International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

# Comparison of Time Complexity of Symmetric and Asymmetric Key Cryptographic Algorithms

**Dr. J P Patra[1], Bhumika Joshi[2], Snigdha Chowdhury[2]**
[1]Professor, Department of Computer Science & Engineering SSIPMT, CSVTU, Raipur, Chhattisgarh, India
[2]Computer Science & Engg.SSIPMT, Raipur, Chhattisgarh, India

## ABSTRACT

Information security is the most important as well as the most challenging aspect when considered for internet and network applications. Since internet and network applications are growing very fast so it has become very important to provide necessary protection to the data against the attackers and that too in time. The intruders may use the data being sent for fraudulent purposes. So in order to reduce data loss and pilfering, data privacy requires more attention. Cryptography is one of the popular means of protecting information in order to achieve confidentiality, integrity, authentication, non-repudiation, access control and availability. Cryptography is a main aspect of computer security that converts data from its actual form into an unreadable form. The two main characteristics that identify and differentiate one algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so. The two widely accepted and used categories of cryptographic algorithms to protect information using the desired key are symmetric and asymmetric. Asymmetric algorithms have been analyzed by researchers to be stronger compared to Symmetric algorithms but has higher time complexity. AES belongs to the category of symmetric key cryptography and RSA belongs to the category of asymmetric key cryptography. This paper comprises of brief description of AES and RSA cryptographic algorithms. Also a theoretical as well as a practical performance analysis and comparison of symmetric and asymmetric cryptography has been provided. The comparison is made on the basis of speed, key size and time complexity. A website has been developed using Bootstrap and PHP to execute the codes.

**Keywords:** Cryptography, Symmetric Key, Asymmetric Key, Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA).

## I. INTRODUCTION

The evolution in the area of internet and network application has lead to increase in data transfer due to which data cloning and data re-distribution by the hackers has also increased. So there is a need to protect the information while transmitting it for which cryptography is used. Cryptography is also known as “the study of secret” and protects data from getting decrypted by the third party by using encryption key.

### Principles of Security

Principles of Security help us to understand the attacks in a better way and also help us to think about the possible solutions to control them. The various principles are as shown in figure below.

## A. Principles of Cryptography

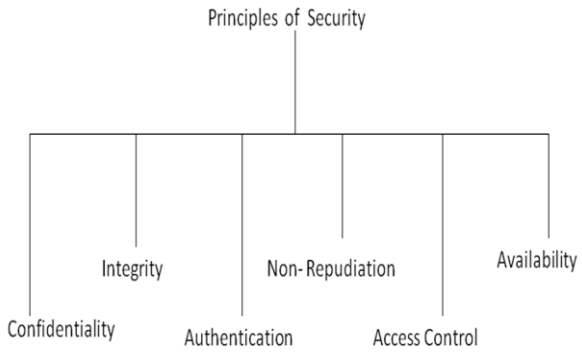



**Figure 1.** Principles of Cryptography

- Non-repudiation: This principle protects against repudiation either by the sender or by the receiver of the data i.e. some situations arise in which the sender sends the message but later refuses that he had sent that message.
- Access Control: This principle protects against unauthorized access to the data i.e. this principle specifies who can access what.
- Confidentiality: This principle specifies that only sender and receiver should be able to access the content of the message. But confidentiality gets compromised when third person which does not have the permission to access is able to access the content of the message.
- Integrity: This principle specifies that changes should be done by authorized entities. But if the content of the message is changed after the sender sends it and before it is received by the receiver then the integrity of the message is lost.
- Authentication: This principle specifies that the origin of the message must be correctly identified.
- Availability: This principle states that the information created or stored in an organization should be available to the authorized party all the times.

### Types of Cryptographic Algorithms based on key

There are many encryption and decryption algorithms that are used for securing the information being sent on a network. They can be classified into Symmetric or Private Key Algorithms and Asymmetric or Public Key Algorithms depending on the type of security keys.

Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization). This template was designed for two affiliations.

