ISSN (Print): 2958-8995
ISSN (Online): 2958-8987

Doi: 10.59799 /APPP6605

Enhancing Hybrid System Based Mixing AES and RSA Cryptography Algorithms

Ali Mahmood Khalaf [1]
Research Scholar
Department of Computer Science
Gujarat University
Ahmadabad, Gujarat, India
alikhalaf@gujaratuniversity.ac.in

Dr. Kamaljit Lakhtaria [2]
Associate Professor
Department of Computer Science
Gujarat University
Ahmadabad, Gujarat, India
kamaljit.lakhtaria@gujaratuniversity.ac.in

Enhancing Hybrid System Based Mixing AES and RSA Cryptography Algorithms

Ali Mahmood Khalaf
Research Scholar
Gujarat University
Department of Rollwala Computer Science
Ahmadabad, Gujarat, India
alikhalaf@gujaratuniversity.ac.in

Dr. Kamaljit Lakhtaria
Associate Professor
Gujarat University
Department of Rollwala Computer Science
Ahmadabad, Gujarat, India
kamaljit.lakhtaria@gujaratuniversity.ac.in

ABSTRACT

Information security is an important matter, especially with the increased demand for information due to the advent of the Internet, as this information has entered many scientific, commercial, and military fields, and this has become widely circulated as the need to protect this information from penetration has arisen by developing techniques to encrypt and preserve information. In this research, a system based on mixing was developed, taking advantage of the strengths of both algorithms, to ensure information protection and more reliability, and to add an additional level of security, where the modified symmetric encryption algorithm, which works with the public key AES, was combined with the modified asymmetric encryption algorithm, which works with the private key, RSA algorithm. In the AES algorithm, there was an increase in speed and a new security prefix by adding Four-S Boxes to the generation key, as well as adding Four-S Boxes to the encryption algorithm to increase the computational complexity of the difficulty of breaking by the attacker. In the RSA algorithm, an additional level of security was added to the modified algorithm by increasing the complexity of (n), which depends on the values of the initial numbers (p, q), in addition to adding other layers of complexity by calculating the value of e. Among the most prominent findings of the study is that hybrid algorithm(AES+RSA), compared with previous studies, has a high level of security, strength, and speed at the time of encryption and decryption, as this hybrid system algorithm was faster than the RSA algorithm and slightly slower than the AES algorithm, as the throughput was high compared to other studies.

Keywords: Cryptography, Cryptography Algorithms, Mixing AES and RSA, Execution Time, Throughput

1. INTRODUCTION

The matter of protecting and preserving information from penetration is a major concern as a result of the increased demand for this information, which is represented by (texts, images, audio files, and video files) that have entered many areas, including wireless networks, and engineering, medical, and military fields, where this information is exchanged through an open environment that is easy to penetrate, as it called on scientists to develop techniques to hide this information, and among these

technologies are cryptography algorithms (Zong & Natgunanathan, 2014)(Abood, 2017).

Cryptography is of Greek origin from two words first, crypto means "hidden secret"; The second is graphein, meaning "covered writing". Encryption is an important science and it is one of the techniques of concealment science. It is an important and necessary technique to protect information from external attacks. Through this technique, the original message is converted into a secret encrypted message between the sender and the receiver using encryption algorithms. There are two types of cryptography algorithms: symmetric key algorithms are also known as the private key cipher system, where this one has one private key for encryption and is itself private for decryption, while the second type of algorithm is known as the asymmetric key cipher system is also known as the public key cipher system, where this type of algorithm has two keys, the first is private for encryption and the second key is private for decryption(Rajkamal & Zoraida,2014)(Bokhari & Shallal,2016)(Timilsina & Gautam,2019), as shown in Figure 1.

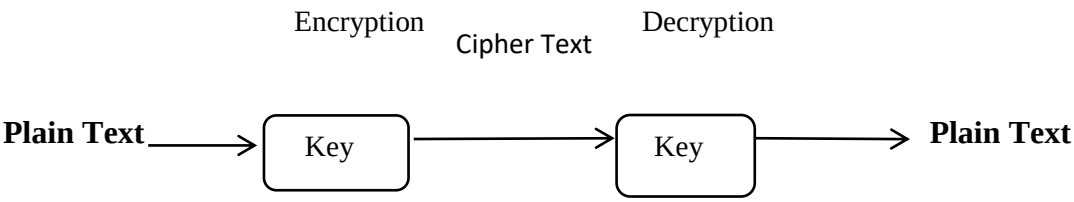

Figure 1: cryptography model

The main term of cryptography can be described as follows (Stallings,2006):

- Plain Text: An original plain message or data, it's nourished into an encryption algorithm.
- Encryption Algorithm: The encryption algorithm converts plain text into ciphertext by using performs various substitutions and transformations.
- Key: The secret value independent of the plain text and encryption algorithm. It's also input into the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the secret key.
- Cipher Text: The ciphertext is a random stream of data, it’s the output incomprehensible of a scrambled message. It depends on the plaintext and secret key.
- Decryption Algorithm: The decryption algorithm run in the opposite. It takes the ciphertext and secret key and produced the plain text(original format),as shown in figure 2.

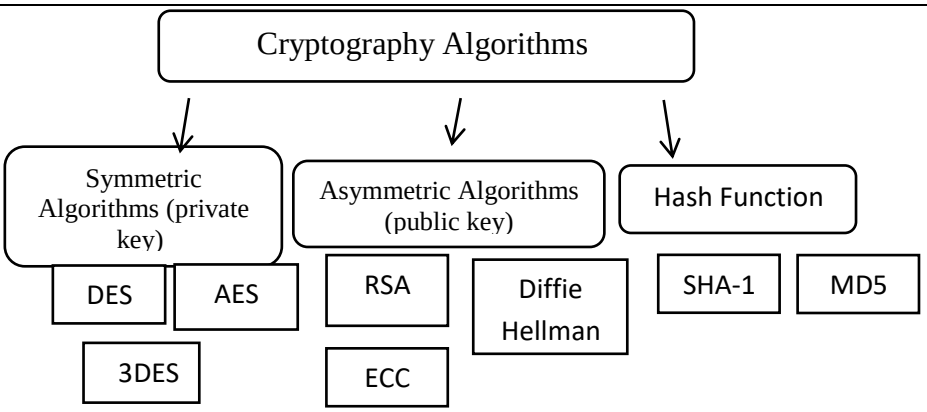

Figure 2: Cryptography Algorithms

2. LITERATURE REVIEW

(Bokhari et al.,2018) "Hybrid Blowfish and RSA Algorithms to Secure Data between Cloud Server and Client." In this paper, a hybrid algorithm is proposed to encrypt and decrypt data during transmission between the server and the client in cloud computing (CCS and CCC). Applying the HMAC feature to the ciphertext that was produced by the fish algorithm, the results of the proposed system were good in comparison with previous literature.

