Paper from Proceeding of the National Conference "Science in Media 2012" Organized by YMCA University of Science and Technology, Faridabad, Haryana (India) December 3rd -4th 2012 Published by
IJMRS's International Journal of Engineering Sciences, ISSN (Online): 2277-9698
www.ijmrs.com

Comparison of symmetric and asymmetric key cryptography: A study

Manish Singh, Shailender Gupta and Bharat Bhushan, YMCA University of Science and Technology, Faridabad

***Abstract*—Cryptography a word with Greek origin means "secret writing". However we use term to refer to the science and art of transforming messages to make them secure and immune to attacks. Two types of approaches are mainly used today symmetric and asymmetric key cryptography. The symmetric key cryptography requires a shared secret key that will be used for encryption and decryption on the other hand asymmetric key cryptography requires public and private keys. The public key is used for encrypting the data while the private key is used for decryption. This paper is an effort to compare both the techniques mentioned above using MATLAB-11 as the simulation tool. The results show that the time complexity of asymmetric key cryptography is quite high but is very much secured.**

Index Terms— **Cryptography, Public key, private key, time complexity**

I. INTRODUCTION

With increase in demand for data communication requirement over the past few decades, the attacks on the internet and internet attached systems have grown more sophisticated. To protect the systems against these attacks various cryptographic mechanisms have been developed. Cryptography [1] is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. Broadly cryptography algorithms can be divided into two categories [2]:-Private Key and Public key cryptography as shown in Fig 1.

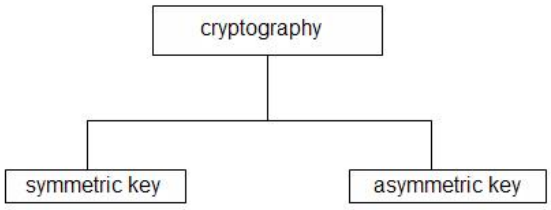

Fig 1 Types of cryptography

In Symmetric key (Private Key) [4] cryptography, same key is used by both the parties. The sender uses this key and an encryption algorithm to encrypt the data and the receiver uses the same key and corresponding decryption algorithm to decrypt the data. The key is shared. The procedure is shown in Fig 2.

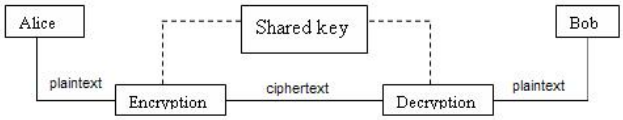

Fig 2 symmetric key cryptography

In asymmetric key (Public key) [3] cryptography, there are two keys: a private and a public key. Private Key is kept by receiver and public key is announced to the public. In Fig. 3, Alice uses the public key to encrypt message. Bob use private key to decrypt the message.

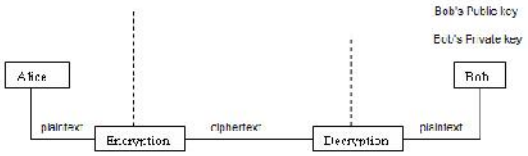

Fig 3 Asymmetric key cryptography

This paper tries to compare the performances of symmetric and asymmetric key cryptography algorithms. For this purpose a simulator was designed in MATLAB and time complexities of the both the mechanisms were calculated.

The rest of the paper is organized as follows: Section 2 provides the literature of the symmetric and asymmetric key cryptography. Section 3 provides the simulation set up parameters. Section 4 provides the result of both the cryptographic techniques followed by conclusion and references.

II. CRYPTOGRAPHIC ALGORITHMS INTO CONSIDERATION

a. RSA Encryption

RSA, named after its inventors Rivest, Shamir, and Adleman. It uses two numbers e and d, as public and private keys [4].

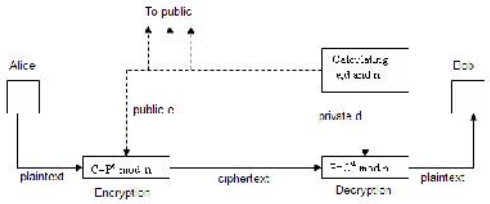

Fig 4 Block diagram of RSA key algorithm

RSA algorithm

1. Select two prime numbers p and q.

*2. Find n=p*q, Where n is the modulus that is made public. The length of n is*

conside

3. Choose a random number 'e' as a public key in the range 0<e<(p-1)(q-1) ..

4. Find private key d such that e x d≡1 (mod (p-1)(q-1)).

Encryption

Consider the device A that needs to send a message to B securely.

5. Let e be B's public key. Since e is public, A has access to e.

6. To encrypt the Plaintext P, represent the message as an integer in the range

0 < M < n.

7. Cipher text C = P^e mod n, where n is the modulus.

Decryption

8. Let C be the cipher text received from A.

9. Calculate Message P = Cd mod n, where d is B's private key and n is the modulus

b. *Data Encryption Standard*

DES was designed by IBM and adopted by U.S. government as the standard encryption method for non-military and non-classified use.

