Comparing Symmetric and Asymmetric cryptography in message encryption and decryption by using AES and RSA algorithms

Ridwan B. Marqas
Department of Computer science
Duhok Private Technical Institute, Duhok, Kurdistan Region, Iraq
Email- pgmr.red@gmail.com

Saman M. Almufti
Department of Computer science
Nawroz University, Duhok,Kurdistan Region, Iraq
Email- Saman.almofty@nawroz.edu.krd

Rasheed Rebar Ihsan
Department of Computer science
Duhok Private Technical Institute, Duhok, Kurdistan Region, *Iraq*
Email- Rasheed.Sarky@gmail.com

Abstract--One of the common problems of sharing resources over a data communication network is security. Generally sharing information's and resources over a network between a huge number of users is important especially in computer science and engineering field, and this becomes a critical problem for data security. Nowadays many algorithms used for encryption and decryption of data. Cryptography algorithms are divided into symmetric and asymmetric algorithms based on the key used between the sender and receiver of the pieces of information. this paper provides a comparison between symmetric and asymmetric algorithms by using two common algorithms such as AES and RSA. The comparison process focused on the execution time for encrypting and decrypting message of various word length.

Keywords--Asymmetric, RSA, Symmetric, AES, encryption, decryption.

I. INTRODUCTION

Cryptography is focused on the safety and confidentiality of data. It consists of many cryptosystems; those are essentially a group of algorithms that purpose in the protection of information and data. Nowadays, a cryptosystem is applied in different fields such as digital technology, emails, and internet banking…etc. [1]

Generally, Cryptography algorithms are divided into two categories: Symmetric and Asymmetric according to using the key in encryption and decryption. [1]

This paper compared the two widely used cryptography algorithms (RSA for Asymmetric and AES for Symmetric) in encryption and decryption of a message.

II. LITERATURE STUDY

In computer science, Cryptography is techniques for protecting communication between sender and receiver. Cryptography word derives from two Greek words Kryptos which mean "hidden" and Graphein means "writing". Cryptography is the science of hidden writing which is encryption and decryption text and messages. [2]

Cryptography divided into two significant operations: encryption and decryption. The encryption process is the converting of plain text (original message) into ciphertext (hidden message) that can't be read by an authorized user

[1,3]. Whereas the decryption process is retrieving of the original message from the hidden message. [3]

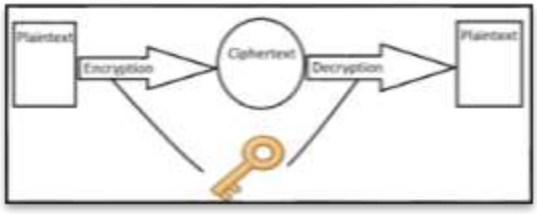

Figure 1: Encryption and Decryption process

Cryptography categories are encryption algorithms specifically symmetric and asymmetric keys. In the encryption and decryption of plain text, symmetric algorithms use only one key. On other hands the public key and private key used in the asymmetric. symmetric key defined as public-key cryptography [2]. The Asymmetric keys utilize pair of keys the first is a hidden key while the second one is a public key. Both keys are different but they are mathematically related. In the cryptosystem, the public key is used for the encoding of plain text (message) whereas the private key is used for decoding the ciphertext (hidden message). [3][4]

Asymmetric key cryptography points to the cryptographic algorithm that needs two different keys: the first of which is hidden whereas the other is public. [4]

The main category of cryptography is showed in Figure2.

