Analysis of Cryptography Techniques

Prof Shivani Desai, Yamini Rathod
Nirma University, INDIA
shivani.desai@nirmauni.ac.in, 11bce078@nirmauni.ac.in

ABSTRACT

Today, the information is a large source and the security of that information is a major challenge. The generation doesn't care that how many techniques are available for transferring the data but they only care about the security of their information. Everyone wants their information to remain secured. While thinking about the current situation of transferring the data from one computer to another computer, there are several techniques available in the form of symmetric and asymmetric cryptography which provides such algorithms that are DES, RSA, RC4 etc. which provides support for secure communication either in symmetric or asymmetric approach. In this research paper we have introduced the basic functionality of DES and RSA algorithm, the comparison of them in terms of security, efficiency, number of elements, computation time, transmission power, reliability, level of protection, complexity results.[2][3]

Keywords

Encryption, DES Algorithm, RSA Algorithm, Symmetric Key Algorithm, Asymmetric Key Algorithm, Symmetric DES, Asymmetric RSA

1. INTRODUCTION

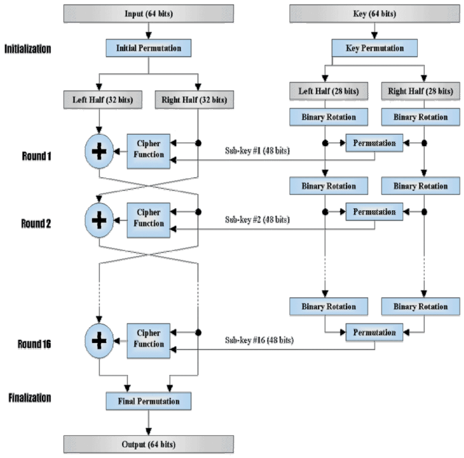
Encryption is the subset of cryptography. The common thing in all the algorithms is to apply encryption at the beginning of the time and to apply description at the ending. There are some common terminologies which required to be understood before coming towards the analysis.

Encryption is the technique which is used to encrypt the information. The process of converting information to secure format from original format. Decryption is the technique which is used to decrypt the information. The process of converting information to original format from secure format. Here the "plain text" is referred as the original text which is to be transferred from source to destination. The encryption technique uses two inputs that are plaintext and the "key". Same way decryption technique uses the same inputs as encryption techniques. The ciphertext is referred as the encrypted information. Cipher is a mathematical function used in encryption and decryption. [1][2][3][4]

2. TWO BASIC TYPES OF CRYPTOGRAPHY

There are two types of cryptography. Symmetric key and Asymmetric key. Symmetric key cryptography uses single key for both encryption and decryption. It's most widely used but the major problem with this approach is the distribution of the key. Nobody else should know except sender and receiver. The well-known symmetric key algorithms are DES, RC2, RC4. Asymmetric key cryptography uses one private key and one public key. The well-known asymmetric key algorithm is RSA. From [1][4]

2.1 Symmetric Key DES



Data Encryption Standard (DES) is symmetric key algorithm. It takes input of 64bits and key of 56bits. Then it will perform initial permutation of input and key permutation of key. Initial permutation of 64bits is divided into left half (32 bits) and right half (32bits), and key permutation of 56bits is divided into left half (28bits) and right half (28bits) with binary rotation. After rotation it combined and performs 56bit permutation.

In round 1, result of 56bits permutation of key and right half of input will be given as input to the cipher function. The cipher function and left half performs addition. In round2, result of round1 and the result of permutation of key will be given to cipher function. And the output of cipher function and right half (32bits) again perform addition. This process will be continued till round 16. In last final output of addition and permutation of key will perform final permutation and gives output of 64 bits. From [2][3][5][6]

2.2 Asymmetric Key RSA

One Key is Private(n,d) and other Key is Public(n,e).
The value of p,q and phi should be kept secret

RSA Algorithm

Two Large Prime Numbers p and q

⇓

n=pq and phi=(p-1)(q-1)

⇓

1<e<phi and gcd(e,phi)=1

⇓

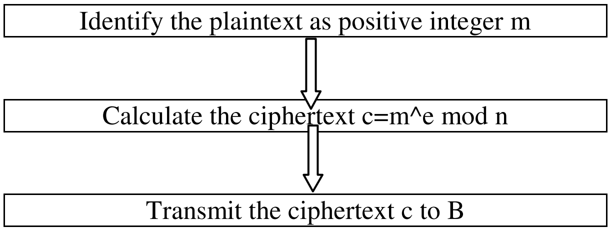
Calculate d,the private key such that de=1 mod phi

Assuming sender as A and receiver as B.