(Abd Zaid &Hassan,2018) "Lightweight RSA Algorithm Using Three Prime Numbers." In this study, a novel strategy is utilized to obtain (n) with the same length as the usual RSA but with fewer bits for prime numbers by using three prime numbers instead of two prime numbers. This method uses three prime numbers and the Chinese Reminder Theory (CRT) to increase speed for both the regular RSA key generation side and the decryption side. Research results indicate that the average speed improvement is 80% in the key generation process, 96% in the decryption process, and only 4% in the encryption process.

(Carlo et al.,2019) “Modified Key Generation in RSA Algorithm”. In this paper, the RSA algorithm is modified based on modulo and public key. , the public key was modified to be a hidden key through the random selection of the collected values and converting it to a different value. From the results of this research, the modification of the RSA algorithm based on modulo and the public key gave a new model consisting of two levels of the encryption process and the decryption process. One of the conclusions of this research is that the new model has the factors to hide the private key.

(Isiaka et al.,2019) “Hybridization of RSA and Blowfish Cryptography Algorithms for Data Security on Cloud Storage”.In this research, a hybrid system is proposed that is able to use the BLOWFISH symmetric encryption algorithm and the other asymmetric RSA, where the algorithms are designed in such a way that one of them authenticates the authorized user and the other provides confidentiality and security

for the data stored on the cloud. One of the most prominent results of this research was a high improvement in data security in cloud storage.

(Ezekiel Bala et al.,2019) “Hybrid Data Encryption and Decryption using RSA and RC4”.In this study, a hybrid system based on two algorithms was designed to add very high security to the public and private keys. The first is private key encryption based on a straightforward symmetric algorithm, and the second is public key encryption based on a linear block cipher. Compared to other encryption algorithms, this one offers a more reliable and secure authentication system. Data is transferred utilizing keys with symmetric encryption to accomplish hybrid encryption. Public key cryptography has been implemented for symmetric random key encryption. Once the symmetric key is retrieved the recipient can use the public key encryption method to decrypt the symmetric key. In comparison to earlier tests, the research's findings indicate a significant improvement in data security and a general improvement in the system's performance. This system was programmed using the C# programming language.

(Alegro et al.,2019) "Hybrid Schnorr, RSA, And AES Cryptosystem.". This study develops a hybrid Schnorr Authentication Algorithm-based authentication algorithm that confirms the identity of the message's sender. When a message is sent from the sender to the receiver and vice versa, algorithms with RSA and AES encryption methods are combined to increase security and lessen the impact of a man-in-the-middle attack on the system. by including further encryption techniques.

(Timilsina et al.,2019) "Performance analysis of hybrid cryptosystem-A technique for better security using blowfish and RSA”.In this research, a hybrid system was created by combining two algorithms, AES and RSA. By combining them with each other, their performance is analysed based on five parameters, which are throughput, encryption time, decryption time, total execution time, and plaintext size to the ratio of ciphertext size with key size. Various for the Blowfish algorithm range from 32-bit-448-bit. As a result of this research, we found that Blowfish RSA with a key size of 448 bits has better performance than all other bit sizes.

(Abd Zaid & Hassan,2019) "Modification advanced encryption standard for design lightweight algorithms.". In this paper, AES-128 encryption has been analysed and made lightweight with respect to power consumption. In the modified AES algorithm, it is proposed to implement the AES mix columns operation and combine the round key addition operation with the mix columns to perform one cycle, and the shift row operation is modified into shift rows and shift columns and the number of rounds is reduced to only 6 rounds for the modified AES. The results of the research were that the modified algorithm excelled and was faster and had a safety ratio of 6 rounds due to the modification in the operations of mix columns and transformation rows higher than the standard algorithm due to its success through the set of statistical tests.

(Gupta &Sanghi,2021) Matrix Modification of RSA Public Key Cryptosystem and its Variant” .In this paper an RSA public key cipher system is proposed using $h \times h$

square matrices. Also, a variant of RSA using the model coefficient $p^r q$ with a matrix with a modified matrix has been proposed.

(Chaloop, & Abdullah,2021) "Enhancing Hybrid Security Approach Using AES And RSA Algorithms." In this study, a hybrid encryption method is introduced to safeguard sensitive data shared between individual users, businesses, organizations, or cloud applications, among other things. During data transmission over the network. Firstly, the algorithm was designed by merging two algorithms, AES and RSA, and secondly, the work of this algorithm was evaluated in comparison with other hybrid algorithms based on its efficiency based on time analysis. In comparison to earlier studies, the experiment findings demonstrated that this hybrid method is more secure.

(Guru & Ambhaikar,2021). "AES and RSA-based Hybrid Algorithms for Message Encryption & Decryption." In order to address security issues, lack of complexity, time, and other issues, a hybrid encryption method that combines the AES and RSA algorithms is developed in this study. According to the research's experimental findings, the hybrid encryption algorithm RSA and AES may not only encrypt files but also improve the technique's efficiency and security.

(Abroshan,2021) "Enhancing Hybrid Security Approach Using AES And RSA Algorithms".In this paper an effective encryption system is proposed to improve security in cloud computing. Improvements have been made to the hybrid algorithm (Blowfish, ECC). In order to improve security and performance, Blowfish will encrypt the data and the elliptical curve technique will encrypt the key. Moreover, digital signature technology is used to ensure data integrity, and the results show improvement in throughput, execution time, and memory consumption parameters.

