Comparative Analysis on RSA Algorithm And DES Algorithm

Dr.A.Banumathi[1], K.Sathiyapriya[2]
[1, 2] Department of Computer science
[1, 2] Government Arts College, Karur, Tamilnadu, India

Abstract- *A set of devices are connected by communication links are knows as network.. Encryption has come up as a solution, and plays an important role in information security system. Encryption is a electronic locking ie sender puts the message in a box and locks the box by using a key. Decryption technique the receiver can view the original data. The receiver unlocks the box with a key and takes out the message. There are many algorithm were proposed in past years. In these two algorithms comparison, now that are RSA(Riverst Shamir Adlemen) and DES(Data Encryption Standard).RSA is public key encryption algorithm.DES means that is encrypts data 64bits at a time. In this paper compares the Thorughput, Input size, Key size, Confidentiality, Encryption, and Decryption by using RSA and DES.*

Keywords- RSA, DES, Encryption, Decryption, Keysize, Blocksize.

I. INTRODUCTION

Cryptography is where security engineering meets mathematics. The provides us with the tools that most modern security protocols. The basic terminology is that cryptography refers to the science. The input to an encryption process is commonly called the plaintext, and the output the ciphertext. The block ciphers may either have one key for both encryption and decryption which case they are called shared key(symmetric key),or have separate keys for encryption and decryption, which case called public key or asymmetric.[1]

Encryption is a mechanism that protects your valuable information, such as your documents, pictures, or online transactions, from unwanted people accessing or changing it. Encryption works by using a mathematical formula called a cipher and a key to convert readable data (plain text) into a form that others cannot understand (cipher text). In the cipher is the general recipe for encryption, and your key makes your encrypted data unique. Only people with your unique key and the same cipher can unscramble it. Keys are usually a long sequence of numbers protected by common authentication mechanisms, such as passwords, tokens, or biometrics (like your fingerprint).It Maintain the overall security of your computer. Encryption does nothing to protect against viruses, worms, Trojans, unmatched vulnerabilities, or social engineering attacks. Always be sure to back up any confidential data securely. Thus ensures that if you lose your device or your encryption keys protecting your data, you can still recover your data. Use encryption based on publicly known algorithm, Also, always be sure you are using the latest version of your encryption programs. The consult an IT professional if you need help. Incorrectly installing, configuring, or using encryption can render your information permanently in accessible

There are used in two keys:

- Private key
- Public key

Here we compared two algorithms one is based on private key is RSA(Rivest-Shamir-Adleman) another one is based on public key is DES(Data Encryption Standard).

II. RSA ALGORITHM

The most commonly used asymmetric algorithm is Rivest-Shamir-Adleman (RSA)[7].It was introduced by its three inventors, Ronald Rivest, Adi Shamir and Leonard Adleman in 1977. It is mostly used in key distribution and digital signature processes. RSA is based on a one-way function in number theory, called “integer factorization”.[2]. The one-way function is a function, which is “easy” to compute one way, but “hard” to compute the inverse of it. Here easy and hard should be understood with regard to computational complexity, especially in terms of polynomial time problems.

1. RSA Cryptosystem

The original RSA algorithm was publicly illustrated in 1977 [2] and after that many related algorithms were projected based of original RSA in order to set right the flaw of the basic algorithm. The Original RSA scheme is as follows:

A. Key Generation Algorithm

Step1: Randomly and secretly choose two large primes: p, q and compute n = p. q
Step2: Compute ϕ (n) = (p – 1) (q – 1) .
Step3: Select Random Integer: e such as 1 < e < n and gcd (e, ϕ) = 1.
Step4: Compute d such as e. d ≡ 1 mod ϕ(n) and 1 < d < ϕ (n) .
Step5: Public Key: (e, n)
Step6: Private Key: (d, n).

B. Encryption process

Step1: Suppose entity R needs to send message m to entity S (represent m as an integer in the range of 0 < m<n).
Step2: Entity S should send his public key to entity R.
Step3: Entity R will encrypt m as c = me mod n and will send c to entity S.

C. Decryption Process

Step1: Entity S will decrypt the received message as m = cd mod n.

