International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 2, Issue 3, May – June 2013 ISSN 2278-6856

A Performance Analysis of DES and RSA Cryptography

Sombir Singh[1], Sunil K Maakar[2] and Dr. Sudesh Kumar[3]

[1]M D University, BRCM CET, M.Tech. Scholar in CSE,
Bahal, Bhiwani 127028, India

[2] M D University, BRCM CET, Asstt. Prof. in CSE,
Bahal, Bhiwani 127028, India

[3] M D University, BRCM CET, Assoc. Prof. & Head in CSE,
Bahal, Bhiwani 127028, India

Abstract: ***Security is playing a vital role in the field of communication system and Internet. Data encryption standard (DES) and the Rivest-Shamir-Adleman (RSA) algorithms are the two popular encryption algorithms that vouch confidentiality and authenticity over an insecure communication network and Internet. There has been paltry cryptanalytic progress against these two algorithms since their advent. This paper presents the comparison between the DES private key based Algorithm and RSA public key based algorithm. The main feature that specifies and differentiate one algorithm from another are the ability to the speed of encryption and decryption of the input plain text. It also includes several computational issues as well as the analysis of DES algorithm and RSA algorithm like the encryption throughput and decryption throughput. The recipe of finding the encryption throughput and decryption throughput is discovered.***

Keywords: Encryption, EET, Decryption, DET, Plain text, Cipher text, RSA, DES, RPT, LPT.

1. INTRODUCTION

The process of encoding the plaintext into cipher text is called Encryption and reverse the process of decoding ciphers text to plaintext is called Decryption. This can be done by two techniques symmetric-key cryptography and asymmetric key cryptography. Symmetric key cryptography involves the usage of the same key for encryption and decryption. But the Asymmetric key cryptography involves the usage of one key for encryption and another, different key for decryption. Secret key cryptography includes DES, AES, 3DES, IDEA, Blowfish algorithms etc. and public key cryptography includes RSA, Digital Signature and Message Digest algorithms [10],[14].

For each algorithm there are two key aspects used: Algorithm type (define size of plain text should be encrypted per step) and algorithm mode (define cryptographic Algorithm mode). Algorithm mode is a combination of a series of the basic algorithm and some block cipher and some feedback from previous steps. We compare and analyzed algorithms DES and RSA [6].

2. DATA ENCRYPTION STANDARD

DES is a block cipher. It encrypts the data in a block of 64 bits. It produces 64 bit cipher text. The key length is 56 bits. Initially the key is consisting of 64 bits. The bit position 8, 16, 24, 32,40,48,56, 64 discarded from the key length [16].

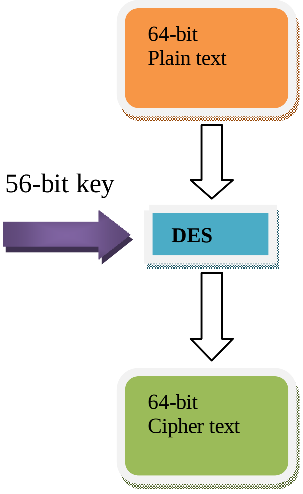

Figure 1 The conceptual working with DES

DES is based on two fundamental attributes of cryptography: Substitution (confusion) and transposition (Diffusion). DES consists of 16 steps, each of which called as a Round.

Algorithm:-

[1] In the first step, the initial 64-bit plain text block is handed over to Initial Permutation (IP) function.

[2] The Initial permutation is performed on plain text.

[3] The initial permutation produces two halves of permuted block: Left Plain text (LPT) and Right Plain (RPT).

[4] Now, each of LPT and RPT goes through 16 rounds of the encryption process, each with its own key:

a. From the 56-bit key, a different 48-bit Sub-key is generated using Key Transformation.

b. Using the Expansion Permutation, the RPT is expended from 32 bits to 48 bits.

c. Now, the 48-bit key is XORed with 48-bit RPT and the resulting output is given in the next step.

d. Using the S-box substitution produce the 32-bit from 48-bit input.

e. These 32 bits are permuted using P-Box Permutation.

f. The P-Box output 32 bits are XORed with the LPT 32 bits.

g. The result of the XORed 32 bits is become the RPT and old RPT become the LPT.This process is called as swapping.

h. Now the RPT again given to the next round and performed the 15 more rounds.

[5] After the completion of 16 rounds the Final Permutation is performed [10], [17].

