Advances in Science, Technology and Engineering Systems Journal Vol. 9, No. 3, 84-91 (2024)

www.astesj.com

Special Issue on Computing, Engineering and Multidisciplinary Sciences

ASTESJ

ISSN: 2415-6698

Automated Performance analysis E-services by AES-Based Hybrid Cryptosystems with RSA, ElGamal, and ECC

Rebwar Khalid Muhammed[1], Kamaran Hama Ali Faraj[2,3], Jaza Faiq Gul-Mohammed[4], Tara Nawzad Ahmad Al Attar[2], Shaida Jumaah Saydah[5], Dlsoz Abdalkarim Rashid[2]

[1]*Computer Science Institute, Sulaimani Polytechnic University, Sulaimani, Kurdistan Region, Iraq*

[2]*Department of Computer Science, University of Sulaimani, Sulaimani, Kurdistan Region, Iraq*

[3]*Department of Computer, Collage of Engineering and Computer Science, Lebanse Frence University, Erbil, Iraq*

[4]*Department of Computer Engineering University of Sulaimani, Sulaimani, Kurdistan Region, Iraq*

[5]*Ministry of education, Kirkuk Education Department of Kurdish Studies, Hawazen Preparatory School for Girls, Kirkuk, Iraq*

ARTICLE INFO

Article history:
Received: 24 February, 2024
Revised: 17 May, 2024
Accepted: 18 May, 2024
Online: 22 June, 2024

Keywords:
Hybrid AES-RSA
Hybrid AES-ECC
Hybrid AES- ElGamal

ABSTRACT

Recently Network safety has become an important or hot topic in the security society (i.e., Encryption and Decryption) developed as a solution of problem that have an important role in the security of information systems (IS). So protected/secure the shared data and information by many methods that require in all internet faciality, data health and the cloud computing that suggestively increased our data every in milliseconds unit. This performance analysis by two factors namely Encryption, Decryption and throughput time of three Hybrid Encryption schemes namely; Hybrid AES-RSA, Hybrid AES-ECC, and Hybrid AES-ElGamal which are based on Encryption and Decryption times by milliseconds unit in the form of throughput. The results evaluation shows clear distinctions schemes capabilities such as; Encryption and Decryption as well as throughput time consume. Nevertheless, the Hybrid AES-RSA emerges as the fastest types. Both encryption and decryption outcome with superior throughput. Hybrid AES-ECC and Hybrid AES-ElGamal results are slower processing times and making them more suitable for scenarios where performance is not the primary concern. The choice between these schemes should consider not only performance but also security requirements and specific application required for testing and realize to select Hybrid AES-RSA due to better performance in milliseconds. The programing language for proposed system is JAVA, this mean that all testing is by JAVA and discover that the Hybrid AES-RSA is better in performance. The security proposed is Hybrid AES-RSA for automated recruitment system is best.

1. Introduction

The rapidly growth of information networking technology (ICT) is main principals for common culture interchanging of the data very considerably. Since the huge amount of data transferred over the communication facility, data security modified the issue. The security requires in order to guard such data which communicates on unsecure channel [1]. The modification that occurred from past until now is create a generation in the security and changed to automated security [2] or online security. Attributable to the development of ICT to necessity reputation of data has directed to the mentioned secure data in several methods. The Insecure information as considered one of the difficulties at the present time with the development of ICT and the use of Internet networks through data correspondence between various sides such as organizations and users. The term security of information refers to a methodology that employed to satisfy the security requirements [3]. The Encryption method is one of the targets that make users to ensure the secrecy and access of the data to the receiving from side without affecting it from any third party. Also, the algorithms of Cryptography prevent third party or public reading of private messages [4]. The working of Encryption and

* Corresponding Author: Rebwar khalid, Sulaimani Polytechnic University, rebwar.khalid@spu.edu.iq

decryption is shown in Figure 1 [5]. The Figure 1 states that users Encrypts the message using secret key and send it through the communication channels. The Decrypt by Receiver the message using the secret key but Cryptography offers a number of security target to ensure the privacy of data with non-modification of data and so on. the great security advantages of Cryptography that widely in nowadays security [6].