*1)* Symmetric Key Algorithms: *In symmetric key encryption and decryption algorithms, only single key is used to encrypt or decrypt the data. Symmetric key algorithm is also known as Secret Key Algorithm. The symmetric (shared) key should be shared between sender and receiver. If the key is not strong, the data may be decrypted by any person. There are many types of symmetric key algorithms such as DES, Triple DES, RC4, AES, Blowfish.*

1. Symmetric Key Cryptography

*2)* Asymmetric Key Algorithms: *Asymmetric key encryption or public key encryption is used to solve the problem of key distribution [1]. In this, two keys are used to encrypt or decrypt the data. The public key is used to encrypt the data whereas the private key is used to decrypt the data. In this, the prior distribution of the keys is not required between the sender and the receiver. These type of algorithms are more efficient in mobile devices. There are many types of asymmetric key algorithms such as RSA, Diffie-Hellman key exchange, Elliptic curve cryptography, Key Serialization.*

2. Asymmetric Key Cryptography

### Description of Advanced Encryption Standard (AES)

In 1990, US Government wanted to standardize a cryptographic algorithm called Advanced Encryption Standard (AES). The need for coming up with a new algorithm was because of the perceived weakness in DES.

The 56-bit keys of DES were no longer considered safe against attacks and the 64-bit blocks were also considered to be weak. AES is based on 128-bit blocks and 128-bit keys.

AES has parallel and symmetric structure.

AES supports adaptation of modern processors like Pentium, RISC and parallel processors.

AES mandates that the plain text block size must be 182-bits & key size must be 128, 192 or 256-bits.

*Versions of AES*

**Two versions of AES used are as follows:**

- ***128-bits plain text block combined with 128-bit key block.***
- ***128-bit plain text block with 256 bit key block.***

*Operation of AES*

Step 1: Expand the 16-byte key to get the actual key block to be used. This process of expanding the key is referred to as Key Expansion. Here 16-byte key is expanded to 176-byte key which is equal to (176/4) words = 44 words.

Step 2: Do one time initialization of the 16-byte plain text block called as state. Here 16-byte plain text block is copied into two dimensional (4 x 4) array called as State.

Step 3: XOR the state with the key block. Now the first 16-bytes of expanded key are XORed state array. Thus every byte in the state array is replaced by XOR of itself and the corresponding byte in the expanded key. As this stage, the initialization is complete & user is ready for rounds.

**Description of Rivest-Shamir-Adleman (RSA)**

The RSA algorithm was developed by Ron Rivest, Adi Shamir and Len Adleman at MIT in 1977. Since that time it has been recognized as the most widely accepted and implemented general purpose approach to public key encryption. It is one of the first public key cryptosystems based on number system and is widely used for secure data transmission. It uses a variable size key and a variable size encryption block. Sender uses public key which is known to all to encrypt the text. However, receiver's private key is used to decrypt the encrypted text. This private key is known only to the receiver. No one else in the network has any knowledge about the key. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power [4].

It uses two prime numbers to generate the public and private keys. The scheme makes use of an expression with exponential.

Some mathematical operations are used in RSA through which one can calculate the encryption key 'e' and decryption key 'd', after that one can easily calculate the cipher text and the plain text respectively.

RSA algorithm does processing in three broad steps: key generation, encryption and decryption.

*Key Generation*

Step 1: Choose two distinct large random prime numbers p and q such that $p \neq q$.

Step 2: Compute $n = P \times Q$.

Step 3: Calculate $\phi = (p-1) \times (q-1)$.

Step 4: Choose the encryption key e such that it is not a factor of $\phi$ and $1<e<\phi$.

Step 5: Choose the decryption key d such that the following condition holds true

$$(d \times e) \bmod \phi = 1.$$

Step 6: The public key is (n, e) and the private key is (n, d).

Step 7: Keep all the values p, q, $\phi$ and d secret.

*Encryption*

Plain Text: PT < n

Cipher Text: $CT = PT^e \bmod n$

*Decryption*

Cipher Text: CT

Plain Text: PT = $CT^d$ mod n

**Working of Project**

The working of the project is illustrated through the following headings.

*About the Software Prototype*

Complexity Comparator is a software built using Bootstrap, PHP and scripting language JavaScript. This software is built mainly to compare the time complexity of symmetric and asymmetric cryptographic algorithms.

The main objective of this software is to find the algorithm which takes lesser time for the given input text. The best algorithm then can be used for encryption or decryption.