3. Double DES

It is also called 2DES. Its process is the same as DES but repeated the same process 2 times using two keys K1 and K2. First it takes plain text, produced the cipher text using K1 and then take up the cipher text as input, produced another cipher text using K2 shown in figure 2. The Decryption Process is shown in figure 3[14].

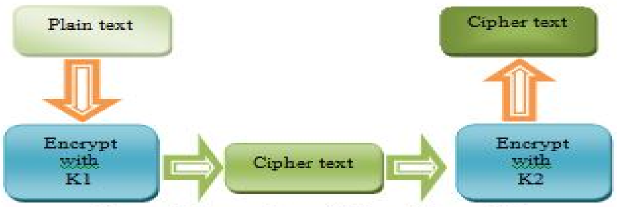

Figure 2 Encryption with key K1 and K2

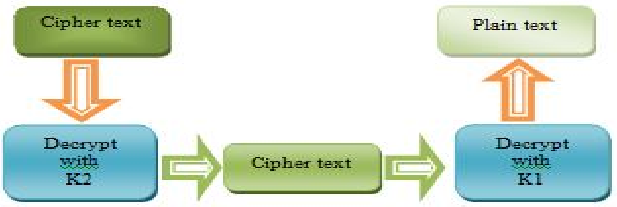

Figure 3 Encryption with key K1 and K2

4. Triple DES

Triple DES is DES -three times. It comes in two flavors: One that uses three keys, and another that uses two keys. The Idea of 3-DES is shown in the figure 4. The plain text block P is first encrypted with a key K1, then encrypted with second key K2, and finally with third key K3, where K1, K2 and K3 are different from each other. To decrypt the cipher text C and obtain the plain text, we need to perform the operation P= DK3 (DK2 (DK1(C))). But in Triple DES with two keys the algorithms work as follows:

[1] Encrypt the plain text with key K1. Thus, we have EK1 (p).

[2] Decrypt the output of step1 above with key K2. Thus, we have DK2 (EK1 (P)).

[3] Finally, encrypt the output of step 2 again with a key K1.Thus, we have EK1 (DK2 (EK1 (P))) [15].

The idea of 3-DES with two keys are shown in figure 5.

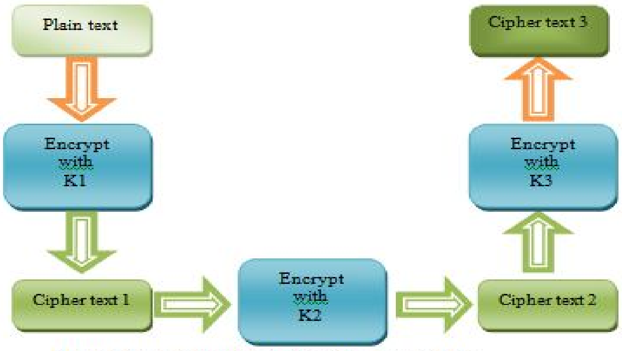

Figure 4 Encryption with key K1, K2 and K3

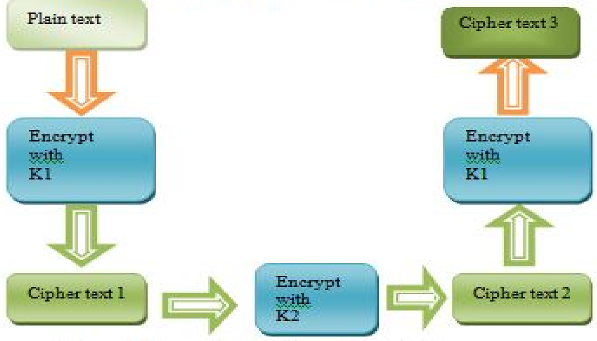

Figure 5 Decryption with key K1and K2

5. The RSA Algorithm

This is a public key encryption algorithm developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977.The RSA algorithm is the most popular and proven asymmetric key cryptographic algorithm. The RSA algorithm is based on the mathematical fact that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product. The private and public keys in the RSA are based on very large (made up of 100 or more digits) prime numbers. The algorithm itself is quite simple (unlike the symmetric key cryptographic algorithms). However, the real challenge in the case of RSA is the selection and generation of the public and private keys. The idea of asymmetric cryptographic is shown in figure 6. In which the A is the sender and B Receiver [4].