The most important advantage of RSA[2] is ensuring about the privacy of the private key because this key will not be transmitted or revealed to another user. However, this algorithm has some considerable weaknesses. The main computational costs of the RSA are the modular exponentiations found during the key generation, encryption and decryption process [2]. Moreover, this algorithm has some weaknesses against certain attacks (i.e., Brute force,)

2. RSA cryptography

There are many interesting applications of number theory and abstract algebra, especially in computer-related subjects. We shall look closer at one famous application to cryptography.[2]

To improve the security of information using RSA Algorithm, Norihidaya Mohammad et al. had proposed Loop Based Key Generation Algorithm using String Identity uses email id of user as public key in their key generation process

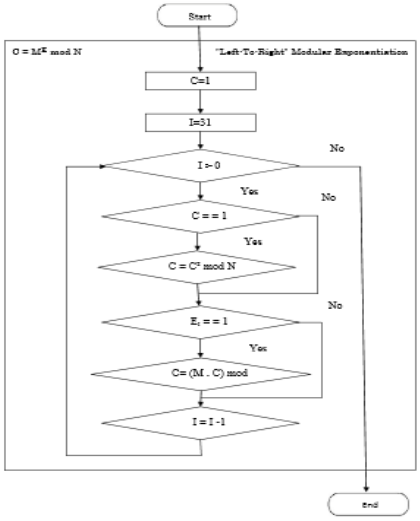

Figure 1. RSA Algorithm

3. Security

The Security of RSA mainly lies with the Selection of a large prime number, an Encryption Key and a Decryption Key. Factoring large numbers is not provably hard, but no algorithms exists today to factor a 200-digit number in a reasonable amount of time. The main feature of RSA algorithm is the selection of large prime number (p, q) because it is logical that fraction of large number is always typical and any users or force attackers could not be able to find the capable numbers, timely to force attack is shortly non-feasible.[4]

a) The problem of secure communication

Suppose that two persons want to communicate with each other, and they want to protect their communication from being overheard by a third party.[5]

This could for example be any of the following situations:

1. I want to buy a book at the online bookshop Amazon. To do this, I send them my credit card number through the Internet, so that they can deduct the correct amount of money from my bank account. A skilled hacker can easily interrupt the communication, get hold of my credit card number, and use it to take all the money in my account.
2. 2Sarah is deeply in love with Otieno, but her parent thinks she is too young to have a boyfriend. So Sarah needs to send secret messages to Otieno that her parents cannot understand, even if they manage to find one of the messages.
3. The researchers at the company Amazing Machines Ltd has come up with an idea for a machine that could produce large amounts of electricity very cheaply. They

want to discuss these ideas through email with some leading physicists in Japan, but if someone else manages to interrupt the email communication, they could steal the idea, and the company could lose millions of dollars. So how can these problems be solved? How can these people communicate in a safe way? These kinds of problems are investigated in the field of cryptography.

The simplest way of solving the problem is to agree on some kind of encoding scheme. For example, Sarah and Otieno could agree that in their letters, every A means B, every B means C, every C means D etc. In this case, Otieno could for example send a letter with the message

H KNUD XNT

and Sarah would be very happy, and write back:

H KNUD XNT SNN, RVDDSHD!
59

If her mother found the piece of paper with these letters, she would not understand, and Sarah could probably convince her that this is just the password for her web mail. There are many other, much more complicated, ways of encoding messages(any such method is called an encoding scheme) so that they are not easily readable to others. However, there are two possible problems with all of these methods.

- Problem 1: If the code is not complicated enough, it could easily be cracked by someone with a computer (perhaps Sarah's mother has computer programming as a hobby. . . scary!)
- Problem 2: Suppose that Sarah's father gets hold of the first letter, where they write down which encoding scheme to use! Then he would be able to understand every subsequent letter he can find, with catastrophic consequences! The first problem can perhaps be solved by making the encoding complicated enough, but the second is a major problem! If for example my computer system agrees with the Amazon website on how to encode the credit card number, and someone gets hold of this information, then they will be able to read my credit card number even if it is encoded! This problem can actually be overcome, by using something called RSA cryptography.[5]

4. Advantages

RSA's biggest advantage is that it uses Public Key encryption. This means that your text will be encrypted with someone's Public Key (which everyone knows about). However, only the person it is intended for can read it, by using their private key (which only they know about). Attempting to use the Public Key to decrypt the message would not work. RSA can also be used to "sign" a message, meaning that the recipient can verify that it was sent by the person they think it was sent by.[4]