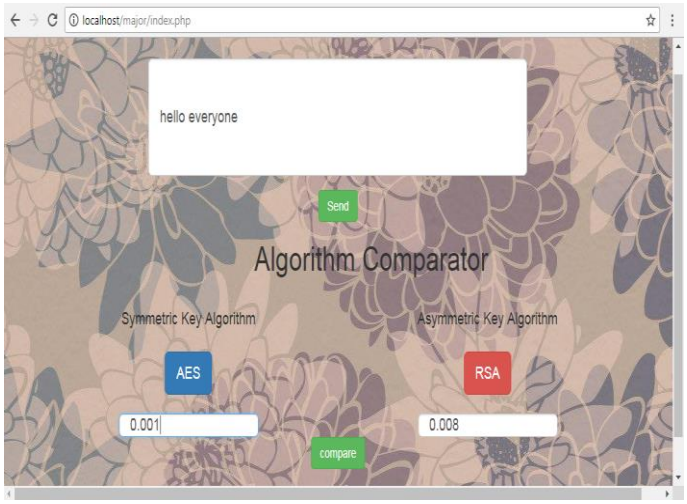
*Need of the Project*

The main aim of the project is to compare the time complexity of symmetric and asymmetric algorithms. When a particular plain text is sent as input then how much time is taken by it to get encrypted is calculated.

*Output of the Project*

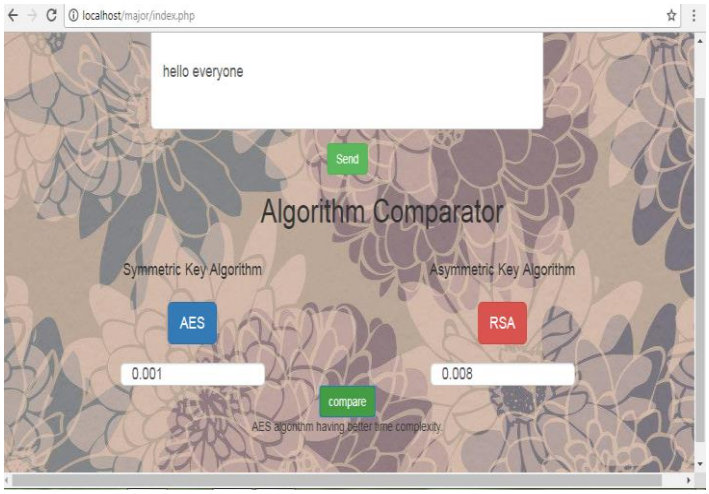
**3) First Snapshot:** ***The snapshot shown below shows the screen of the software. It consists of a Text Box to take input from the user in the form of text. Then as we click the Send button, the entered text goes to the code and produces the output in the Text Boxes of both the algorithms. The output gives the time complexity of the algorithms for encrypting the input text in milliseconds. In this screen only the time complexity of individual algorithms is calculated and comparison is not done.***

For comparing the time complexities of both the algorithms, the Compare button is clicked. The Second Snapshot shows the result after comparing the time complexities.




3. Time Complexity of individual algorithms

**4) Second Snapshot:** ***The snapshot shown below shows the screen of software which shows the comparison of algorithms. After clicking the Compare button a text comes which shows the algorithm having better time complexity. By this the algorithm which takes lesser time to encrypt the input text is known. This tells that which algorithm is better amongst the two and hence will tell that whether symmetric key of asymmetric key cryptographic algorithm is better.***




4. Comparison of algorithms

**Comparison**

The comparison of symmetric and asymmetric algorithms is done on the basis of some parameters. The final conclusion will be based on these parameters. The comparison of AES and RSA is shown in the table below.

1. COMPARISON OF AES AND RSA

| S.No | Comparison | | |
|---|---|---|---|
| | *Parameter* | *AES* | *RSA* |
| 1. | Approach | Symmetric | Asymmetric |
| 2. | Encryption | Fast | Slow |
| 3. | Decryption | Fast | Slow |
| 4. | Key Distribution | Difficult | Easy |
| 5. | Complexity | O(log N) | $O(N^3)$ |
| 6. | Security | Moderate | Highest |
| 7. | Nature | Closed | Open |
| 8. | Secure Services | Confidentiality, integrity, non-repudiation | Confidentiality |

## Conclusion

This paper presents a theoretical as well as a practical performance analysis of symmetric key and asymmetric key cryptographic algorithms. The selected algorithms for the performance analysis purpose are AES and RSA. We have calculated the time complexity of both the algorithms with the help of a software.

It has been developed by using Bootstrap and PHP. The conclusion drawn from our analysis is that symmetric key algorithms are faster in comparison to asymmetric key algorithms when time complexity is considered whereas asymmetric key algorithms are better in comparison to symmetric key algorithms when security is considered. So AES is more suitable when lesser execution time is required while RSA is suitable when greater security is required.

## II. REFERENCES


[1]. Prof. R.M.Sahu, Akshay Godase, Pramod CONTROL ENGINEERING, Vol. 4.

[2]. Kanchan Mahajan, Proff.J.S.Chitode, "Waste Bin Monitoring