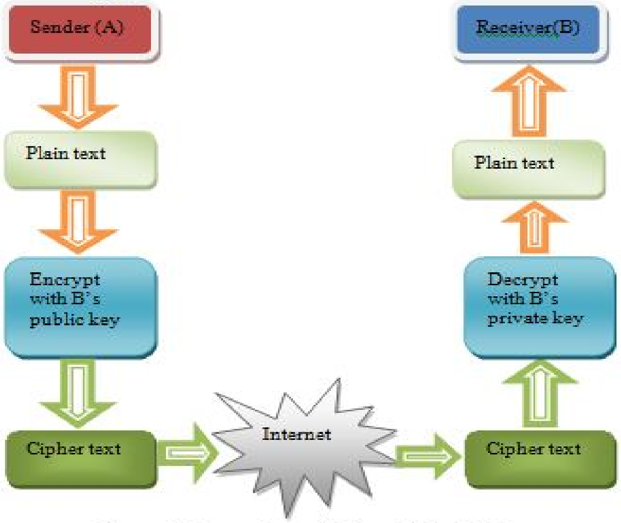

Figure 6 Decryption with key K1and K2

Algorithm:

[1] Choose two large prime numbers P and Q.

[2] Calculate N= P X Q.

[3] Select the public key (i.e. the encryption key) E such that it is not a factor of (P-1) and (Q-1).

[4] Select the private key (i.e. the decryption key) D such that the following equation is true: (D X E) mod (P-1) X (Q-1) =1

[5] For encryption, calculate the cipher text CT from text PT as follows: CT = PTE mod N [4], [10].

6. Experimental Design

The five different size text data files are given to the algorithms as input to check the performance of DES, 2DES and RSA. The experiment is performed on the machine [Intel® Pentium ® CPU G 630 @ 2.70 GHz, 2GB of RAM].The operating system and system software used for these algorithms are Windows XP Service Pack 3.0 and Turbo C++ 3.0.

7. Evaluation Parameters

Performance measurement criteria are time taken by the algorithms to perform the encryption and decryption of the input text files. The following are the parameters which calculate the performance of algorithms.

A. Encryption Computation Time

B. Decryption Computation Time

The encryption computation time is the time which taken by the algorithms to produce the cipher text from the plain text. The encryption time can be used to calculate the Encryption Throughput of the algorithms. The decryption computation time is the time taken by the algorithms to produce the plain text from the cipher text. The decryption time can be used to calculate the Decryption Throughput of the algorithms.

8. Experimental and Simulation Analysis

The TABLE 1 represents the five different sizes of files and corresponding encryption execution time taken by DES, 2DES and RSA algorithms in seconds. By analyzing the Table 1 we conclude that the encryption time taken by DES is very small as compare to 2DES and relatively small as compared to RSA. RSA has taken the large encryption time as compare to DES. The encryption time taken by DES, 2DES, RSA and five different size input files are also shown in figure 7.

The Table 2 represents the five different sizes of files and corresponding decryption time taken by DES, 2DES 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 2DES and relatively small as compare to RSA.RSA have taken the large decryption time as compare to DES. The encryption time taken by DES, 2DES, RSA and five different size input files are also shown in figure 8.

Input File Size (KB)	Encryption Execution Time(Seconds)		
	DES	2DES	RSA
15	4.543859	9.087718	5.637362
30	9.087718	18.17544	11.27472
45	13.63158	27.26315	16.91209
60	18.17544	36.35087	22.54945
75	22.7193	45.43859	28.18681

Table 1: Encryption Execution Time

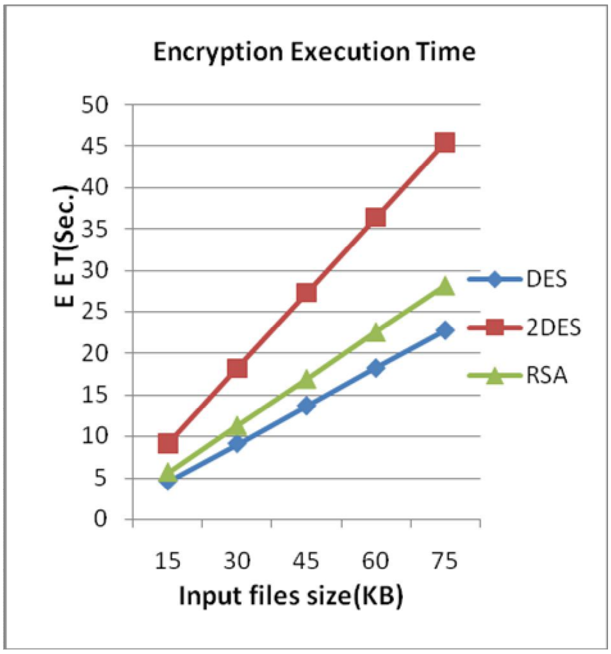

Figure 7 EET among DES, 2DES and RSA

$$\text{Encryption Throughput (KB/Sec.)} = \frac{\sum \text{input files}}{\sum \text{EET}}$$

∑input files [DES] = 225 KB

∑EET [DES] = 68.15789 Sec.