(Sahin,2023) “Memristive chaotic system-based hybrid image encryption application with AES and RSA algorithms” .In this paper, we propose a two-stage image encryption model, the first stage is the logistic map, chaotic Lorenz system and memristor-based super similar system, and the second stage with AES and RSA encryption algorithms applies the scheme to improve the security of encrypted images. The results of this research show the effectiveness of the proposed image encryption scheme in terms of security, speed, and reliability and provide valuable insights for the development of chaos-based encryption systems in the future. This research was evaluated through statistical tests and compared with previous studies.

1. PRINCIPLES OF ALGORITHMS AND TECHNIQUE

1.1 AES Symmetric Algorithm

It is a symmetric algorithm that was replaced by the DES algorithm in 1991. The AES algorithm supports three key sizes 128,192,256. The AES algorithm is an analog algorithm that uses a single key for encryption and decryption. The AES algorithm gives more security and high confidence in the encryption of information, as AES 10 passes Rounds for the 128-bit key, 12 rounds for the 192-bit key, and 14 rounds for the 256-bit key[Stallings,2006][Chowdhury et al.,2010]. The AES algorithm goes through four stages [Mandal et al.,2012]:-

1- First Stage (Substitute Byte)

In this stage. The AES algorithm contains a 128-bit data block, which means that each data block is 16 bytes, in this type, every byte (8 bits) of one block of data is converted to another block using an (8-bit) square known as Rijndael Sbox.

2- Second Stage (Shift of Rows)

In this stage and depending on the location of the row, the data in the three rows of the case is shifted periodically, a circular left shift of 1 byte is made, and a circular left shift of 2 bytes is performed, for the third and fourth rows.

3- Third Stage (Mix Columns)

In this process polynomial bytes are taken instead of numbers as the fix matrix is multiplied by each of them as polynomial vectors.

4- Fourth Stage (Add Round Key)

In this stage. It is a single XOR between 128 bits of the current state and 128 bits of the round key. Figure 3 shows the steps of AES algorithm.

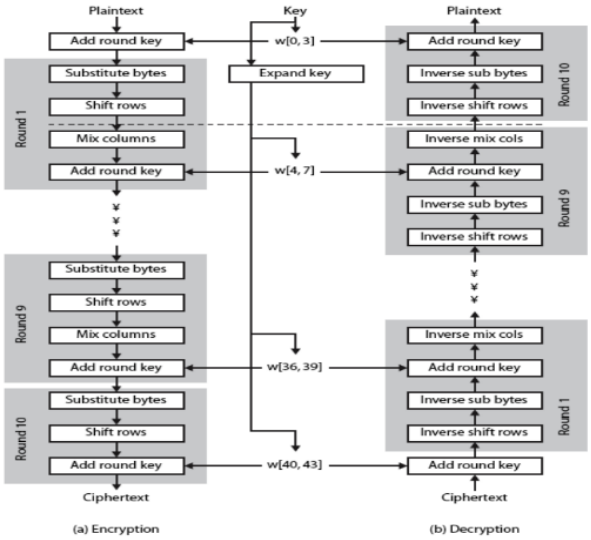

Figure 3: AES Encryption and Decryption Diagram

1.2 RSA Asymmetric Algorithm

This algorithm was published in 1977 by scientists (Rivest-Shamir-Adleman), which is an encryption algorithm used to encrypt information and increase its security, and this type of algorithm is asymmetric as it consists of the public key that is for encryption and the private key that is for decryption, simply the RSA algorithm is slow, and the calculation is RSA is of integer modulo n=p*q, where this algorithm requires a key of at least 1024 bits to increase the security of information encryption, the larger the key size such as 2048, 4096, the more secure the information encryption[Sadkhan & Sattar,2014]. To create public and private keys, follow these steps [Chuang et al.,2016]:

Steps of RSA Asymmetric Algorithm

Step-1: consider two large prime numbers *p* and *q*.

Step-2: compute *n=p*q*

Step-3: compute φ(pq)=(*p*-1)*(*q*-1)
Step-4: select integer *e* such that GCD *(φ(n),e)=1; 1<e< φ(n),* then get public key: KU={e,n}using for encryption.
Step-5: Calculate d=e^{-1}(mod φ(*n*)), then get private key: KR={d,n} using for decryption
Step-6: Calculate cipher text C from plain text M such that (C=M^e mod *n*) for encryption, then calculate plain text M from cipher text (M=C^d mod *n*) for decryption. Figure 4 shows the steps of RSA algorithm.

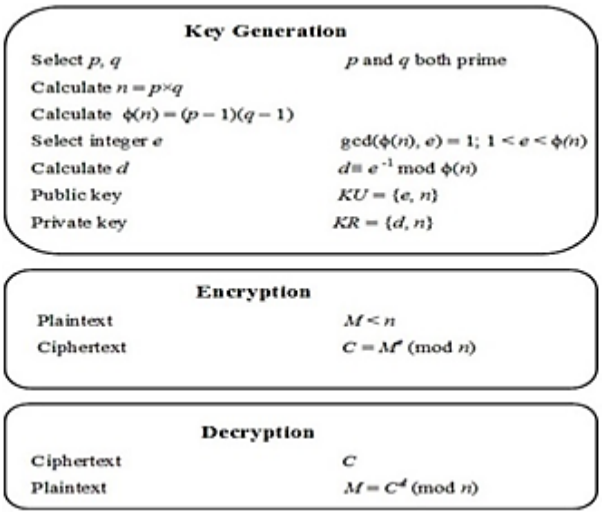

Figure 4: RSA Encryption and Decryption Diagram

3. METHODOLOGY

In this paper, a hybrid system based on three steps was developed. The first step is the encryption and decryption of information using the modified AES algorithm with a symmetric key, the second step is the encryption and decryption of information using the modified RSA algorithm with two keys, and the third step is the combination of the two algorithms to produce A new algorithm takes advantage of the strengths of the two algorithms called mixing AES and RSA cryptography algorithms represented in speed, security and computational complexity. The steps are divided into the following:

3.1 First Step (AES Algorithm Modification)

The first stage of the research methodology is the modification of Advanced Encryption Standard (AES) algorithm with one symmetric key AES with a key size of 128 bits. The purpose of developing the algorithm is to increase the percentage of security and speed and add complexity to the key and encryption to be four times higher than the standard algorithm by adding (Four S- Boxes) to generate the key and (Four S-Boxes) to encrypt the original data so that it is difficult for the attacker to break it and access the original information.