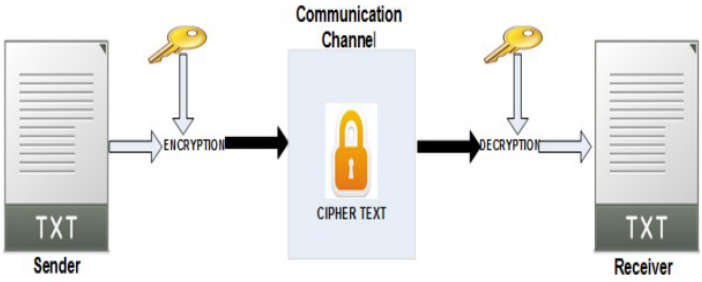

Figure 1: Working of Encryption and Decryption [1]

Cryptography algorithms can be intitled two important categories: Symmetric key Cryptography and Asymmetric key cryptography [7]. Figure 2 shows three types of Cryptography.

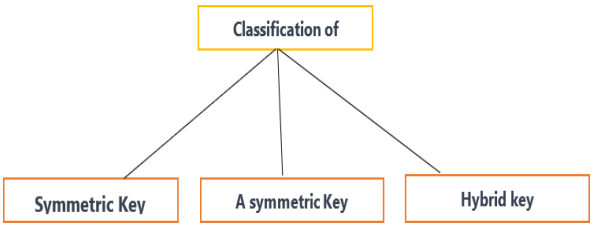

Figure 2: Shows three types of Cryptography [8]

2. Classification of Cryptography

2.1. Symmetric Key Cryptography

Symmetric algorithm is also called shared key Cryptography. During data transmission, the sender and the receiver share the same key for Encryption and Decryption [5]. The different types of Symmetric algorithms as same as to Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES) and Blowfish [8]. Hence, AES is a type of symmetric key cryptography and very powerful and more reliable than the other.

2.2. Asymmetric Key Cryptography

Public key Cryptography is another name for the Asymmetric Algorithm with two keys element that namely 'Private key' and 'Public key'. While the data transmission the users encrypts the clear text with the help of public key known as the cipher text and the receiver Decrypts this cipher text with the help of its private key [8]. The different types of asymmetric algorithms are Rivest Shamir Adlemen (RSA), Diffie Hellman (DH) and Digital Signature Algorithm (DSA), ECC [8].

2.3. Hybrid Cryptography

The concept which combines the both shared key cryptography and public key Cryptographic techniques create new version of algorithms and mentioned as Hybrid Cryptography. A Hybrid Cryptosystem is a protocol using Symmetric and Asymmetric Cryptographic technics together, each to its best advantage. Hybrid Encryption is considered a highly secure type of encryption as long as the public and private keys are fully secure. Hybrid Cryptography is achieved through data transfer using unique session keys along with Symmetrical Encryption. public key Encryption is implemented for random Symmetric key Encryption. The recipient then uses the public key Encryption method to Decrypt the Symmetric key. Once the Symmetric key is recovered, it is then used to Decrypt the message [9]. The blended OR combined in between Symmetric and Asymmetric Cryptographic techniques and create Hybrid Cryptography with three key. However, the three key Hybrid must be more secure than the two key Asymmetric and one key Symmetric. The Table 1 below show the comparison between three different algorithms in respect of key type namely; Symmetric Cryptography, Asymmetric Cryptography and Hybrid Cryptography.

Table1: Shows the comparison between three different algorithms

Aspect	**Symmetric Cryptography**	**Asymmetric Cryptography**	**Hybrid Cryptography**
Key Type	Uses a single shared key	Uses a key pair (public and private keys)	Uses both shared and key pairs
Key Distribution	Securely sharing a single key can be challenging	Public keys can be freely distributed, private keys must be kept secret	Securely share a symmetric key, then use asymmetric encryption for key distribution
Speed	Generally, faster for encryption/decryption	Slower compared to symmetric encryption	Slower than symmetric but faster than pure asymmetric
Security	Vulnerable if the key is compromised	More secure due to the key pair, but still vulnerable if private key is compromised	Combines the strengths of both symmetric and asymmetric encryption for improved security

3. Related Work

In [7], a comparative theory of techniques Encryption in terms of (Symmetric and Asymmetric) keys to algorithms analyzed. In the Symmetric key Encryption (AES) algorithm is found to be better in terms of cost, security and implementation.