5. Disadvantages

A disadvantage of using public-key cryptography for encryption is speed. There are many secret-key encryption methods that are significantly faster than any currently available public-key encryption method. Nevertheless, public-key cryptography can be used with secret-key cryptography to get the best of both worlds. For encryption, the best solution is to combine public and secret-key systems in order to get both the security advantages of public-key systems and the speed advantages of secret-key systems. Public-key cryptography may be vulnerable to impersonation, even if users' private keys are not available.[4]

III. DES ALGORITHM

The Data Encryption Standard DES is a symmetric-key block cipher published by the National Institute of Standards and Technology NIST.DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm function as check bits only.[6]

There are following steps in algorithm

- It takes 64 bit long plain text data block as in put and 56 bit key and generates output of 64 bit block.[7]
- The plaintext undergoes an initial permutation when it enters the encryption function, IP. It undergoes a reverse final permutation at the end IP.
- The 64 bit plain text passes through an initial permutation (IP) that rearranges the bit to produce the permutated bit.
- The IP produces 2 halves of permuted block- left plain text and right plain text.
- 16 rounds of encryption is done each with its own keys.
- The output of above 16 rounds consists of 64 bits that are function of input plain text and key.

- At last the output is passed through final permutation (FP) also called inverse IP to pro 64 bit cipher text.[7]

The following flow chart shows the DES algorithm :

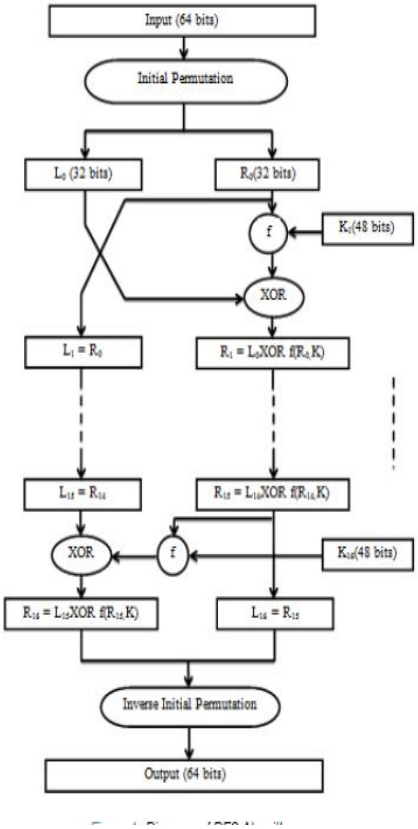

Figure 2. DES Algorithm

General Structure of DES is depicted in the following illustration[6]

Then the mode of encryption is called Electronic Code Book(ECB) mode. There are two other modes of DES encryption, namely Chain Block Coding (CBC) and Cipher Feedback (CFB), which make each cipher block dependent on all the previous messages blocks through an initial XOR operation.

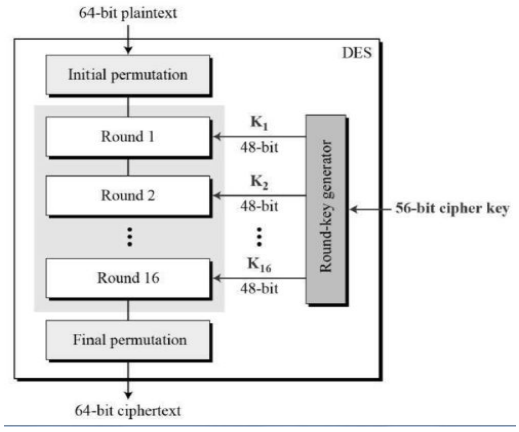

Figure 3. General structure

Since DES is based on the Feistel Cipher, all that is required to specify DES is −

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

1. Initial and Final Permutation

The initial and final permutations are straight Permutation boxes P − boxes that are inverses of each other. They have no cryptography significance in DES.