Encryption Process
Inputs: Plaintext data block.

Output: Ciphertext data subblock right.

- Use a latch selector to select the right block of 128 bit from the input data block.
- Store the plaintext in 2d 4x4 state matrix $S_{4\times4}$.
- Select the round key of 128 bit.
- For key expansion, generate the word0 of key$k[0]$ from

$$\boldsymbol{K[n]:w[0] = K[n-1]:w[0] \oplus SubByte(K[n-1]:w[3] \gg 8) \oplus Recon[i]}$$

- Generate the remain words from $\boldsymbol{K[n]:w[i] = K[n-1]:w[i] \oplus k[n]:w[i-1]}$
- Store the round key in 2d 4x4 key matrix $K_{4\times4}$.
- Add round key matrix to the plaintext using xor-function $\acute{S}_{4\times4} = S_{4\times4} \oplus K_{4\times4}$.
- Select two bits, $(Byte\ 3.2)\ mod\ 2$ and $(Byte\ 3.3)\ mod\ 2$ of key matrix $K_{4\times4}$.
- The selected two bits determine one of four sub byte (s-box table).
- Each value of produced state matrix $\acute{S}_{4\times4}$ replaced with the corresponding value in the selected S-box to produce $SB_{4\times4}$.
- Each row in $SB_{4\times4}$ is moved over (shifted) 0,1, 2, or 3 spaces over the right depending on the row to produce $SR_{4\times4}$.
- Product the state matrix $SR_{4\times4}$ by mixing columns matrix $M_{4\times4}$ to produce $CM_{4\times4} = M_{4\times4} \times SR_{4\times4}$.
- Repeat the above steps 10 times from Add round key.
- The ciphertext of 128-bit produced $CM_{4\times4}$

$$k1: \begin{matrix} w[0]: w_{00} & w_{01} & w_{02} & w_{03} \\ w[1]: w_{10} & w_{11} & w_{12} & w_{13} \\ w[2]: w_{20} & w_{21} & w_{22} & w_{23} \\ w[3]: w_{30} & w_{31} & w_{32} & w_{33} \end{matrix}$$

$Where\ w_{ij}\ 2\ hexadecimal\ digits\ for\ word\ w[0]$

Decryption Process

Inputs: Ciphertext data subblock right.

Output: Plaintext data block.

- Product the state matrix $SR_{4\times4}$ by mixing of Inverse Columns Matrix $M_{4\times4}$ to produce $ICM_{4\times4} = M_{4\times4} \times SR_{4\times4}$.
- Each row in $ICM_{4\times4}$ is moved over (shifted) 0,1, 2, or 3 spaces over the left depending on the row to produce $ISR_{4\times4}$.
- Each value of produced state matrix $ISR_{4\times4}$ replaced with the corresponding value in the selected S-box to produce $ISB_{4\times4}$.
- Apply inverse for the selected two bits to determine one of four sub-bytes (s-box table).
- Select two bits, $(Byte\ 3.2)\ mod\ 2$ and $(Byte\ 3.3)\ mod\ 2$ of key matrix $K_{4\times4}$.
- Add inverse round key matrix to the plaintext using xor-function $\acute{S}_{4\times4} = S_{4\times4} \oplus K_{4\times4}$.

- Store the plaintext in 2d 4x4 state matrix $S_{4\times4}$.
- Select the round key of 128 bit.
- For key expansion, generate the word0 of key$k[0]$ from

$$\boldsymbol{K[n]:w[0] = K[n-1]:w[0] \oplus SubByte(K[n-1]:w[3] \gg 8) \oplus Recon[n]}$$

- Generate the remain words w's from $\boldsymbol{K[n]:w[i] = K[n-1]:w[i] \oplus k[n]:w[i-1]}$
- Store the round key in 2d 4x4 key matrix $K_{4\times4}$.
- Repeat the above steps 10 times from Add round key to find deciphered text.

AES Modified Encryption and Decryption, as shown in figure 5.

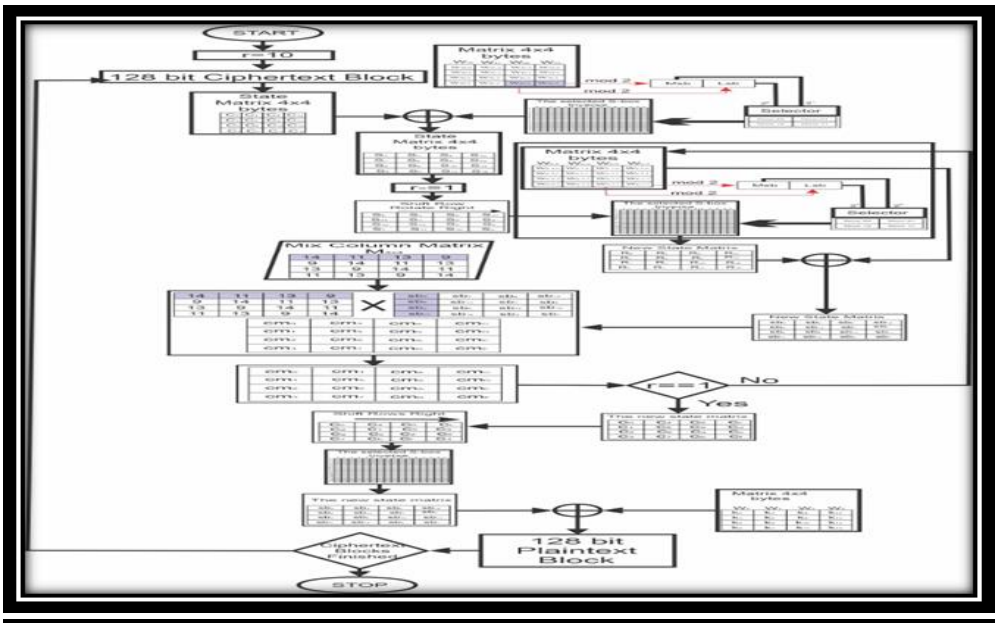

Figure 5: AES Modified Encryption and Decryption

3.2 Second Step (RSA Algorithm Modification)

The second stage of the research methodology is the modification of the standard asymmetric algorithm with two keys. The purpose of developing the algorithm is to increase the security rate and add complications to the clear text by dividing it into a matrix with dimensions (*h*h*) and calculating its determinant, in addition to adding complexity to the key by giving large values to (*p*,*q*) and thus The value of (n, N) increases, in addition to adding other complications to the algorithm, so that it is difficult for the attacker to break it and access the original information.