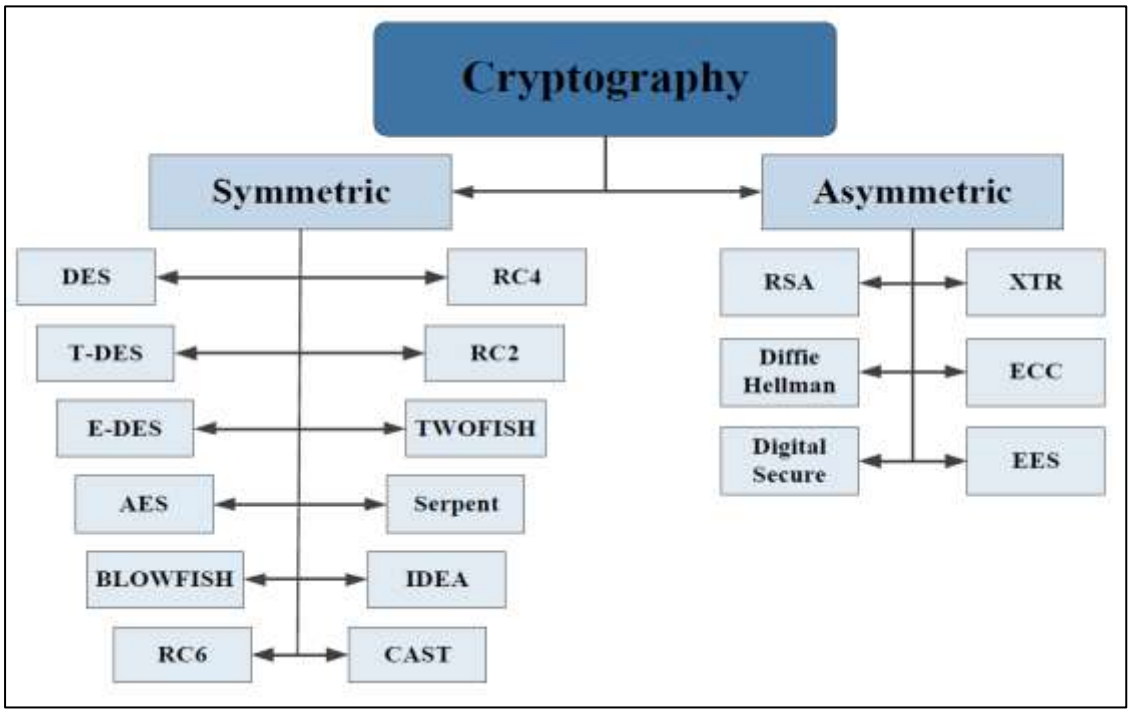

Figure 2: Cryptography Categories [5]

This paper compared the RSA algorithm as a sample for Asymmetric cryptography with AES algorithm as a sample for Symmetric cryptography.

A. RSA

RSA algorithm is Asymmetric cryptography algorithm, named according to inventors (Rivest, Shamir, and Adleman), the headmost algorithm that has the ability to encrypting and decrypting digital signature RSA security relies on the hardness of decomposition of huge numbers. Two different numbers used in an algorithm for creating the public and private key. It leads to the difficulty of estimating the message from single key and the hidden message equals that decomposition of the output of two numbers. [4]

RSA Algorithm:

Stage 1: Begin

Stage 2: Choose two numbers

x = 3 and y = 11

Stage 3: Calculate the value for 'z'

z = x * y = 3 * 11 = 33

Stage 4: Compute the value for φ (z)

φ (z) = (x - 1) * (y -1) = 2 * 10 = 20

Stage 5: Choose e such that 1 < e < φ (z) and e and z.

Let e = 7

Stage 6: Compute a value for d such that (d * e) %? (z) =

1. d = 3

Public key is (e, z) => (7, 33)

Private key is (d, z) => (3, 33)

Stage 7: Stop.

Let T, is plain text (message), T= 2.

Encryption of M is: C = Me % n.

Cipher text is, C = 27 % 33.

C = 29.

Decryption of C is: M = Cd % n.

Plain text (message), M= 293 % 33.

M= 2

The RSA algorithm flowchart is shown in figure 3.