2. Round Function

The heart of this cipher is the DES function, f. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

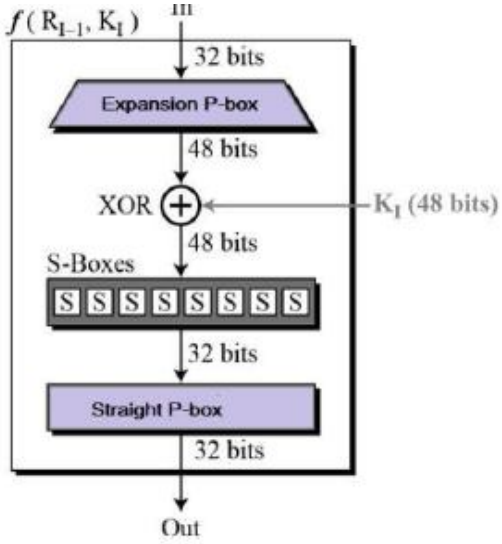

Figure 4. Round Function

3. Advantages

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

Avalanche effect –

A small change in plaintext results in the very grate change in the cipher text.

Completeness –

Each bit of cipher text depends on many bits of plaintext. During the last few years, cryptanalysis have found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.

4. Triple DES

The speed of exhaustive key searches against DES after 1990 began to cause discomfort amongst users of DES. However, users did not want to replace DES as it takes an enormous amount of time and money to change encryption algorithms that are widely adopted and embedded in large security architectures. The pragmatic approach was not to abandon the DES completely, but to change the manner in which DES is used. This led to the modified schemes of Triple DES sometimesknownas3DES.Incidentally, there are two variants of Triple DES known as 3-key Triple DES 3TDES and 2-key Triple.[8]

1) 3-KEY Triple DES

Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys K1, K2 and K3. This means that the actual 3TDES key has length 3×56 = 168 bits. The encryption scheme is illustrated as follows[8]

The second key is used to DES-decrypt the encrypted message. (Since the second key is not the right key, this decryption just scrambles the data further.) The twice-scrambled message is then encrypted again with the first key to yield the final cipher text. This three-step procedure is called triple-DES.

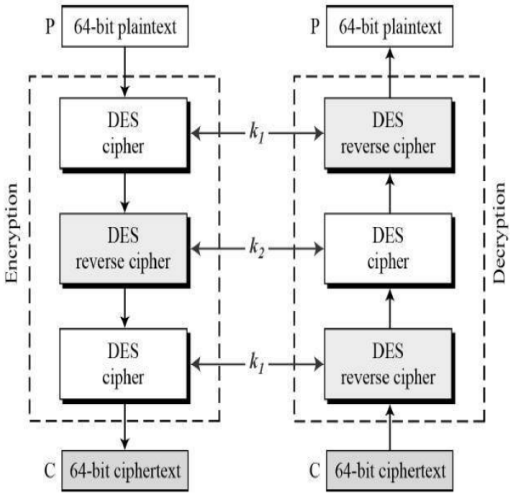

Figure 5. Triple DES

The encryption-decryption process is as follows :

- Encrypt the plaintext blocks using single DES with key K1.
- Now decrypt the output of step 1 using single DES with key K2.
- Finally, encrypt the output of step 2 using single DES with key K3.
- The output of step 3 is the cipher text.
- Decryption of a cipher text is a reverse process. User first decrypt using K3, then encrypt with
- K2, and finally decrypt with K1.

Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES hardware implementation for single DES by setting K1, K2, and K3 to be the same value. This provides backwards compatibility with DES. Second variant of Triple DES 2TDES is identical to 3TDES except that K3is replaced by K1. In other words, user encrypt plaintext blocks with key K1, then decrypt with key K2, and finally encrypt withK1 again. Therefore, 2TDES has a key length of 112 bits. Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.[8]

5. Disadvantages

The brute force attack has decryption the DES without any algorithm. This is the main drawback of DES. To avoid this NIST(national institute for science and technology)has announce a competition. In that many algorithm has submitted.

IV. COMPARTIVE ANALYSIS

Comparison on of secret key and public key based DES and RSA algorithms. RSA solves the problem of the key agreement and key exchange problem generated in secret key cryptography .But still its confidentiality is low .So DES is used. RSA and DES differ from each other in certain features[7].In the table below comparative study between Block size, Key, Developed, Throughput, Confidentiality, Power consumption, Rounds.

The decryption throughput of different algorithms are used for data security. The selected algorithms DES and RSA are discussed with their working mechanisms.

