Volume 2, Issue 7, July 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Comparative Analysis between DES and RSA Algorithm's

Aman Kumar
(M.Tech student)
BRCM Bahal (Bhiwani)
aman.nehra063@gmail.com

Dr. Sudesh Jakhar
Associate Professor
BRCM Bahal (Bhiwani)
ksudesh@brcm.edu.in

Mr. Sunil Makkar
Assistant Professor
BRCM Bahal (Bhiwani)
skumar@brcm.edu.in

Abstract—Internet use and network growing quickly. 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. Encryption is the process of translating, plaintext in "readable" form to a cipher text "non-readable" to provide the security again different attacks. Thus, to provide a secure service to the network there two wide DES and RSA secret and public key cryptography based algorithms are used. This paper presents the comparison between DES secret key based algorithm and RSA public key based algorithm. There are two main features that specify and differentiate one algorithm from another are the ability to secure and protect the data against attacks and speed of encryption and decryption. This paper presents the performance of three most useful algorithms: DES, 3DES and RSA. Performance of different algorithms is different according to data loads.

Keywords—Encryption, Decryption, Plaintext, Cipher text, RSA, Bits, Triple DES, DES, 2 DES, Blowfish, throughput, RPT, LPT.

INTRODUCTION

Encryption is a process of converting information in"hidden" form. So that it is intelligible only to some one who knows how to decrypt it. For encryption and decryption there are two aspects: algorithm and key used. 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. And if different keys are used for 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, AES, 3DES, IDEA,Blowfish algorithms etc. and public key cryptography includes RSA, Digital Signature and Message Digest algorithms.[3,4]

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 combination of series of the basic algorithm and some block cipher and some feedback from previous steps .

DES—It uses block cipher. It encrypts the data in block size of 64 bits each. Same algorithm and key are used for encryption and decryption. Key is 56 bits long. The position of 8, 16,24,32,40,48,56,64 are discarded. DES is based on two fundamental attributes of cryptography Diffusion (Substitution) and Confusion (Permutation) consisting 16 rounds. In each round key and data bits are shifted, permuted, XORed and sent through, 8 s-box. In the first round 64 bit plaintext is handed to initial permutation(IP).Then IP generates two halves left plaintext(LPT)and right plaintext(RPT).Each LPT and RPT goes through 16 rounds. At the last LPT and RPT are rejoined. Decryption is same process perform rounds in reverse order [1, 3].

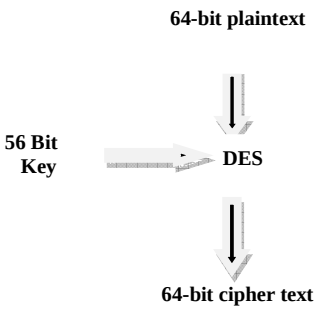

Fig.1 DES Block

Algorithm:-

[1] DES takes an input of 64-bit long plaintext data block and 56-bit key (8 bits of parity) and generates output of 64-bit block.
[2] The plaintext block is subject to an Initial Permutation to shift the bits around.
[3] The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
[4] The plaintext and key are processed in 16 rounds consisting of:
    a. The key is split into two 28-bit halves.

b. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
c. The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed key is used to encrypt this round's plaintext block.
d. The rotated key halves from step 2 are used in next round.
e. The data block is split into two 32-bit halves.
f. One half is subject to an Expansion Permutation to increase its size to 48 bits.
g. Output of step 6 is exclusive-OR'ed with the 48-it compressed key from step 3.
h. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
i. Output of step 8 is subject to a P-box to permute the bits.
j. The output from the P-box is exclusive-OR'ed with other half of the data block.
k. The two data halves are swapped and become the next round's input.

2DES—It performs twice same as DES normally do once. It uses two different key k1 and k2.It firstly performs the DES on the original plain text by k1 key. And then again perform encryption on encrypted text with the other key K2 shown in fig.2.And decryption is shown in fig.3 [2].

