang, "A study of DES and Blowfish encryption algorithm," in Proceedings of 10th IEEE Region Annual International Conference TENCON, pp. 1–4, 2009.
[17] M. E. Smid and D. K. Branstad, "Data Encryption Standard: past and future," Proceedings of the IEEE, vol. 76, no. 5, pp. 550–559, 1988.
[18] J. Daemen, V. Rijmen, and K. U. Leuven, AES Proposal: Rijndael. (NIST), National Institute of Standards, 1999. [19] N. I. of Standards-(NIST), Advanced Encryption Standard (AES). Federal Information Processing Standards Publication197, 2001.
[20] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (Blowfish)," in Proceedings of the Fast Software Encryption: Cambridge Security Workshop Cambridge, U. K., pp. 191–204, 1994.
[21] S. Jamel, M. M. Deris, I. T. R. Yanto, and T. Herawan, "The hybrid cubes encryption algorithm (HiSea)," Communications in Computer and Information Science, Springer-Verlag Berlin Heidelberg, vol. 154, pp. 191–200, 2011.
[22] W. Stallings, "The RC4 stream encryption algorithm," in Cryptography and network security, 2005.
[23] S. B. Sasi, N. Sivanandam, and Emeritus, "A survey on cryptography using optimization algorithms in WSNs," Indian Journal of Science and Technology, vol. 8, no. 3, pp. 216–221, 2015.
[24] S. Jamel, "The hybrid cubes encryption algorithm (HiSea)," Ph.D Thesis, Univ. Tun Hussein Onn Malaysia (UTHM), Johor, Malaysia, pp. 1–138, 2012.
[25] S. Burnett and S. Paine, RSA Security‟s Official Guide to Cryptography. McGraw-Hill, 2001.
[26] A. Escala, G. Herold, and C. Ràfols, "An algebraic framework for Diffie - Hellman assumptions," Journal of Cryptology, 2015.
[27] M. F. Mushtaq, S. Jamel, K. M. Mohamad, S. A. A. Khalid, and M. M. Deris, "Key generation technique based on triangular coordinate extraction for hybrid cubes," Journal of Telecommunication, Electronic and Computer Engineering (JTEC), vol. 9, no. 3-4, pp. 195-200, 2017.
[28] A. H. Disina, S. Jamel, M. Aamir, Z. A. Pindar, M. M. Deris, and K. M. Mohamad, "A key scheduling algorithm based on dynamic quasigroup string transformation and All-Or-Nothing key derivation function," Journal of Telecommunication, Electronic and Computer Engineering, vol. 9, no. 3–5, pp. 1–6, 2017.
[29] A. H. Disina, S. Jamel, Z. A. Pindar, and M. M. Deris, "All-or-nothing key derivation function based on quasigroup string," in proceeding of IEEE International Conference on Information Science and Security (ICISS), pp. 6–10, 2016.
[30]. A COMPARITIVE STUDY OF ELGAMAL BASED CRYPTOGRAPHIC ALGORITHMS Ramzi A. Haraty, Hadi Otrok Lebanese American University P.O.Box 13-5053 Chouran, Beirut, Lebanon 1102 2801 Email: rharaty@lau.edu.lb, hadiotrok@hotmail.com A. N. El-Kassar Mathmatics Department, Beirut Arab University, Beirut, Lebanon Email: ak1@bau.edu.lb
[31] Global Journal of Computer Science and Technology: E Network, Web & Security Volume 15 Issue 4 Version 1.0 Year 2015 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350 Implementation of AES with Time Complexity Measurement for Various Input By Shraddha More & Rajesh Bansode