A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security

Gurpreet Singh
M.Tech Research Scholar, Department of Computer Science and Engineering
Sri Guru Granth Sahib World University,
Fatehgarh Sahib, Punjab, India.

Supriya
Assistant Professor, Department of Computer Science and Engineering
Sri Guru Granth Sahib World University,
Fatehgarh Sahib, Punjab, India.

ABSTRACT

Encryption is the process of scrambling a message so that only the intended recipient can read it. Encryption can provide a means of securing information. As more and more information is stored on computers or communicated via computers, the need to insure that this information is invulnerable to snooping and/or tampering becomes more relevant. With the fast progression of digital data exchange in electronic way, Information Security is becoming much more important in data storage and transmission. Information Confidentiality has a prominent significance in the study of ethics, law and most recently in Information Systems. With the evolution of human intelligence, the art of cryptography has become more complex in order to make information more secure. Arrays of Encryption systems are being deployed in the world of Information Systems by various organizations. In this paper, a survey of various Encryption Algorithms is presented.

General Terms

Information Security, Encryption

Keywords

Encryption, RSA, DES, 3DES, AES

1. INTRODUCTION

In recent years, a lot of applications based on internet are emerged such as on-line shopping, stock trading, internet banking and electronic bill payment etc. Such transactions, over wire or wireless public networks demand end-to-end secure connections, should be confidential, to ensure data authentication, accountability and confidentiality, integrity and availability, also known as *CIA triad* [1].

The NIST *Computer Security Handbook* [NIST95] defines the term computer security as, "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)." Security is the mechanism by which information and services are protected from unintended or unauthorized access, change or destruction. Security in networking is based on *Cryptography* (a word with Greek origins, means "secret writing"), the science and art of transforming messages to make them secure and immune to attack [2].

Encryption is one of the principal means to guarantee security of sensitive information. Encryption algorithm performs various substitutions and transformations on the plaintext (original message before encryption) and transforms it into ciphertext (scrambled message after encryption). Many encryption algorithms are widely available and used in information security. Encryption algorithms are classified into two groups: *Symmetric-key* (also called secret-key) and *Asymmetric-key* (also called public-key) encryption.

Symmetric key encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption.

Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys – one a public key and one a private key. It is also known as public-key encryption [3].

A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. The strength of the encryption algorithm relies on the secrecy of the key, length of the key, the initialization vector, and how they all work together [4].

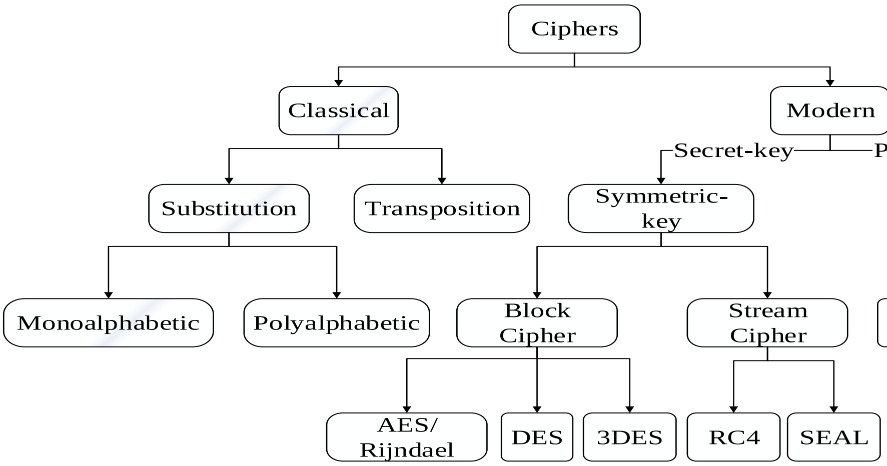
Asymmetric encryption techniques are about 1000 times slower than Symmetric encryption which makes it impractical when trying to encrypt large amounts of data. Also to get the same security strength as symmetric, asymmetric must use a stronger key than symmetric encryption technique [5]. The classification of major encryption techniques is shown in Figure 1.

Note: RSA = Asymmetric therefore, image idea for project most likely will not work.

2. RELATED WORKS

To give more prospective about the performance of the encryption algorithms, this subsection describes and examines previous work done in field of data encryption. The metrics taken into consideration are processing speed, throughput, power consumption, avalanche effect, packet size and data types. This subsection also discusses the results obtained for some of the algorithms.

Arora et al. [6] 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).



Note: Diffie Hellman and RSA for project use asymmetric keys but AES uses symmetric key

Fig 1: Classification of Encryption Methods

$$\text{Speed-Up Ratio} = \frac{\text{Mean processing time on single processor}}{\text{Mean processing time on cloud}}$$

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.

Seth et al. [7] have done the 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 consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm.