Table 1. Comparative analysis

FEATURES	DES	RSA
BLOCKSIZE	64bits	Minium512bits
KEY	Same key for encryption and decryption	Different key for encryption and decryption
DEVELOPED	1977	1978
THROUHPUT	Very high	Low
CONFIDENTIALITY	High	Low
POWER CONSUPTION	Low	High
ROUNDS	16	1

Key is similar to one time pad used in vernam cipher. If same key is used for encryption and decryption then this is called secret key cryptography[11]. And if different keys are used encryption and decryption we call this public key cryptography. In secret key cryptography single key is used. So as before distributing the data between entities the key must be transferred. Secret key cryptography includes DES etc. Throughput of the encryption algorithms is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm. Thus, if throughput increased the power consumption is decreased. The use block cipher. It encryption the data in block size of 64 bits each[11]. The substitution is simply a mapping of one value to another whereas permutation is a reordering of the bit positions for each of the inputs. These techniques are used a number of times in iterations called rounds. Generally, the more rounds there are, the more secure the algorithm. A non-linearity is also introduced into the encryption so that decryption will be computationally infeasible without the secret key. The throughput is the most important parameters, which differentiate RSA from DES. Because DES provides in 24% more throughput than RSA. The above comparison shows that DES provide better results than RSA.

V. IMPACT OF RSA AND DES ALGORITHM

RSA will provide good result in Trojan horse attack.DES will provide security from Zombie, Lovekiler attack.RSA will used in Digital signatures. RSA are used to authentication purpose. DES are used to create the key stream. The fundamentally serial nature of many cryptography algorithms. It means that single process thread level parallelism is rare. The numerous permutations and non-linear transformations also tend to hide much of data level parallelism. An interesting attribute of many cryptography algorithms is that the operation to be performed on input data is completely deterministic.

VI. MEASURE OF RSA ALGORITHM AND DES ALGORITHM

1. RSA algorithm Encryption, Decryption :

$$c = m^e \bmod n$$

$$m = c^d \bmod n.$$

2. DES algorithm Encryption, Decryption:

(i) Initial permutation

P(n,r)=n!(n-r)!

(ii) XOR Gate

- 2 input XOR gate

1) Message Data
2) Key Data

Table 2.

M	K	Y
0	0	0
0	1	1
1	0	1
1	1	1

3. Throughput Encryption

$$Throughput = \frac{\sum All\ input\ size}{\sum EET}$$

4. Throughput Decryption

$$Throughput = \frac{\sum \text{All input size}}{\sum \text{DET}}$$

VI. RESULT ANALYSIS

The Table 1 represents the five different size and corresponding encryption execution time taken by DES and RSA algorithm in seconds by analyzing the table. we conclude that the encryption time taken by DES is very small as compare to relatively small as compared to RSA. RSA has taken the large encryption time as compare to DES. The encryption time taken by DES, RSA and five different size input files are also shown in figure 7.1.

Table 3. Encryption Execution Time

Input File Size(KB)	DES	RSA
10KB	3.0292	3.7582
20KB	6.0584	7.5164
25KB	7.5730	9.3956
40KB	12.1169	15.0329
50KB	15.1461	18.7912
145KB	43.9238	54.4943
Throughput Size	3.30 KB/Seconds	2.660 KB/Seconds

The Table 4 represents the five different sizes of files and corresponding decryption time taken by

Table 5. Decryption Execution Time

Input File Size(KB)	DES	RSA
10KB	3.0292	3.7582
20KB	6.0584	7.5164
25KB	7.5730	9.3956
40KB	12.1169	15.0329
50KB	15.1461	18.7912
145KB	43.9238	54.4943
Throughput Size	3.30 KB/Seconds	2.660 KB/Seconds

DES,and RSA algorithms in seconds. By analyzing the table 2 we conclude that the encryption time taken by DES is very small as compare to relatively small as compare to RSA.RSA have taken the large decryption time as compare to DES. The encryption time taken by DES, RSA and five different size input files are also shown in figure7.2.