Nevertheless, the Asymmetric key Encryption (RSA) algorithm is much better in terms of speed and security. Nevertheless, in paper [7] show and discover that the two algorithms namely AES and RSA are good individually in term of the security and cost but didn't mention Hybrid techniques OR combined technique simultaneously. The AES with RSE are combined in our proposed system and came out with better results than before Paper [10] by Verma, P. Guha, and S. Mishra that comparative study of different key algorithms namely: AES, DES, 3DES, Blowfish and RSA are analyzed and compared with the results that found among the symmetric encryption algorithm, AES and Blowfish are the most secure and efficient algorithms. The performance and energy consumption of these algorithms are better compared to the others. In case of Asymmetric Encryption algorithm, RSA is secure and can be used for application in wireless network because of its good speed and security. However, in paper [10] show and compare between: AES, DES, 3DES, Blowfish and RSA algorithms individually but didn't mention Hybrid techniques OR combined technique simultaneously working between mentioned techniques. The AES, DES, 3DES, Blowfish and RSA algorithms are NOT combined and results came out individually.

In paper [11], ECC is explained in detail. Elliptic curve Cryptography (ECC) is a relatively newer form of public key Cryptography that provides more security per bit than other forms of Cryptography still being used today .

In paper [12], Encryption and Decryption of text using ECC is explained with mapping technique. It is concluded that ECC has low power consumption, less memory requirement, small key size and high security.

In paper [13], Hybrid Cryptography technique using AES and ECC is proposed. The system is intended to provide security to a variety of multimedia data ranging from text documents, images, audio, video. Proposed Hybrid system capable of Encrypting and Decrypting the sensitive data to protect it from unauthorized access and attacks.

In paper [14], Hybrid Cryptography approach implemented using AES and ECC. This system provides encryption to the multimedia data such as text, image, audio, video which resulted in an output with 100 percent accuracy without any loss of information.

In paper [15], Different text files are taken as input and encrypted using AES-ECC Hybrid approach. Analysis of AES Encryption with ECC is done on the basis of different parameters like storage requirement, Encryption time, Decryption time.

In paper [16], Hybrid approach for Encryption technique is implemented over a binary image, which provides more accuracy to the encryption process. The ECC and AES are combined in such a way that differentiates them from the usual manner of Encryption. These days with the increasing trend of security it becomes essential to protect the data and information in a better way.

4. Problem Definition

Cryptographic techniques provides the secure data transmission in automated performance analysis of E-services by AES-Based Hybrid Cryptosystems with RSA, ElGamal, and ECC which be a target for our proposed system. The complications existing systems such as a Cryptographic technique with time consume processes. Nevertheless, exactly techniques that isn't includes the reliability checks on transmitted data and another issue in key changing the presence of security. Thus, the implement an operational Cryptographic algorithm in all phases must be well thought-out to sort a strong method (i.e. AES-Based Hybrid Cryptosystems with RSA, ElGamal, and ECC) with complications in to the proposed method. The proposed Hybrid Cryptographic technique which uses the best features of Symmetric AES-Based Hybrid Cryptosystems with RSA, ElGamal, and ECC. The designed technique helps to reduce the time complexity in Encryption-time, Decryption-time and Throughput-time. This paper solves the performance in time consume also select fewer time response by throughput-time. Finally, our proposed algorithms AES-Based Hybrid Cryptosystems with RSA.