Encryption Process

- Select p, q, where p, q both prime, p ≠ q.
- Calculate $n = p \times q$.
- Construct $(M)_{h\times h}$ matrix from plaintext block into.
- Calculate determinate $|M|$.
- Calculate $N = p(p^h - 1) \times (q^h - 1)$
- Calculate the Greatest Common Divisor $gcd(|M|, n)$.

- Select integer e where $gcd\ (e,N) = 1;\ 1 < e < N$
- Select integer k, where $0 < k < e;\ \ d|e.$
- Calculate $d = \frac{k \times N+1}{e}$, where: $d \equiv e^{-1}\ mod\ N$
- Select r, where $r \geq 2$.
- Calculate $x = r + 2e$
- Calculate $y = 2n - r$
- Public Key $PU = \{x, y, r\}$
- Private Key $RP = \{d, y, r\}$
- Calculate ciphertext $C = M^{\frac{x-r}{2}}\ mod[\frac{y+r}{2}])$

Decryption Process

- Calculate decipher text $M = C^d\ mod[\frac{y+r}{2}])$

RSA Modification Algorithms Encryption and Decryption, as shown in figure 6.

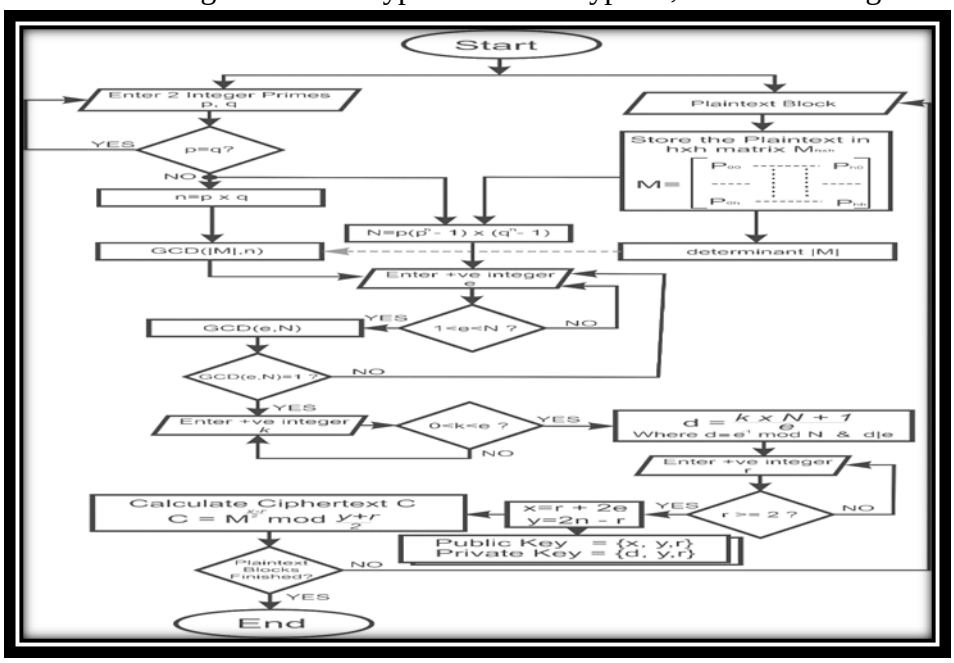

Figure 6 : RSA Modification Algorithms Encryption and Decryption

3.3 Third Step (Mixing AES and RSA Cryptography Algorithms)

In the third step, the files are encrypted and decrypted using the hybrid or combined system by merging the two modified algorithms AES and RSA, where the file is divided into two parts, one part works with the modified AES algorithm with a 128-bit key, and the other part works with the RSA algorithm. . That works with a 128-bit key. Thus, after the encryption process between the two algorithms, the encrypted file is obtained, through the decryption algorithm of this mixing algorithm, the original file is obtained. The primary purpose of mixing two algorithms is to take advantage of the strengths of security, speed, reliability, and throughput of each form of encryption. The second primary purpose, by combining public and private key cryptographic

systems, is to overcome some of the drawbacks of each algorithm. The block diagram of mixing AES and RSA cryptography algorithms, as shown in figure 7.

