COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS

Mohit Marwaha
Beant College of Engineering and Technology, Gurdaspur

Rajeev Kumar Bedi
Sardar Beant Singh State University, Gurdaspur

Amritpal Singh
Chandigarh University

Research Paper

COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS

Mohit Marwaha, Rajeev Bedi, *Amritpal Singh, Tejinder Singh

Address for Correspondence

[1,2,3]Assistant Professor, BCET, Gurdaspur, [4]Assistant Professor, Global Institute of Management, Amritsar

ABSTRACT

Cryptography is the study of Secret (crypto-) writing (-graphy) that is concealing the content of message from all except the sender and the receiver and to authenticate the correctness of message to the recipient. Data security is the challenging issue of today that touches many areas including computers and communication. Recent cyber security attacks have certainly played with the sentiments of the users. Cryptography is one such way to make sure that confidentiality, authentication, integrity, availability and identification of user data can be maintained as well as security and privacy of data can be provided to the user. We have analysed three algorithms DES, Triple DES and RSA. DES and Triple DES is symmetric key cryptographic algorithm and RSA is an asymmetric key cryptographic algorithm, they have been analysed on their ability to secure data, time taken to encrypt data and throughput the algorithm requires. Performance of different algorithms is different according to the inputs

Keywords: Cryptography, Encryption, DES, RSA, Triple DES, Throughput.

INTRODUCTION

Cryptography is a word with Greek origins, means "secret writing". However it is the science and art to transform the messages to make them secure and immune against security attacks. It is the technique to provide secure communication in presence of adversaries to maintain information securities such as data confidentiality, data integrity, authentication, and non-repudiation. The process to convert ordinary information or the plain text into unintelligible text or the cipher text in cryptography is called encryption. The cipher text is understandable only to someone who knows how to decrypt it. The message or information is encrypted using an encryption algorithm. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm which usually requires a secret decryption key. Encryption schemes are divided into two groups:

Symmetric-key

In this scheme same key is used for encryption and decryption it is also known as the secret key encryption

Asymmetric key

In this scheme different keys are used for encryption and decryption it is also known as the public-key encryption.

COMPARISON OF ALGORITHMS

DES

Data Encryption Standard is based on a cipher known as the Feistel block cipher. This was a block cipher developed by the IBM cryptography researcher Horst Feistel in the early 70's. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive OR operations. 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 [6]. DES is based on two fundamental attributes of cryptography Diffusion (Substitution) and Confusion (Permutation) consisting of 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.

Algorithm

[1] DES takes an input of 64-bit long plaintext and 56-bit key (8 bits of parity) and generates output of 64 bit block.

[2] The plaintext block is subject to an 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.

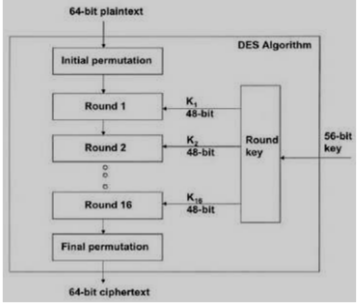

Figure 1: Working of DES algorithm.

Triple DES

As an enhancement of DES, the3DES (Triple DES) encryption standard was proposed. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level [8]. It was used to remove the meet-in-the-middle attack occurred in 2-DES and the brute force attacks in DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES.

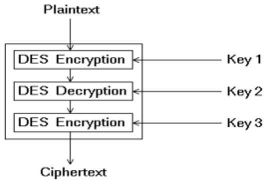

Figure 2: Working of Triple DES algorithm.

RSA

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 [2]. 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.

Algorithm

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

$C=M^e \bmod n$

Decryption

$M=C^d \bmod n=M^{ed} \bmod n$

Comparative analysis of algorithms

We have studied different techniques used for fulfilment of data encryption purpose. There are some comparisons generated on different important features such as:

Input data size- Different algorithm required different memory space to perform the operation. The memory space required by any algorithm is determined on the basis of input data size, number of rounds etc. The algorithm is considered best which use small memory and perform best task.

Time- The time required by algorithm to complete the operation depends on processor speed, algorithm complexity. Less the time algorithm takes to complete its operation better it is.

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.

Theoretical Analysis

The theoretical analysis is as follow:

Features	DES	Triple DES	RSA
Key Used	Same key is used for encryption and decryption purpose.	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.	It is scalable algorithm due to varying the key size and block size.	No scalability
Avalanche Effect	No more effected	No more effected	More effected
Power Consumption	Low	More than DES and Less than RSA	High
Throughput	Very high	High	Low
Confidentiality	High	Very high	Low

Simulation Analysis

We have used Java and ASP.net for simulation. We have taken two parameters time and memory for the simulation setup and calculated throughput by dividing the total plaintext encrypted on total encryption time for each algorithm. We have calculated time taken by each algorithm in milliseconds and calculated memory by subtracting size of original data from encrypted data.

The Tables below represents the speed of RSA, Triple DES and DES algorithm to encrypt the data of same length [1]. Throughput of the encryption algorithms is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm. Thus, if the throughput increased than power consumption decreased. So, as speed of the DES encryption is twice the speed of RSA encryption speed. And DES also consumes small power as comparison to RSA power. Finally, Triple DES still requires more time than DES because DES encrypts the data once and Triple DES encrypts the data three times. Triple DES has more power consumption and fewer throughputs 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. But the aspect the DES and RSA lacks that make Triple DES as our choice of algorithm is security.

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	79	119
319	155	89	157
560	177	131	179
899	299	240	369
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(KB)	3 DES	DES	RSA
45	45	36	55
55	42	31	48
96	65	49	73
236	104	88	105
319	135	89	157
560	160	131	169
899	181	152	173
5345.28	845	785	880
Throughput (MB/Sec.)	**4.03**	**5.012**	**2.147**

CONCLUSION

The advantage of proven reliability and a longer key length that eliminates many of the attacks that can be used to reduce the amount of time it takes to break DES. Confidentiality and scalability provided by Triple DES over RSA and DES is much higher that makes it suitable even though DES consume less power memory and time to encrypt and decrypt the data but on security front DES can be easily broken by brute force technique as compared to Triple DES and RSA making it the least secure algorithm .

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