Abdul. Elminaam et al. [5] studied about the performance of Symmetric Encryption Algorithms. This paper provides evaluation of six of the most common encryption algorithms: AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. 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 following results. There is no significant difference when the results are displayed either in hexadecimal base encoding or in base 64 encoding. In case of changing packet size, it was found that RC6 requires less time than all algorithms except Blowfish. In case of changing data type such as image instead of text, it was found that RC2, RC6 and Blowfish has disadvantage over other algorithms in terms of time consumption. Also, 3DES still has low performance compared to algorithm DES. Finally -in the case of changing key size (possible only in AES and RC6 algorithms) it can be seen that higher key size leads to clear change in the battery and time consumption.

Pavithra et al. [8] compares the performance evaluation of various cryptographic algorithms. On the basis of parameter taken as time various cryptographic algorithms are evaluated on different video files. Different video files are having different processing speed on which various size of file are processed. Calculation of time for encryption and decryption in different video file format such as .vob and .DAT, having file size from 1MB to 1100MB. Results shows that AES algorithm is executed in lesser processing time and more throughput level as compared to DES and BLOW FISH.

Alanazi et al. [9] 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.

Mandal et al. [10] in this paper compared two most widely used symmetric encryption techniques i.e. data encryption standard (DES) and advanced encryption standard (AES) on the basis of avalanche effect due to one bit variation in plaintext keeping the key constant, avalanche effect due to one bit variation in key keeping the plaintext constant, memory required for implementation and simulation time required for encryption. Avalanche effect is the property of any encryption algorithm in which a small change in either the key or the plaintext should produce a significant change in the cipher text.

$$\text{Avalanche Effect} = \frac{\text{Number of flipped bits in ciphered text}}{\text{Number of bits in ciphered text}}$$

Avalanche effect is very high for AES as compared to DES whereas memory requirement and simulation time for DES is greater than that of AES, which shows AES is better than DES. AES is ideal for encrypting messages sent between objects via chat-channels, and is useful for objects that involve monetary transactions.

Kakkar et al [11] 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.

3. DETAILED DESCRIPTION OF COMMON ENCRYPTION ALGORITHMS

The generation, modification and transportation of keys have been done by the encryption algorithm. It is also named as cryptographic algorithm. There are many cryptographic algorithms available in the market to encrypt the data. The strength of encryption algorithm heavily relies on the computer system used for the generation of keys. Some important encryption algorithms are discussed here:

3.1 Rivest-Shamir-Adleman (RSA)

RSA is designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. It is one of the best known 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 [12, 13]. 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 [11]. Figure 2 illustrates the sequence of events followed by RSA algorithm for the encryption of multiple blocks.

3.1.1 Key Generation Procedure [14]

1. Choose two distinct large random prime numbers p & q such that p ≠ q.
2. Compute n= p × q.
3. Calculate: phi (n) = (p-1) (q-1).
4. Choose an integer e such that 1<e<phi(n)
5. Compute d to satisfy the congruence relation d × e = 1 mod 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.

3.1.2 Encryption

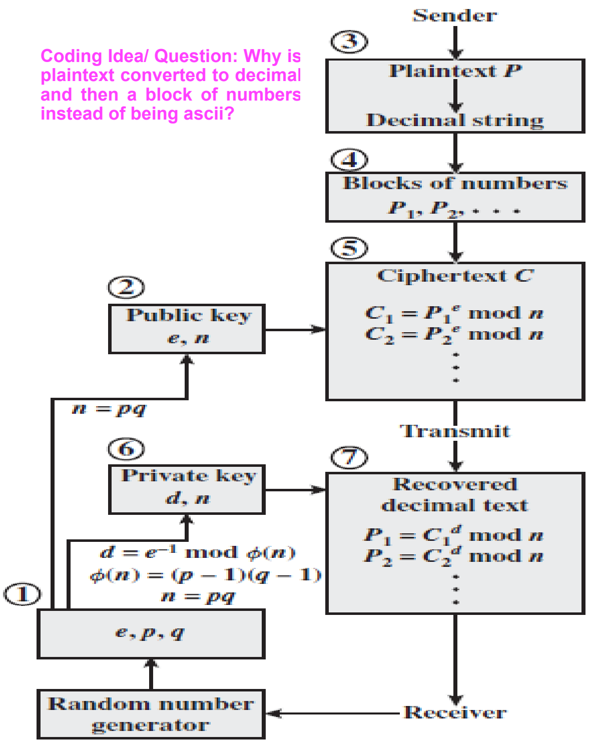
Plaintext: P < n
Ciphertext: C= P^e mod n.

3.1.3 Decryption

Ciphertext: C
Plaintext: P=C^d mod n.

3.2 Data Encryption Standard (DES)

DES is one of the most widely accepted, publicly available cryptographic systems. It was developed by IBM in the 1970s but was later adopted by the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46). The Data Encryption Standard (DES) is a block Cipher which is designed to encrypt and decrypt blocks of data consisting of 64 bits by using a 64-bit key [10, 15].