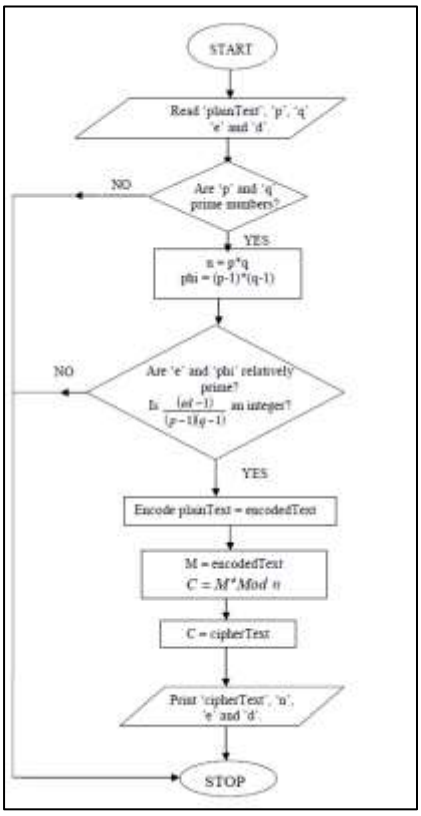

Figure 3: RSA Flowchart

B. AES

Advanced Encryption Standard (AES) algorithm announced by National Institute of Standard and Technology (NIST) in 2001 as a symmetric encryption algorithm. AES can encrypt/decrypt data length of 128 bits (16 bytes) and a key length of 128 bits, 192 bits (24 bytes) and 256 bits (32 bytes) [6]. The 128 bits consist of 10 rounds, 192 bits is 12 rounds and 14 rounds for 256 bits. AES for 128 bits plain text divided into 4 operational blocks array 4x4 of bytes. In the process of encrypting and decrypting message Advanced Encryption Standard uses Substitution-box (S-Box) as HEX values matrix used as lookup table. By computing the multiplicative inverse of Galois field ($GF\ (2^8)$) as shown in equation 1. [7]

$$GF\ (2^8)\ =\ GF\ (2)\ [x]\ /\ (x8\ +\ x4\ +\ x3\ +\ x\ +\ 1) \qquad (1)$$

multiplicative inverse determined by an affine transformation in the form of the vector that is the sum (XOR operation) of multiple rotations of bytes. [7]

The AES in each round includes the following transformations [8]:

- Substitution byte transformation: data block bytes are transformed from block to another by using S-Box, as shown in figure 4 [8].

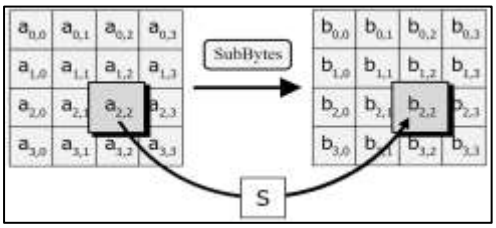

Figure 4. substitution bytes.

- Rows shift transformation: the matrix rows are regularly left-shifted up on their row position (n bytes for n+1 row round left-shifted) as shown in figure 5 [8].

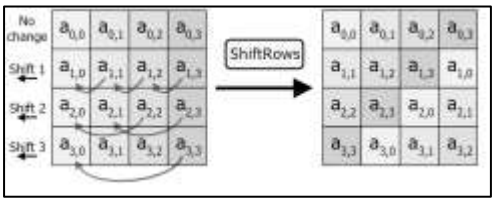

Figure 5. shifted rows.

- Column Mix transformation: Is the matrix-multiplication where each column in the state matrix is multiplied with its corresponding column in a fixed matrix, as shown in figure 6 [7, 8].

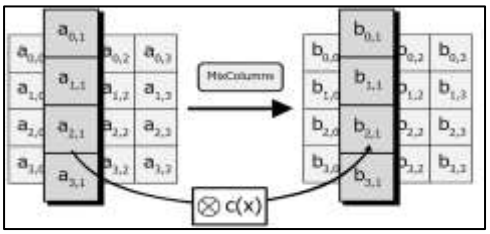

Figure 6. mixed columns.

- Round key adding: It's the XOR process among state and round key matrix, as shown in figure 7 [8,9].

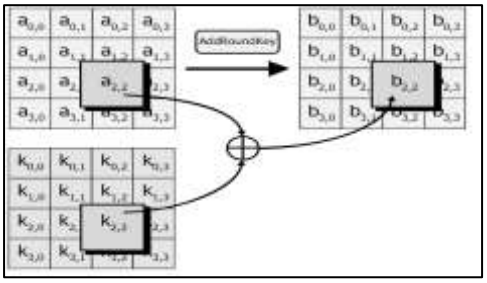

Figure 7. adding round key.

Advanced Encryption Standard (AES) algorithm flowchart is shown in figure 8.