This algorithm [3] encrypts a 64 bit plain text block using a 64 bit key as shown in fig. DES has two transpositions blocks (P blocks) and 16 complex round ciphers. Although 16 iteration round ciphers are conceptually the same, each uses a different key derived from original key.

The initial and final permutations are keyless straight permutations that are the inverse of each other. The permutation takes a 64-bit input and permutes them according to predefined values. DES function applies a 48 bit key to the rightmost32 bits Ri to produce a 32 bit output.

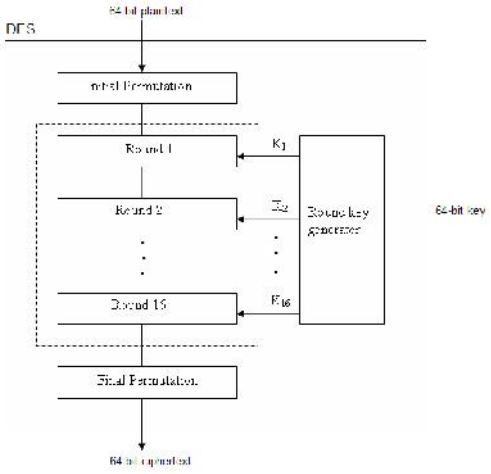

Fig 5 Block diagram of DES algorithm

3. Simulation Set up

a) Simulation Set up parameters

Table1: Set up parameters

Set Up parameters	
Processor	2.4 Ghz, i3 2370 M CPU
RAM	4 Gb
Operating system	64 bit
Key Size	64 bit
Tool used	MATLAB

b) Metrics Used

To measure the efficacy of the cryptographic algorithms, time complexity and brute force search time were calculated. Which are defined as follows:

i. Time Complexity: Defined as the total time taken for the complete encryption and decryption of a particular file.

ii. Brute Force search time: Time taken by cryptanalyst to decrypt the data without knowing the key used.

These parameters are very useful while designing any cryptographic algorithm since any cryptographic algorithm should take minimal time for encryption at the same time should have very high brute force search time.

4. Results

a) Impact on Time complexity :

Fig. 4 shows the impact of varying text size on the time complexity of symmetric and asymmetric key cryptographic mechanism. The following inferences can be drawn

- As the size of text file increases, the time complexity of both the algorithm increases linearly (approximately).
- The time complexity of asymmetric key cryptography is nearly three times compared to symmetric key cryptography.

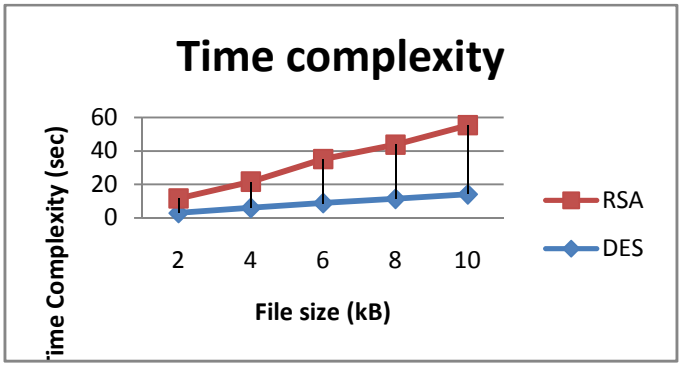

Fig. 4 : Time complexity for RSA and DES

b) Impact on Brute force search time

The brute force search time in both the cases will be same as the key size was taken to be 64 bit.

The average brute force search time for both the algorithms can be calculated as follows:

Table 2: Brute force search time calculation

Key size	Number of alternate keys required	Time required at 10^6 encryption / microsecond
64	2^{64}	$(2^{64} \text{ X } 10^{-12})/2$ Average time taken

Overall Conclusion

From the above results, the following things can be inferred

- The time complexities of asymmetric key cryptographic algorithms is quite high since they involve large mathematical calculations
- The average brute force search time of both the algorithms was same for the same key size.
- The symmetric key algorithms require third party or asymmetric key algorithms for creation of secret key whereas it is not so with asymmetric one.

The above results show that the asymmetric algorithms mechanism makes the process too slow. Hence it is advisable to use these mechanisms for smaller data sizes. They can also be very useful for secret key sharing between two nodes.

REFERENCES

1. Shailender Gupta,Ankur Goyal and Bharat Bhushan, Information Hiding Using Least Significant Bit Steganography and Cryptography" ,I.J.Modern Education and Computer Science, 2012, 6, 27-34.
2. "Cryptography and Network Security: principles and practices", William Stallings, pearsons education, first Indian reprint 2003.
3. R.L.Rivest A.Shamir L.Adleman. Certificateless public key cryptography. pages 120–126. Communications of the ACM 21, 1978.
4. Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth) Author(s): Bruce Schneier.