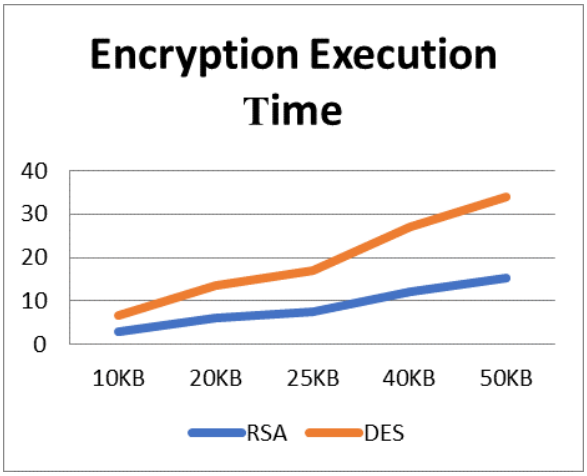

Figure 6. EET among DES and RSA

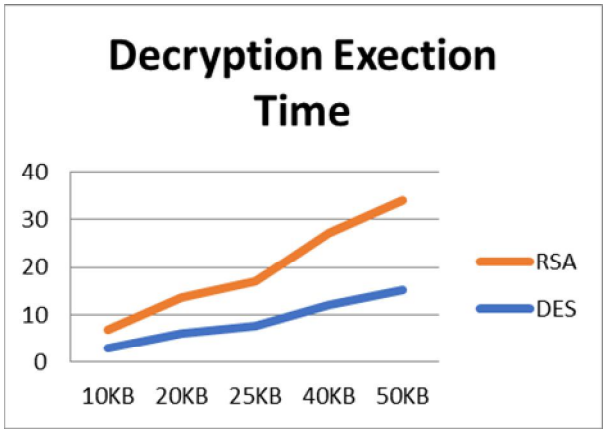

Figure 7. DET among DES and RSA

Decryption speed of DES algorithm is also high as compared to RSA algorithm

VII. CONCLUSION AND FUTURE SCOPE

In this paper, studied that the Encryption and decryption execution time consumed by DES algorithm is least as compared to RSA algorithm. Recent days, there is many of algorithm are proposed to avoid data modification, and corruption. But some algorithms are failed to satisfy above mentioned requirements. By this way RSA and DES are the algorithms are proposed in previous years. Here both algorithm are compared with various parameters like Throughput, Input size, Key size, Confidentiality, Encryption, Decryption.The throughput is the most important parameters, which differentiate RSA from DES. Because DES provides in 24% more throughput than RSA. The above comparison

shows that DES provide better results than RSA.The comprition result a new algorithm is proposed as AES, and provide confidentiality and integrity during data transmission.

REFERENCES

[1] G. Julius Caesar, John F. Kennedy Xyawo Gaooa Gpemo Hpqcw Ipnlg Rpixl Txloa Nnycs Yxboy Mnbin Yobty

[2] S.Hemalatha, Dr.R.Manickachezian "Seurity Strength of RSA and Attribute Based Encryption for Data Security" .

[3] Dr. Prerna Mahajan, Abhishek Sachdeva " A Study of Encryption Algorithms AES,DES and RSA for Security ".

[4] Gururaja.H.S, M.Seetha, Anjan K Koundinya, Shashank.A.M and Prashanth.C.A."Comparative Study and Performance Analysis of Encryption in RSA, ECC and Goldwasser-Micali Cryptosystems" Assistant Professor, Department of Information Science & Engineering, B.M.S. College of Engineering, Bangalore, India

[5] Application: RSA cryptography

[6] http://www.tutorialspoint.com/cryptography/data_encryption_standard.htmCopyright©tutorialspoint.com.DATA ENCRYPTION STANDARD

[7] Mr.Ankit Gambhir, Mr.Student, M.tech (CE), Galgotias University, U.P, India RSA algorithm and DES algorithm

[8] http://www.tutorialspoint.com/cryptography/triple_des.htmCopyright©tutorialspoint.comTRIPLE-DES

[9] Mr.MILIND MATHUR ,Mr.AYUSH KESARWANI COMPARISON BETWEEN DES , 3DES , RC2 , RC6 , BLOWFISH AND AES

[10] Mr.Ankita Verma,Mr.Paramita Guha,Mr.Sunita Mishra Comparative Study of Different Cryptographic Algorithm

[11] Mr.Aman Kumar, Mr. Sunil Makkar, Dr. Sudesh Jakhar Analysis between DES and RSA Algorithm'

[12] Mr.Sangita A. Mr.Jaju,Santosh Mr.S. ChowhanAnalytical Study of Modified RSA AlgorithmS for Digital Signature

[13] Mr. Hemant Kumar, Dr. Ajit Singh An Efficient Implementation of Digital Signature Algorithm with SRNN Public Key Cryptography

[14] Sombir Singh1, Sunil K Maakar, Dr. Sudesh Kumar A Performance Analysis of DES and RSA Cryptography

[15] Mr.Vaibhav Shrivastava,Mr.Gurpal Singh Impact of Security over System performance.