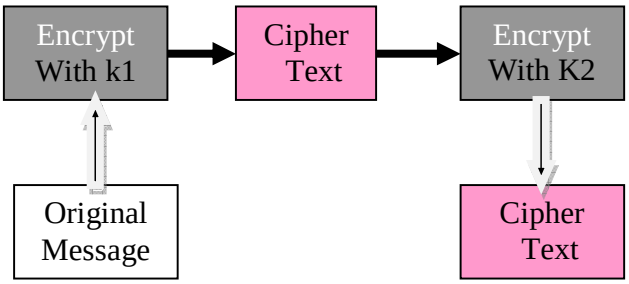

Fig.2. Operation of 2-DES Encryption

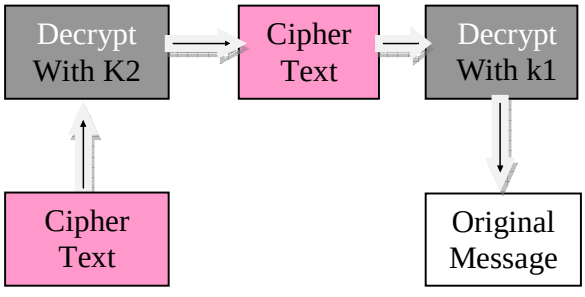

Fig.3. Operation of 2-DES Decryption

3DES— It is enhancement version of DES. And used to remove the meet-in-the-middle attack occurred in 2-DES. In this 3 times iterations of DES encryption on each block is performed as shown in fig.4 & 5. In 3-DES the 3-times iteration is applied to increase the encryption level and average time. Common method of 3-DES is Minus Encrypt-Decrypt-Encrypt (-EDE). Each iteration of 3DES using –EDE will encrypt a block using a 56-bit key shown in fig.4. After encryption, use a different 56-bit key to decrypt the block. On the last pass, a 56-bit key is used to encrypt the data again. This is equivalent to using a 168-bit encryption key method that is Minus Encryption- Encryption – Encryption (-EEE) shown in fig.5.All three keys can be different or identical or first and third key can be same[2].

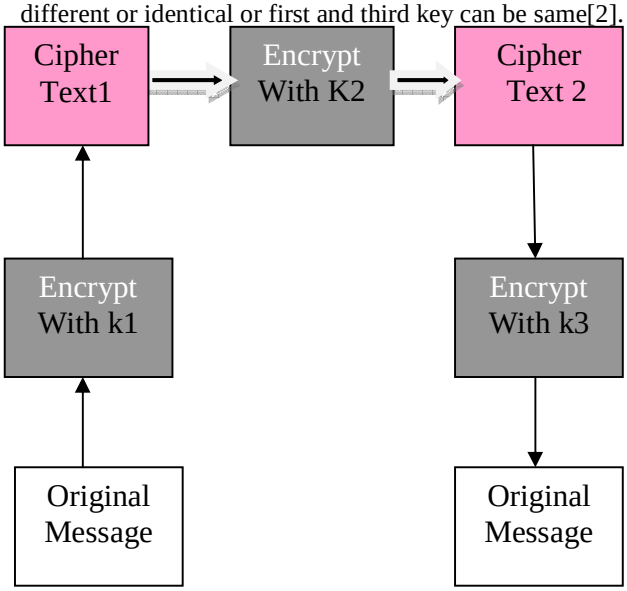

Fig.4. Operation of 3-DES with three keys (-EEE)

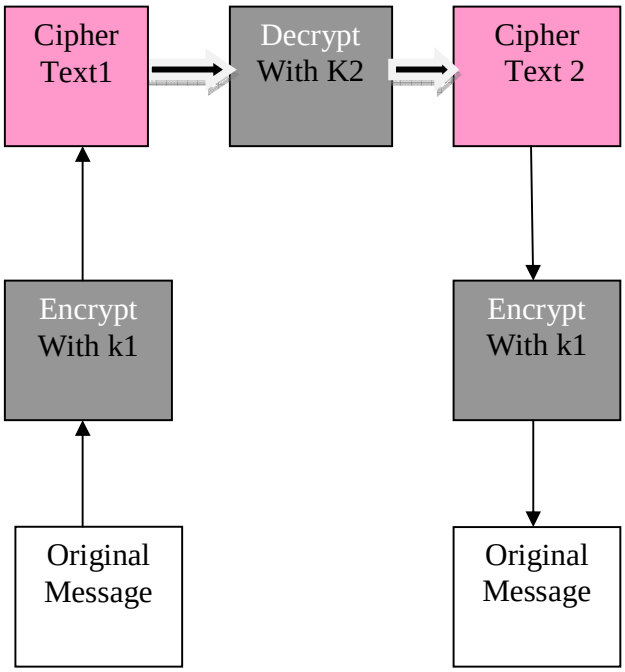

Fig.5. Operation of 3-DES with two keys (-EDE)