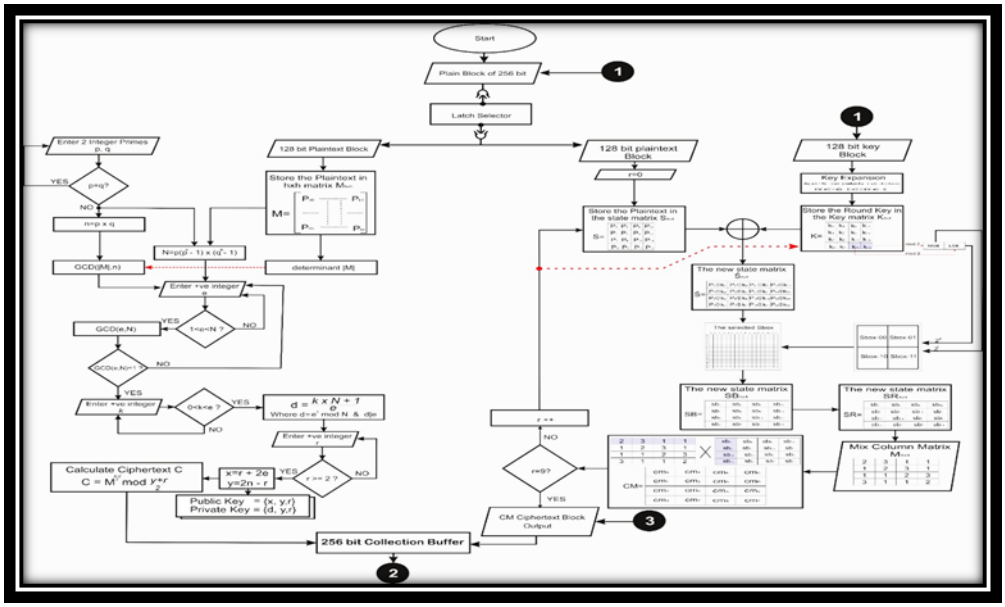

Figure 7: Block Diagram of Mixing AES and RSA Cryptography Algorithms

4 QUANTITATION ANALYSIS

There are many performance measures, used to measure the performance which is used to enhance hybrid system-based AES-RSA Algorithms and the hopping technique, and they are as follows [Isiaka et al.,2019]:

4.1 Time of Encryption: It takes to convert a plain text to a cipher text.

Time of Encryption = recording time after Encryption - recording time before Encryption ….(1)

4.2 Time of Decryption: It takes to convert a cipher text to a plain text.

Time of Decryption = Record time after Decryption – Record time before Decryption …(2)

4.3 Time of Execution: Is the summation the encryption time and the decryption time.

Time of Execution = Encryption Time + Decryption Time…...(3)

4.4 Throughput: Is the rate at which data or file is transferred. It is the size of the file uploaded divided time it takes to recover the file.

Throughput = Total size of the file uploaded /Total Evaluation Time of Algorithm……(4)

4.5 File Size: Is the size of the file uploaded to the server.

5 RESULTS EVALUATION

In this research, two algorithms, AES and RSA, were modified and a third integrated algorithm called Hybrid Algorithm(AES+RSA) was produced. Where these algorithms were evaluated in terms of speed in encryption and decryption time as well as different file sizes for information, as well as calculating the throughput of each algorithm, through the use of the platform Microsoft Visual Studio Community 2022 (64-bit), Version 17.6.5 Visual Basic language to construct the algorithms, under Windows 10 64-bit, The CPU Intel(R) Core(TM) i5-3230M CPU @ 2.60GHz, RAM 8 GB DDR3 and HARD 320 GB are the device specifications used. This paper uses ten files with sizes of different (1.19 MB, 5.384 MB, 11.804 MB, 21.4 MB, 35.350 MB, 42.8 MB, 46.4 MB, 50 MB, 59.809 MB, 106 MB). In this paper calculates the encryption and decryption time for (AES, RSA, and Hybrid System), and compares this study with previous studies. The results in this paper depend on two approaches as shown below.

5.1 Securing Data

In this research, three algorithms were developed and tested on ten files format (.txt, .jpg, .mp3, .mp4, .pdf) of different sizes, where the encryption and decryption time measured (in seconds) were calculated for each of the AES, RSA, Hybrid Algorithms (AES+RSA). The results showed that the hybrid algorithm provides reliability and has a high level of security of the transmitted the data when comparing the algorithms RSA and AES, as shown in table 1 and figure 8.

Table 1: Time for each Algorithm in second

No of File	Plain file size (MB)	Modification Algorithms				Mixing Algorithms	
		AES		RSA		AES+ RSA	
		Encryption Time	Decryption Time	Encryption Time	Decryption Time	Encryption Time	Decryption Time
1.	1.19	0.011	0.028	0.1	0.2	0.01	0.19
2.	5.384	0.09	0.07	0.2	0.9	0.1	0.3
3.	11.804	0.18	0.12	0.25	0.95	0.15	0.45
4.	21.4	0.3	0.33	0.35	1.55	0.25	0.7

5.	35.350	0.55	0.61	0.65	2.85	0.35	0.95
6.	42.8	0.79	0.8	0.83	4.57	0.5	1.1
7.	46.4	0.88	1.01	1.1	5.1	0.75	1.35
8.	50	1.04	1.14	1.25	5.65	0.87	1.43
9.	59.809	1.1	1.19	1.3	6.2	1.02	1.48
10.	106	2.18	1.35	2.38	7.62	1.5	2.1

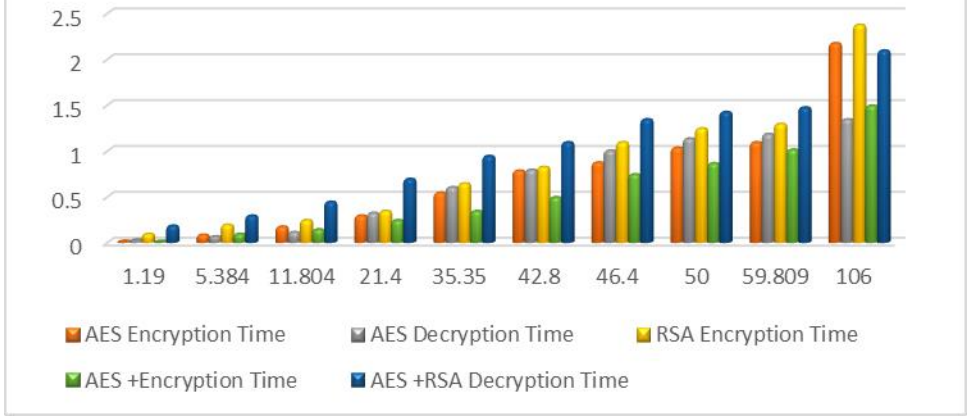

Figure 8:Time in Second for each algorithm

By calculating the total execution time in table 2 of the three algorithms for ten files of different sizes, it is shown in figure 9. Because compared to other algorithms, the hybrid algorithm produces outcomes that are better and has higher levels of information security. And that the speed of the hybrid algorithm in the overall execution is faster much slower than RSA algorithm and much slower than AES algorithm