5. Description of Algorithms

Advanced Encryption Standard (AES), Rivest Shamir Adleman (RSA), Elliptic Curve Cryptography (ECC), and ElGamal are indeed powerful cryptographic procedures and use for different purposes and have different features. The AES is a Symmetric-key algorithm widely used for secure facts encryption while RSA operates as an Asymmetric-key algorithm for secure communication and digital signatures. ECC, another asymmetric-key algorithm, relies on elliptic curves for enhanced security with shorter key lengths. ElGamal, also asymmetric are utilized for public-key Encryption and digital signatures based on the discrete logarithm problem. In below explain in detail about all types of Algorithms.

5.1. Advanced Encryption Standard (AES)

The AES algorithm are operating as a Symmetric block cipher system that employs a replace or exchange network. The data block length and key length in AES can be adjusted based on specific requirements, with key lengths available in 128, 192, and 256 bits. The iteration cycle numbers for these round keys are 10, 12, and 14 rounds, respectively. The AES algorithm primarily comprises three components: round change, turns, and key expansion. Each round transformation consists of a non-linear layer, a linear mixture layer, and an add round key layer. The

Encryption process of AES is illustrated in Figure 3. Also, there are three different key lengths with round key iteration.

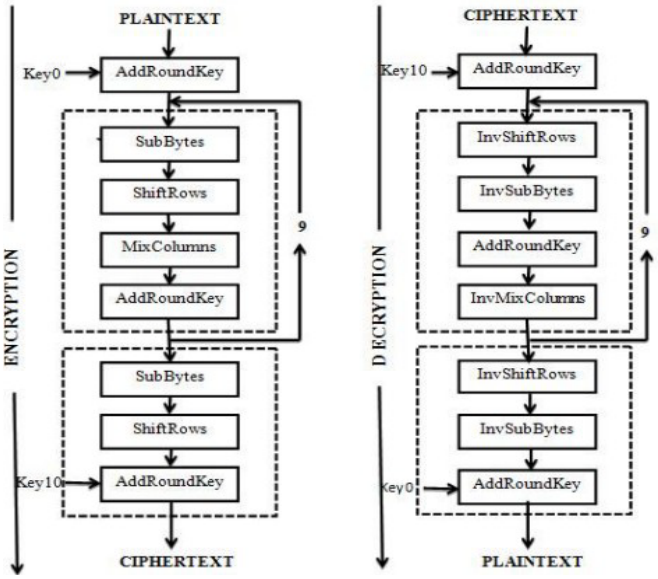

Figure 3: AES Encryption & Decryption process [17]

5.2. *Elliptic Curve Cryptography (ECC)*

In order to compare the public key cryptography that is comparatively more established by an elliptic curve cryptography (ECC) because offers more security per bit than other Cryptographic methods that are still in use nowadays technologies. Nevertheless the Mathematically an elliptic curves are cubic curves that are equivalent to tori topologically. Despite their name which is not closely related to the ellipse. The name of elliptic is integral. By Weierstrass normal equation form. The basic general elliptic curve used for cryptography is of the equation form

$$y2 = x3 + ax + b \quad (1)$$

which showed in Figure 4. The Curves of this form are defined by different values for a and b and modifying these values to visualize of the curve and expand, contract, or pinch off to be two separate pieces. Practically the Curves used for Cryptography to defined very large integer values for aa and bb respectively. The modification of a and b in the mentioned equation is modify the elliptic curve visualization. This mean that is a direct relation between a and b values and elliptic curve.

5.3. *RSA Algorithm*

The invented of the most widely Asymmetric key cryptosystem known as RSA algorithm is very powerful and user-friendly algorithms that Encryption and authentication Cryptosystem used since that time in many Cryptographic applications for instance an e-mail security, banking, e-commerce and digital signature over web operating systems over the internet facility.

The main security algorithm depends on the difficulty of finding prime numbers factor of large integers. RSA operation consists of three main stages key generation, Encryption and Decryption processes which are explained briefly in following [18].