Encryption Throughput [DES] = 3.301159 KB/Sec.

∑input files [RSA] = 225 KB

∑EET [RSA] = 84.56043 Sec.

Input File Size (KB)	Decryption Execution Time(Seconds)		
	DES	2DES	RSA
15	4.543859	9.087718	5.637362
30	9.087718	18.17544	11.27472
45	13.63158	27.26315	16.91209
60	18.17544	36.35087	22.54945
75	22.7193	45.43859	28.18681

Encryption Throughput [RSA] = 2.660819 KB/Sec.

Table 2: Decryption Execution Time

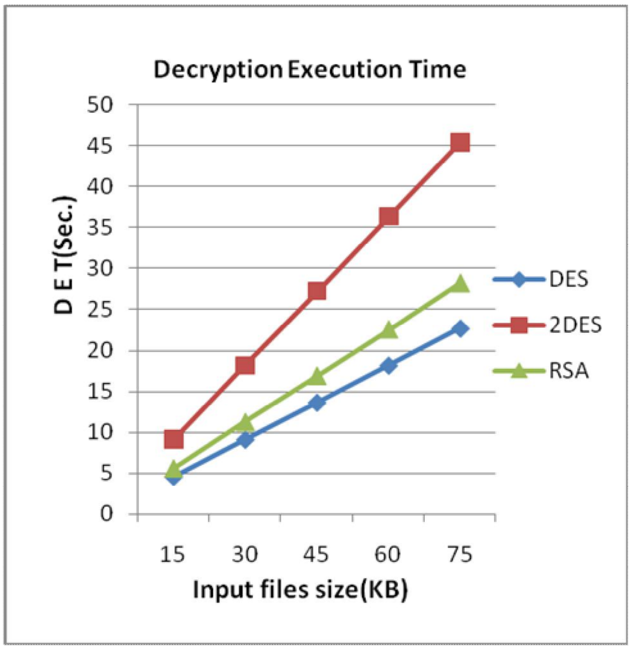

Figure 8 DET among DES, 2DES and RSA

$$\text{Decryption Throughput (KB/Sec.)} = \frac{\sum \text{input files}}{\sum \text{DET}}$$

∑size of input files [DES] = 225 KB

∑DET [DES] = 68.15789 Sec.

Decryption Throughput [DES] = 3.301159 KB/Sec.

∑input files [RSA] = 225 KB

∑DET [RSA] = 84.56043 Sec.

Decryption Throughput [RSA] = 2.660819 KB/Sec.

9. CONCLUSION

In this paper, we have studied that the encryption and decryption execution time consumed by DES algorithm is least as compared to RSA algorithm. The encryption and decryption speed of DES algorithm is fast as compared to RSA .The encryption execution time and decryption execution time consumed by DES algorithm is equal. The encryption execution time and decryption execution time consumed by RSA algorithm is same. The performance of DES is very good as compared to RSA. The throughput also explained that the encryption speed of DES is high as compared to RSA algorithm.

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

ACKNOWLEDGMENT

I would like to articulate our deep gratitude to my thesis guide Asst. Prof. Sunil Maaker who has always been my motivation for carrying out the paperwork. I express my deep sense of gratitude to Dr. Sudesh Kumar, Professor and Head of Computer Science and Engineering Department of BRCM College of Engineering and Technology, Bahal, Haryana for providing the necessary facilities during the research and encouragement from time to time. Special thanks to the institute, BRCM College of Engineering and Technology, for giving me such a nice opportunity to work in the great environment. Thanks to my friend and colleague who have been a source of inspiration and motivation that helped me during my dissertation period. And to all other people who directly or indirectly supported and help me to fulfill my task. Finally, I heartily appreciate my family members for their motivation, love and support in my goal.

References

[1] Abdullah Al Hasib, Abul Ahsan Md. Mahmudul Haque," A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography", Third International Conference on Convergence and Hybrid Information Technology,2008.