Encryption

Get B's Public Key (n,e)

⇓

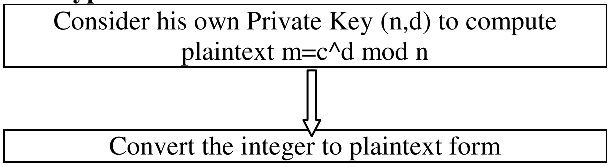


Identify the plaintext as positive integer m

Calculate the ciphertext c=m^e mod n

Transmit the ciphertext c to B

Decryption



Consider his own Private Key (n,d) to compute plaintext m=c^d mod n

Convert the integer to plaintext form

RSA is Asymmetric Key Algorithm where one key is private(n,d) and another key is public(n,e). RSA Algorithm takes input of two large prime numbers p and q. The value of p,q and phi should be kept secret. Then find the value of n=pq and phi=(p-1)(q-1) such that the criteria 1<e<phi and gcd(e,phi) should be satisfied. The last step would be calculating d, the private key such that de=1 mod phi. Here, we are assuming sender A and receiver B. Encryption algorithm takes input of B's public key(n,e) and identify the plaintext as positive integer m. Then calculate ciphertext c=m^e mod n and transmit the ciphertext c to B. Decryption algorithm consider his own private key(n,d) to compute plaintext m=c^d mod n. In the last it will convert the integer to plaintext form. [7][8]

3. COMPARISION OF DES AND RSA

Table 1 shows the comparison between DES and RSA algorithms based on the parameters like execution time, throughput, key used, scalability, avalanche effect, power consumption, security and confidentiality. [5]

Table 1: Comparison Table

Features	DES	RSA
Execution Time	Low	High
Throughput	High	Low
Key Used	Same key is used for encryption and decryption	Different key is used for encryption and decryption
Scalability	It is scalable	Not scalable
Avalanche Effect	No more effected	More effected
Power Consumption	High	Low
Security	High	Low
Confidentiality	High	Low

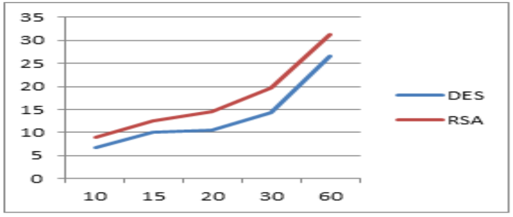
3.1 Comparison in Execution time

Table 2 shows the comparison in execution time with respect to DES and RSA algorithms.

Table 2: Comparison in execution time

Size of File (Bytes)	DES (s)	RSA (s)
10	6.766s	8.997s
15	9.994s	12.504s
20	10.434s	14.566s
30	14.347s	19.601s
60	26.497s	31.353s

Figure 1 shows the graph of the implementation results in which X-axis shows the size of file and Y-axis shows execution time.[5][9]



Throughput is calculated by the ratio of size of file to the execution time.

Throughput = $\sum$(File Size) / $\sum$(Execution Time)

1) DES

Throughput = 135/68.038

= 1.984 bytes/sec

2) RSA

Throughput = 135/87.021

= 1.551 bytes/sec

4. CONCLUSION

This paper describes the different encryption techniques used for security such as Symmetric DES and Asymmetric RSA algorithm. Here we are working on the device in which source and destination are on same device. The execution time of RSA is more than DES algorithm. DES algorithm gives good efficiency, high throughput and performance than RSA. Where throughput is calculated by dividing the plaintext on execution time for each algorithm.[5]

5. REFERENCES

[1] Hector M Lugo-Cordero. Overview of Cryptographic Techniques.CIS 4361 Secure Operating System Administration.

[2] A.V.KRISHNA. Performance evaluation of new encryption algorithms. William Stallings. Cryptography and Network Security,5th edition

[3] Classical Encryption Techniques, CSE 651 Introduction to Network Security

[4] Aman Kumar, Dr. Sudech Jakhar, Mr. Sunil Makka.Comparative Analysis between DES and RSA Algorithms, IJARCSSE Research Paper.

[5] Dr. Jean-Yves Chouinard. Design of Secure Computer Systems CSI1438/CEG4394, Notes on the Data Encryption Standard.

[6] Betty Huang. Analysis of the RSA Encryption Algorithm, Computer System Lab 2009-2010.

[7] M. Preetha and M. Nithya. A Study and Performance Analysis of RSA Algorithm, IJCSMC Research Article.

[8] Sombir Singh, Sunil K Maakar and Dr. Sudesh Kumar. A Performance Analysis of DES and RSA Cryptography, IJETTCS.

[9] Amritpal Singh, Mohit Marwaha, Baljinder Singh, Sandeep Singh. Comparative Study of DES,3DES,AES and RSA, ISSN 22773061.