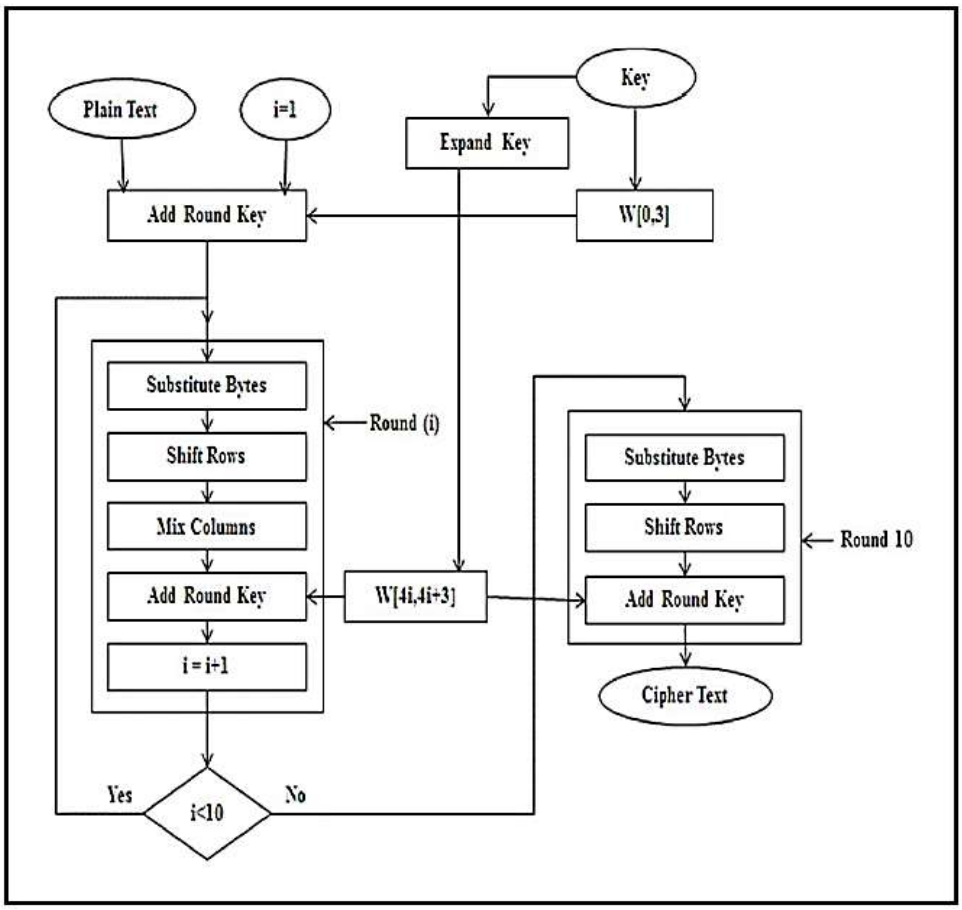

Figure 8. flowchart of AES

III. COMPARISON & RESULT

In this part, the RSA and AES cryptography algorithms are compared with respect to a year, creator, block size, key size, structure, flexibility and features, as shown in table 1.

Table 1. comparison between RSA and AES algorithms.

Items	year	Creator	Block size	Key size (bits)	Structure	Flexible	Features
AES	2001	Joan Daeman & Incent Rijmen	128 bits	128, 192,256	Substitution permutation	Yes	Excellent security. In security and encryption is the best performance
RSA	1978	Rivest Shamir Adlema	128 bits	1024,4096	Public Key Algorithm	No	Security is excellent with low speed

The tested of RSA and AES algorithms up on diverse numbers of words, the tests manner used Intel-R core-tm i-7 4510U CPU 2.60-GHz, x64 based-process, 12 GB of RAM, 64 bit operating-system. The analysis of security tested as according to time of Encryption and Decryption; the time needed to transform plain-text to ciphertext is defined as encryption time of the algorithm. The applied time to execute decryption of the algorithm is defined as decrypt time.

Table 2 and figure 9 shows the difference between RSA and AES in execution encryption time for the message with various words length.