[2] Manikandan.G, Rajendiran.P, Chakarapani.K, Krishnan.G, Sundarganesh.G, “A Modified Crypto Scheme for Enhancing Data Security”, Journal of Theoretical and Advanced Information Technology, Jan 2012.

[3] Duncan S. Wong, Hector Ho Fuentes and Agnes H. Chan, “The Performance Measurement of Cryptographic Primitives on Palm Devices”, College of Computer Science, Northeastern University, Boston, MA 02115, USA.

[4] Adi Shamir Ronald Rivest and Len Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21:120–126, 1978.

[5] Kofahi, N.A. Turki Al-Somani Khalid Al-Zamil. Performance evaluation of three encryption/decryption algorithms.Circuits and Systems, 2003. MWSCAS ’03. Proceedings of the 46th IEEE International Midwest Symposium on, 2:790–793, 27-30 December 2003.

[6] William Stallings. Cryptography and Network Security Principles and Practices. Prentice Hall, November 16, 2005.

[7] A.Nadeem, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, pp.84-89, 2006.Bn

[8] DiaasalamaAbdElminaam, HatemMohamadAbdual Kader, Mohly Mohamed Hadhoud, “Evalution the Performance of Symmetric Encryption Algorithms”, international journal of network security vol.10,No.3,pp,216-222,May 2010. technologies, pp.84-89, 2006.Bn

[9] Diaasalama, Abdul kader, MohiyHadhoud, “Studying the Effect of Most Common Encryption Algorithms”, International Arab Journal of e-technology, vol 2,no.1,January 2011.

[10] Atul Kahte.Cryptography and Network Security.Tata Mcgraw Hill, 2007.

[11] Shasi Mehlrotra seth, Rajan Mishra “ ComparativeAnalysis of Encryption Algorithms For Data Communication”, IJCST Vol. 2, Issue 2, June 2011.

[12] Wuling Ren. A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication. Second International Conference on Modeling, Simulation and Visualization Methods (WMSVM), 2010.

[13] Sung-Jo Han, Heang-Soo Oh, Jongan Park, The improved Data Encryption Standard (DES) Algorithm,Department of Electronic Engineering, Chosun University. South Korea.1996 IEEE.

[14] Charels Connell, An Analysis of New DES: A Modified Version of DES, Locust Street Burlington, USA, Boston MA 02215 USA.

[15] D.B. Ojha, Ramveer Singh, Ajay Sharma, Awakash Mishra and Swati garg, An Innovative Approach to Enhance the Security of Data Encryption Scheme. International Journal of Computer Theory and Engineering, Vol. 2, No. 3, June, 2010

[16] Subbarao V. Wunnava, Data Encryption Performance and Evaluation Schemes, Florida International University, Miami, FL Ernest0 Rassi; Florida Intemational University, Miami, FL 0-7803-7252- 2/02/$10.00 0 2002 IEEE Proceedings IEEE Southeastcon 2002.

[17] D. Coppersmith, The Data Encryption Standard (DES) and Its strength Against attacks, IBM J. RES. Develop. VOL.38 NO.3 MAY 1994.

[18] Gaurav Shrivastava. Analysis Improved Cryptosystem Using DES with RSA. VSRD-IJCSIT, Vol. 1 (7), 465-470, 2011.

AUTHOR

Sombir Singh is a scholar of master of technology in computer science and engineering at BRCM College of Engineering and Technology, Bahal, Haryana, India. He is also Teaching Assistant in Computer science and Engineering Department at BRCM CET, Bahal, and Haryana, India. He has completed his AMIE in computer science and Engineering from The Institution of Engineers (India), Kolkata, India. His present area of interest is Network Security.

Sunil maker is an Assistant Professor in computer science and engineering Deptt. at BRCM College of Engineering and Technology, Bahal, Haryana, India. He has completed his AMIE in computer science and Engineering from The Institution of Engineers (India), Kolkata, India.He has received his M. Tech. (CSE) degree from NIT, Jalandhar, Punjab, India. He is pursuing his Ph.D in CSE from Punjab Technical Univercity, Jalandhar,Punjab,India.

Dr. Sudesh Kumar is a Professor and Head in computer science and engineering at BRCM College of Engineering and Technology, Bahal, Haryana, India.He is completed his B.Tech. in Information Technology .He has received his M.Tech. and Ph.D(CSE).