Coding Idea/ Question: Why is plaintext converted to decimal and then a block of numbers instead of being ascii?

Fig 2: RSA processing of Multiple Blocks [3]

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 [3, 16].

The flow of DES Encryption algorithm is shown in Figure 3. The algorithm processes with an initial permutation, sixteen rounds block cipher and a final permutation (i.e. reverse initial permutation).

3.3 Triple DES (3DES)

3DES or the Triple Data Encryption Algorithm (TDEA) was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Data Encryption Standard (DES) uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. 3-DES simply extends 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 (3 times 56). TDEA involves using three 64-bit DEA keys (K1, K2, K3) in Encrypt-Decrypt- Encrypt (EDE) mode, that is, the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3 [17]. The standards define three keying options:

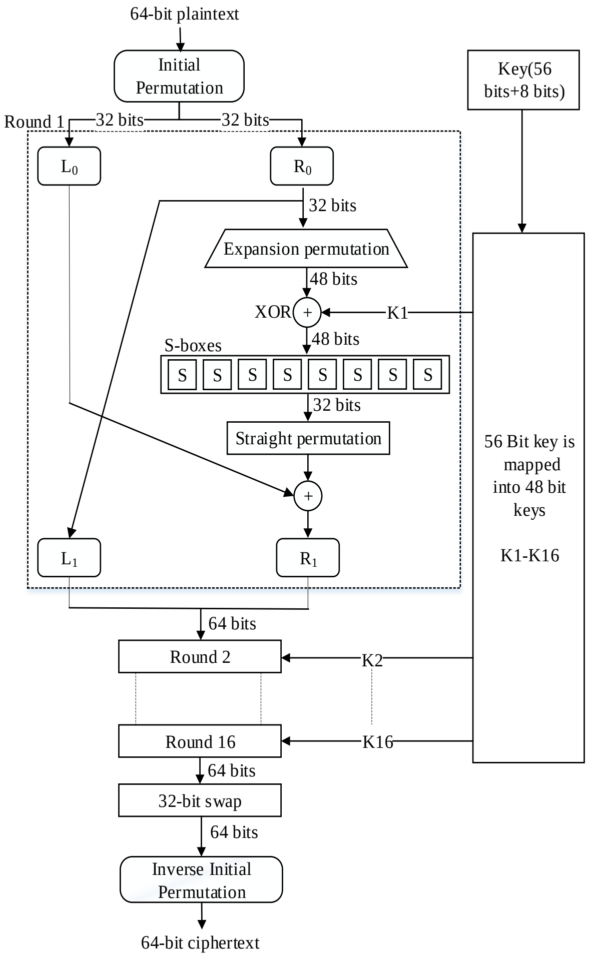


Fig 3: General Depiction of DES

Option 1, the preferred option, employs three mutually independent keys (K1 ≠ K2 ≠ K3 ≠ K1). It gives keyspace of 3 × 56 = 168 bits.

Option 2 employs two mutually independent keys and a third key that is the same as the first key (K1 ≠ K2 and K3 = K1). This gives keyspace of 2 × 56= 112 bits.

Option 3 is a key bundle of three identical keys (K1 = K2 = K3). This option is equivalent to DES Algorithm.

In 3-DES the 3-times iteration is applied to increase the encryption level and average time. It is a known fact that 3DES is slower than other block cipher methods [11, 18].

3.4 Advanced Encryption Standard (AES)

AES is the new encryption standard recommended by NIST to replace DES in 2001. 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 [19]. 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 AddRoundKey stage. However, before reaching the final round, this output goes though 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 [3, 20]. Figure 4 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 [10]:

Need more review. Dont quite understand this

3.4.1 *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 substitution box which is known as Rijndael Sbox.

3.4.2 *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.

3.4.3 *Mixcolumns 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.

3.4.4 *Addroundkey 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.