Blowfish:-It uses block cipher of 64-bit block. It takes a key of variable length ranging from 32 bits to 448 bits [11]. It was designed with of following objectives.

- High speed-It encryption rate is 26 clock cycles per byte on the 32-bit microprocessor.
- Compactness-It can execute less than 5kb memory.
- Simplicity-It uses only primitive operations like addition, XOR and lookup table for design and simple implementation.
- Secure-As blowfish have a variable length key up to 448 bits long, which make it secure and flexible.

Blowfish encrypts 64-bit blocks with a variable length key. It two main parts:-

1. Sub key Generation: - This process convert the key up to 448 bits long to sub-keys totaling 4168 bits.
2. Data encryption:-It involves the iteration of 16 rounds. Each round contains a key dependent permutation and data dependent substitution.

We have studied a no. of different techniques used for fulfillment of data encryption purpose. So there are some comparisons generated on different important features [6]:

- *Avalanche effect***: -** Small change in plaintext or key will change the cipher text is Known as advance effect. Either change in on bit of plaintext or key will change no. bits of output value.
- *Memory required***:-**Different algorithm required different memory space to perform the operation. The memory space required by any algorithm is determined on the basis of data size, no. of rounds etc.From different algorithm a algorithm is considered best which use small memory and perform best task.
- *Simulation time:* The time required consumed by algorithm to complete the operation is known as simulation time. It depends on processor speed, algorithm complexity. Small simulation time is desirable requirement. [9].
- *Throughput*-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**.**

II. RSA ALGORITHM

This is public key encryption algorithm developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977. It is most popular and asymmetric key cryptographic algorithm. It may used to provide both secrecy and digital signature. It uses the prime no. to generate the public and private key based on mathematical fact and multiplying large numbers together. It uses the block size data in which plaintext and cipher text are integers between 0and n1 for some n values. Size of n is considered 1024bits or 309 decimal digits. In this two different keys are used for encryption and decryption purpose. As sender knows encryption key and receiver knows decryption key [4].

Following steps are followed in RSA to generate the public and private keys [8, 10]:
Choose large prime numbers p and q such that p~=q.
Compute n=p*q
Compute φ (pq) = (p-1)*(q-1)
Choose the public key e such that
gcd (φ (n), e) =1; 1<e< φ (n)
Select the private key d such that
d*e mod φ (n) =1
So in RSA algorithm encryption and decryption are performed as-

Encryption
Calculate cipher text C from plaintext message M such that
C=M ^e mod n
Decryption
M=C^d mod n=M^ed mod n

III.SIMULATION RESULT

As the given figure represents the speed of RSA, Triple DES and DES algorithm to encrypt the data of same length. 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 than power consumption decreased. So, as speed of the DES encryption is twice times to the speed of RSA encryption speed as shown in figure 6.And DES also consumes small power as comparison to RSA power consumption.

Table1: Execution Time (Milliseconds) of Encryption of Different data packet size

Input Size(KB)	3 DES	DES	RSA
45	50	25	55
55	44	29	46
96	76	45	89
236	113	39	119
319	155	89	157
560	171	131	169
899	299	240	309
5345.28	1166	1296	1441
Throughput (MB/Sec.)	2.08	3.01	1.67

Table2: Execution Time (Milliseconds) of Decryption of Different data packet size

Input Size	3 DES	DES	RSA
45	49	34	61
55	47	22	59
96	63	53	57
236	67	62	64
319	85	98	154
560	161	125	163
899	171	152	183
5345.28	835	783	827
Throughput (MB/Sec.)	4.03	5.012	2.147