Table 2: Total Time in Seconds for Each Algorithm

	Plain file size (MB)	**Modification Algorithms**		**Hybrid Algorithms**
No of File		AES Total Time (Second)	RSA Total Time (Second)	AES+ RSA Total Time (Second)
1.	1.19	0.039	0.3	0.2
2.	5.384	0.16	1.1	0.4
3.	11.804	0.3	1.2	0.6
4.	21.4	0.63	1.9	0.95
5.	35.350	1.16	3.5	1.3
6.	42.8	1.59	5.4	1.6
7.	46.4	1.89	6.2	2.1

8.	50	2.18	6.9	2.3
9.	59.809	2.29	7.5	2.5
10.	106	3.53	10	3.6

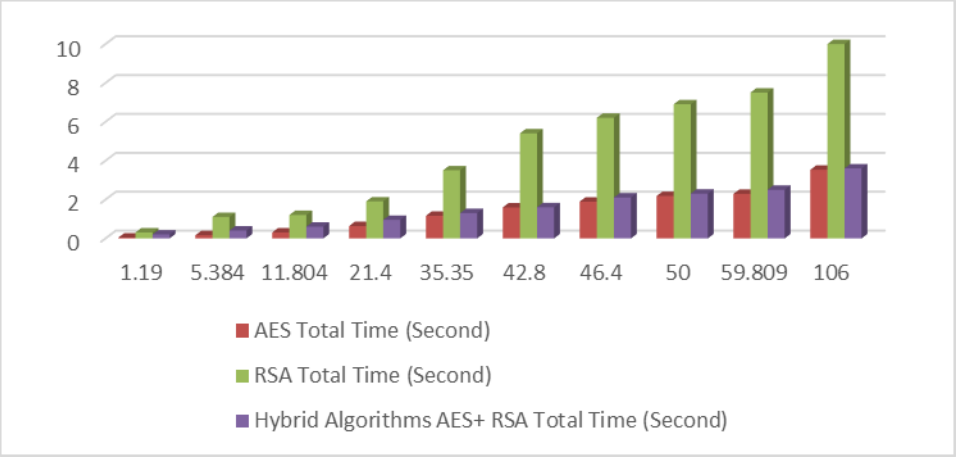

Figure 9: Total Time Execution Time for Three Algorithms

The results in this research showed that the hybrid algorithm in this research was faster 23.31% execution time compared with previous studies (Chaloop, & Abdullah,2021) (Ghaly & Abdullah, 2021) and table 3 shows that.

Table 3: Compare Hybrid Algorithms with Existing Systems

No of File	Plain file size (MB)	Existing Systems (Second)	Hybrid Algorithms AES+RSA (Second)
1.	1.19	0.53	0.2
2.	5.384	0.67	0.4
3.	11.804	0.90	0.6
4.	21.4	1.26	0.95
5.	35.350	1.73	1.3
6.	42.8	2.15	1.6
7.	46.4	2.45	2.1
8.	50	2.78	2.3
9.	59.809	2.95	2.5
10.	106	4.26	3.6

Figure 10 shows the execution time of the hybrid algorithm with execution time for previous studies

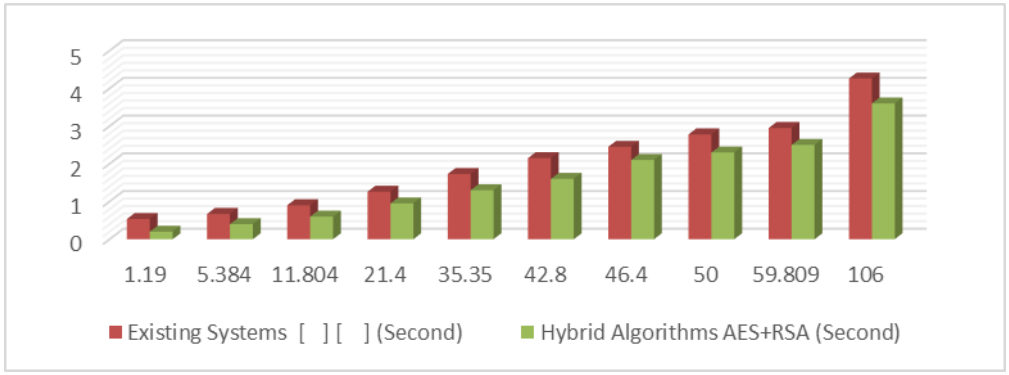

Figure 10: Execution Time for Hybrid Algorithms with Existing Systems

5.1 Throughput

Throughput means the sum of file sizes different divided by the average execution time of the algorithm. The table shows the values of throughput of the three algorithms (MB/second). Analysis of throughput shown in table 4 and figure 11.

Table 4: Throughput values for the algorithms

Total Files Sizes (MB)	RSA Throughput	Hybrid Algorithms Throughput	AES Throughput
380.137	86.395	244.461	276.082

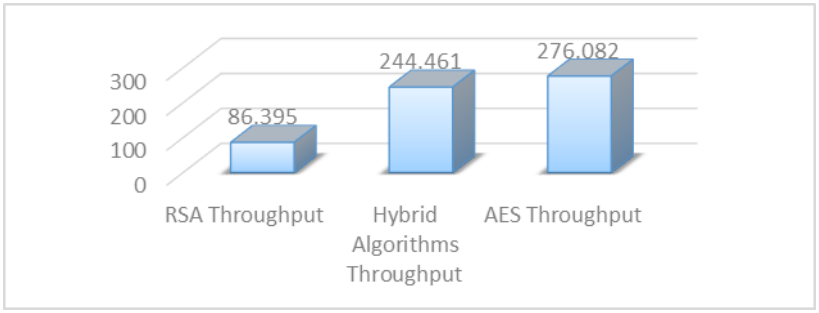

Figure 11: Throughput values for the algorithms

The results of this research , through table 5 showed that the throughput of the hybrid algorithm was higher according to the size of the files and compared with the throughput of previous studies (Chaloop, & Abdullah,2021) (Ghaly & Abdullah, 2021) , and the figure 12 shows the throughput analysis.