Table 2. time execution encryption of RSA and AES

No. of words	*AES*	*RSA*
100	0.41271	1.8438
200	0.81641	3.5367
400	1.5961	7.0457
800	3.2224	14.1674
1000	4.037	18.5096
2000	8.0976	34.7036
5000	20.282	86.7242

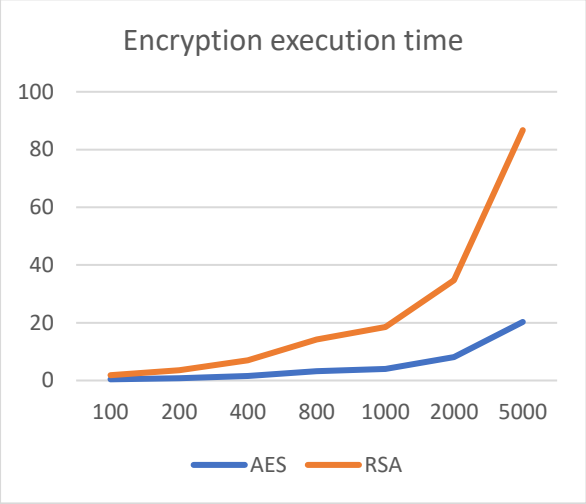

Figure 9. encryption execution time.

Table 3 and figure 10 shows the different between RSA and AES in execution decryption time for message with various words length.

Table 3. decryption execution time of RSA and AES.

No. of words	*AES*	*RSA*
100	0.408306	1.7743
200	1.16398	3.453
400	2.33085	7.1067
800	4.6168	13.8771
1000	5.0771	18.4126
2000	10.3325	33.9662
5000	29.1165	84.3077

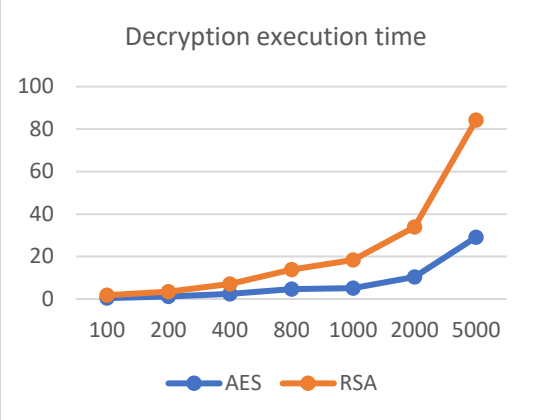

Figure 10. Decryption execution time.

IV. CONCLUSION

This paper computes the execution time consumed for asymmetric encrypting algorithm (RSA) and symmetric encrypting algorithm (AES) cryptography algorithm in encryption and decryption for message of various words length. The experimental result shows that AES has better execution time than RSA in encryption and decryption. The paper also shows that AES has three different key sizes (128,192,256) whereas RSA has only two different key size (1024,4096) in other way the AES is more flexible than RSA and in addition the features of AES shows better performance and faster than RSA.

Over all the result shows that symmetric algorithms (AES) are better than an asymmetric algorithms (RSA).

V. References

[1] R. Asaad, S. Abdulrahman and A. Hani, "Advanced Encryption Standard Enhancement with Output Feedback Block Mode Operation", Academic Journal of Nawroz University, vol. 6, no. 3, pp. 1-10, 2017. Available: 10.25007/ajnu.v6n3a70.

[2] F. Aufa and A. Affandi, "Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm - IEEE Conference Publication", Ieeexplore.ieee.org, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8528584/.

[3] S. Garg, "A Review on RSA Encryption Algorithm", International Journal Of Engineering And Computer Science, 2016. Available: 10.18535/ijecs/v5i7.07.

[4] a. Jain and V. Kapoor, "Secure Communication using RSA Algorithm for Network Environment", International Journal of Computer Applications, vol. 118, no. 7, pp. 6-9, 2015. Available: 10.5120/20755-3153.

[5] O. Abood and S. Guirguis, "A Survey on Cryptography Algorithms", International Journal of Scientific and Research Publications (IJSRP), vol. 8, no. 7, 2018. Available: 10.29322/ijsrp.8.7.2018.p7978.

[6] S. Wadehra, S. Goel and N. Sengar, "AES Algorithm: Encryption and Decryption", International Journal of Trend in Scientific Research and Development, vol. -2, no. -3, pp. 1075-1077, 2018. Available: 10.31142/ijtsrd11221.

[7] M. Albahar, O. Olawumi, K. Haataja and P. Toivanen, "Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption", Journal of Information Security, vol. 09, no. 02, pp. 168-176, 2018. Available: 10.4236/jis.2018.92012.

[8] "Advanced Encryption Standard", En.wikipedia.org, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard. [Accessed: 15- Dec- 2019].

[9] G. Singh and S. Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications, vol. 67, no. 19, pp. 33-38, 2013. Available: 10.5120/11507-7224.