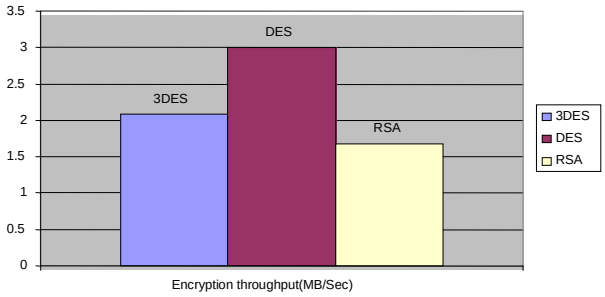

Fig.7 Decryption speed of RSA, 3DES and DES algorithms

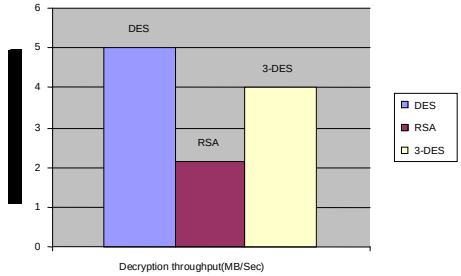

Fig.6 Encryption speed of RSA, 3DES and DES algorithms

IV **COMPARISION**

Comparison of secret key and public key based DES and RSA algorithms is done. RSA solves the problem of the key agreement and key exchange problem generated in secret key cryptography .But it does not solve all the security infrastructure .So DES is used. RSA and DES differ from each other in certain features.

Simulation result implemented in Mat Lab is shown in Fig.7.The given figure is used to represent the decryption throughput of different algorithms are used for data security. Thus we find in decryption that DES is better than all other algorithms in throughput and power consumption. Finally, triple DES still requires more time than DES

Table 3: Distinction between DES and RSA Algorithm's

Features	*DES*	*RSA*
Key Used	Same key is used for encryption and decryption purpose.	Different keys are used for encryption and decryption purpose.
Scalability	It is scalable algorithm due to varying the key size and block size.	No scalability occurs.
Avalanche Effect	No more effected	More effected
Power Consumption	Low	High
Throughput	Very High	Low
Confidentiality	High	Low

V.**CONCLUSIONS**

The selected algorithms DES and RSA are discussed with their working mechanisms. As DES is secret key based algorithm suffers from key distribution and key agreement problems .But RSA consumes large amount of time to perform encryption and decryption operation Simulation result showed that DES has better performance than RSA. From the simulation result, I evaluated that throughput of DES algorithm is much better than the throughput of RSA algorithm. And, I also pragmatic that 3DES has more power consumption and less throughput than the DES due to its triple phase characteristics. It had been also observed that decryption of DES algorithm is better than other algorithms in throughput and less power consumption.

REFERENCES

[1] Ferguson, N.,Schnier, B.and KonhoT.(2010), "Cryptography Engineering: Design principles and Practical applications"

[2] Aman Kumar,Dr.Sudesh Jakhar,Mr. Sunil Maakar"Distinction between Secret key and Public key Cryptography with existing Glitches" IJEIM-0067, vol.1, 2012.

[3] Yogesh Kumar, Rajiv Munjal, "comparison of symmetric and asymmetric cryptography with existing vulnerabilities" IJCMS-Oct.2011.

[4] Atul Kahte"Cryptography and Network Security, 2nd Ed".
[5] Eli Biham and Adli Shamir, "Differential Cryptanalysis of full DES".
[6] Dan Boneh and Glenn Durfee "Cryptanalysis of low exponent RSA"
[7] W. Diffie,M.E Hellman" New Directions in Cryptography".
[8] Piper,F "Encryption". Security and Detection, Ecos 97. European Conference
[9] Schweighofer E (1997) Downloading information Info I & Common Technology.
[10] Himani Agarwal &Manish Sharma" Implementation and analysis of various Cryptography" Dec-2010
[11] Kofahi, N.A., Turki Al-Somani,Khalid Al-Zamil"Performance evaluation of three Encryption/decryption algorithms"
[12] Shasi Mehlrotra seth, Rajan Mishra " Comparative Analysis of Encryption Algorithms For Data Communication", IJCST Vol. 2, Issue 2, June 2011

[13]