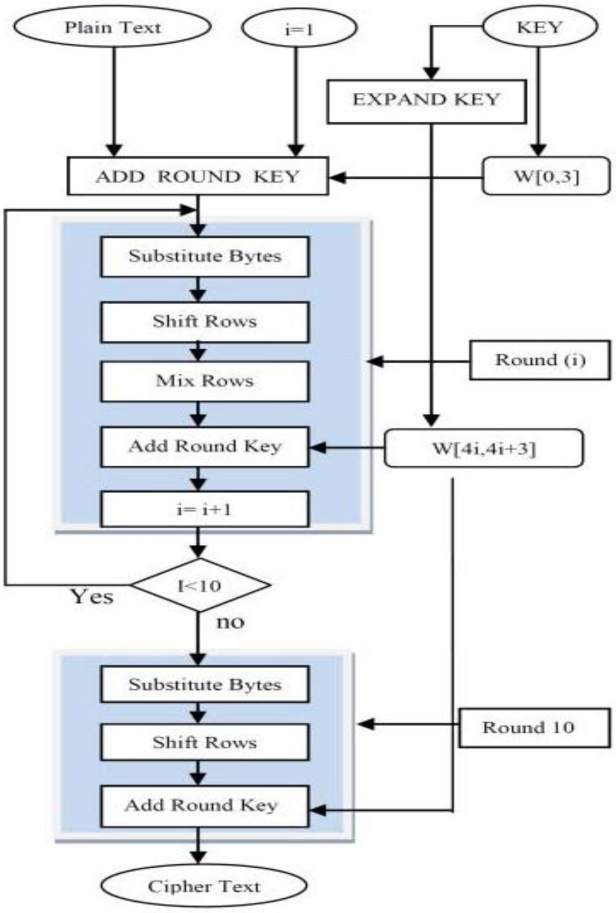


Fig 4: AES (Advanced Encryption Standard) process [10]

4. COMPARITIVE STUDY OF SECURITY ALGORITHMS

Table 1. shows that Asymmetric Algorithms such as RSA etc. are slower than that of Symmetric Algorithms and RSA is least secure algorithm as compared to DES, 3DES and AES.

5. CONCLUSION AND SCOPE OF FUTURE WORK

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. 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 pro's and con's. 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.

6. REFERENCES

[1] Tingyuan Nie, Chuanwang Song and Xulong Zhi, "Performance Evaluation of DES and Blowfish Algorithms", IEEE International Conference on Biomedical Engineering and Computer Science (ICBECS- 2010), pp. 1-4, 23-25 Apr 2010.

[2] Behrouz A Forouzan, "Data Communications and Networking", McGraw-Hill, 4th Edition.

[3] William Stallings, "Cryptography and Network Security: Principles and Practice", Pearson Education/Prentice Hall, 5th Edition.

[4] E. Thambiraja, G. Ramesh and Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, pp. 226-233, July 2012.

[5] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, pp. 280-286, December 2008.

[6] Priyanka Arora, Arun Singh and Himanshu Tiyagi, "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, 2012.

[7] Shashi Mehrotra Seth, Rajan Mishra, "Comparative Analysis of Encryption Algorithms for Data Communication", International Journal of Computer Science and Technology, Vol. 2, Issue 2, pp. 292-294, June 2011.

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

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

[10] Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2012.

[11] Ajay Kakkar, M. L. Singh and P.K. Bansal, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network", International Journal of Engineering and Technology, Volume 2 No. 1, pp. 87-92, January 2012.

[12] Aman Kumar, Dr. Sudesh Jakhar and Mr. Sunil Makkar, "Comparative Analysis between DES and RSA Algorithm's", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, pp. 386-391, July 2012.

[13] Xin Zhou and Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", the 6th International Forum on Strategic Technology, pp. 1118 – 1121, 2011.

[14] Uma Somani, Kanika Lakhani and Manish Mundra, "Implementing Digital Signatures with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 1st International Conference on Parallel, Distributed and Grid Computing (PDGC), pp. 211-216, 2010.

Table 1. Comparision of RSA, DES, 3DES and AES

Factors	RSA	DES	3DES	AES
Created By	Ron Rivest, Adi Shamir, and Leonard Adleman In 1978	IBM in 1975	IBM IN 1978	Vincent Rijmen, Joan Daemen in 2001
Key Length	Depends on number of bits in the modulus n where n=p*q	56 bits	168 bits (k1, k2 and k3) 112 bits (k1 and k2)	128, 192, or 256 bits
Round(s)	1	16	48	10 - 128 bit key,12 - 192 bit key,14 - 256 bit key
Block Size	Variable	64 bits	64 bits	128 bits
Cipher Type	Asymmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Speed	Slowest	Slow	Very Slow	Fast
Security	Least Secure	Not Secure Enough	Adequate Security	Excellent Security

[15] Sriram Ramanujam and Marimuthu Karuppiah, "Designing an algorithm with high Avalanche Effect", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1, pp. 106-111, January 2011.

[16] “DES”, http://www.tropsoft.com/strongenc/des.htm

[17] “3DES”, http://www.cryptosys.net/3des.html

[18] “3DES”, http://en.wikipedia.org/wiki/Triple_DES

[19] Mr. Gurjeevan Singh, Mr. Ashwani Singla and Mr. K S Sandha, "Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System", International Journal of Multidisciplinary Research, Vol.1 Issue 4, pp. 143-151, August 2011.

[20] Zilhaz Jalal Chowdhury, Davar Pishva and G. G. D. Nishantha, “AES and Confidentiality from the Inside Out”, the 12th International Conference on Advanced Communication Technology (ICACT), pp. 1587-1591, 2010.