Table 5: Values of Throughput of Hybrid Algorithms with Existing System

Total File Size (MB)	Existing System Throughput	Hybrid Algorithms Throughput
380.137	193.110	244.461

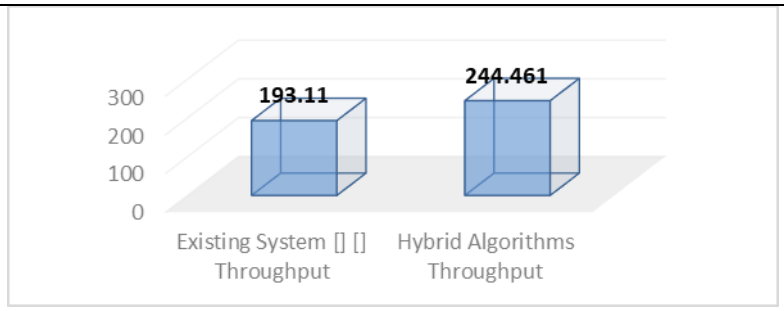

Figure 12: Values of Throughput of Hybrid Algorithms with Existing System

6 Conclusion

In this research, a hybrid system based on the combination of the symmetric and asymmetric encryption algorithm AES-RSA has been improved. Where the purpose of this research was to improve encryption performance, enhance data security, store keys, calculate encryption and decryption time, execution time, and throughput for the standard algorithms and the hybrid algorithm, and compare it with previous studies.

Among the most important findings of this research is that the improved hybrid AES-RSA algorithm is 63.15% faster than RSA Algorithm, and 36.85% slower than the AES algorithm.

References

Abd Zaid, M., and Soukaena Hassan. (2019) .Modification advanced encryption standard for design lightweight algorithms. *J. Kufa Math. Comput.* 6.1: 21-27.

Abd Zaid, Mustafa M., and Soukaena Hassan. (2018) .Lightweight RSA Algorithm Using Three Prime Numbers. *Int. J. of Engineering & Technology* 7.4.36 :293-295.

Abood, M. H. (2017). An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms. 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT). doi:10.1109/ntict.2017.7976154.

Abroshan, Hossein. (2021) .A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms. *International Journal of Advanced Computer Science and Applications* 12.6: 31-37.

Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari (2012). Performance Evaluation of Cryptographic Algorithms: DES and AES. IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5.

Alegro, Jhoanne Kris P., et al. (2019) .Hybrid Schnorr, RSA, And AES Cryptosystem. *Int. J. Sci. Technol. Res* 8.10: 1777-1781.

Bokhari, Mohammad Ubaidullah, and Qahtan Makki Shallal (2016). A review on symmetric key encryption techniques in cryptography. *International Journal of Computer Applications* 147.10.

Bokhari, Mohammad Ubaidullah, Qahtan Makki Shallal, and Md Zeyauddin.(2018). Hybrid Blowfish and RSA Algorithms to Secure Data between Cloud Server and Client.

Carlo A. Intila, Bobby D. Gerardo, Ruji P. Medina. (2019). Modified Key Generation in RSA Algorithm" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878 (Online), Volume-8 Issue-2, July.

Chaloop, Samir G., and Mahmood Z. Abdullah. (2021). Enhancing Hybrid Security Approach Using AES And RSA Algorithms. *Journal of Engineering and Sustainable Development* 25.4 : 58-66.

Ezekiel Bala, Ajibola Aminat, and Ebelogu Christopher. (2019).Hybrid Data Encryption And Decryption Using RSA And RC4. International Journal of Scientific & Engineering Research Volume 10, Issue 10, ISSN 2229-5518, October.

Ghaly, S., & Abdullah, M. Z. (2021). Design and implementation of a secured SDN system based on hybrid encrypted algorithms. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *19*(4), 1118-1125.

Guru, Mr Abhishek, and Asha Ambhaikar.(2021) .AES and RSA-based Hybrid Algorithms for Message Encryption & Decryption. *Information Technology in Industry* 9.1: 273-279.

Isiaka, O. S., et al.(2019). Hybridization of RSA And Blowfish Cryptography Algorithms for Data Security on Cloud Storage.", International Journal of Engineering Technologies and Management Research, ISSN: 2454-1907 DOI: 10.5281/zenodo.3595252, December.

Rajkamal, M., and B. S. E. Zoraida (2014). Image and Text Hiding using RSA & Blowfish Algorithms with Hash-Lsb Technique. *Int. J. Innov. Sci. Eng. Technol* 1.6.

S.C. Gupta and Manju Sanghi.(2021) .Matrix Modification of RSA Public Key Cryptosystem and its Variant. ISSN No. (Print): 0975-8364 ISSN No. (Online): 2249-3255, International Journal on Emerging Technologies 12(1): 76-79.

Sadkhan A. M., Sattar B. (2014). Multidisciplinary Perspectives in Cryptology and Information Security: Advances in Information Security, Privacy, and Ethics", Book, IGI Global, ISBN: 978- 1466658097.

Sahin, M. Emin. (2023). Memristive chaotic system-based hybrid image encryption application with AES and RSA algorithms." *Physica Scripta* 98.7: 075216.

Stallings, William (2006) .Cryptography and Network Security: Principles and Practice. Pearson Education/Prentice Hall, 5th Edition.

Stallings, William (2006). Cryptography and network security, 4/E. Pearson Education India.

Timilsina, Suresh, and Sarmila Gautam. (2019) .Performance analysis of hybrid cryptosystem-A technique for better security using blowfish and RSA. *Journal of Innovation in Engineering Education* 2.1.

Ting-Wei Chuang, Chaur-Chin Chen and Betty Chien (2016). Image Sharing and Recovering based on Chinese Remainder Theorem. Proceedings of International IEEE Symposium on Computer, Consumer and Control, pp. 487- 494.

Zilhaz Jalal Chowdhury, Davar Pishva and G. G. D. Nishantha, (2010). AES and Confidentiality from the Inside Out", the 12th International Conference on Advanced Communication Technology (ICACT), pp. 1587-1591.

Zong, T., Xiang, Y., &Natgunanathan, I. (2014). Histogram shape-based robust image watermarking method. 2014 IEEE International Conference on Communications (ICC). doi:10.1109/icc.2014.6883430.