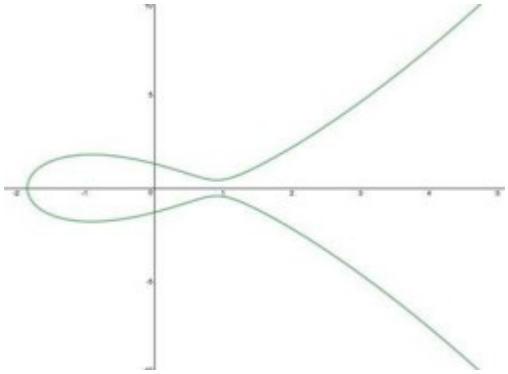

Figure 4: Simple elliptic curve visualization [11]

5.3.1 *Key Generation*

- Select two large prime integer numbers p and q to calculate the modulus n using the formula $n = p \times q$.
- Calculate $\emptyset$ using the formula $\emptyset(n) = (p - 1) \times (q - 1)$.
- Select an integer e which is the public exponent, such that GCD $(e, \emptyset(n)) = 1$,
- where GCD refers to greatest common divisor function between two numbers.
- Calculate d which is the private exponent, such that $e \times d = 1$ mod $\emptyset(n)$, where mod symbolizes to the modulus operation or the reminder after division.

Hence, (n,e) represents the public Encryption key, while (n, d) represents the private decryption key [18]. The two prime numbers are the target of the algorithms.

5.3.2 *Encryption/Decryption Processes*

Let m be a message that wanted to be encrypted, then the encrypted message c is calculated via the public key (n, e) using the equation: $c = m^e \, mod \, n$. To extract the original message m, the received encrypted message c is decrypted via the private key (n, d) using the equation: $m = c^d mod \, n$ [18].

5.4. *ElGamal algorithm*

Security mentioned algorithm depends over hard to calculating discrete logarithms of large prime numbers. If the same plaintext is encrypted using this cryptosystem, then a different cipher text is obtained in each time of Encryption. El-Gamal operation can be described in 3 main steps:

1) key generation, 2) Encryption and 3) Decryption processes which are explained briefly as follows.

5.4.1 Key Generation

- First, select a random prime number p and two other random numbers x and g, such that both of them are less than p.
- Calculate y using the formula: $y = gx \ mod \ p$.
- Thus, (p, g, y) represents the public key which can be shared between a group of users, while x represents the private key which should be kept secret [19].

5.4.2 Encryption/Decryption Processes

In order to Encrypt a message m, firstly, a random integer number k is selected, such that k is relatively prime with $(p - 1)$. Secondly, the cipher text pairs ($c1$, $c2$) is calculated using the equations: $c1 = g^k mod \ p$ and $c2 = (y^k \times m) \ mod \ p$. Finally, the cipher text ($c1$, $c2$) is transmitted to the recipient. To Decrypt the cipher text, pair ($c1$, $c2$), the private key x is employed to recover the original message m using the equation: $m = \frac{c2}{c1^x} \ mod \ p$ [19].

The following pseud codes for ElGamal Algorithms namely Key Generation, Encryption and Decryption. Figure 5: Pseudo-code key generation stage: encryption and decryption.

➢ **Encryption Stage**

ElGamal_Encryption (e_1, e_2, p, P) // P is the plaintext
{
Select a random integer r in the group $\mathbf{G} = < \mathbf{Z}_p^*, \times >$
$C_1 \leftarrow e_1^r \bmod p$
$C_2 \leftarrow (P \times e_2^r) \bmod p$ // C_1 and C_2 are the ciphertexts
return C_1 and C_2
}

➢ **Decryption Stage**

ElGamal_Decryption (d, p, C_1, C_2) // C_1 and C_2 are the ciphertexts
{
$P \leftarrow [C_2 (C_1^d)^{-1}] \bmod p$ // P is the plaintext
return P
}

➢ **Key Generation Stage**

ElGamal_Key_Generation
{
Select a large prime p
Select d to be a member of the group $\mathbf{G} = < \mathbf{Z}_p^*, \times >$ such that $1 \le d \le p - 2$
Select e_1 to be a primitive root in the group $\mathbf{G} = < \mathbf{Z}_p^*, \times >$
$e_2 \leftarrow e_1^d \bmod p$
Public_key $\leftarrow$ (e_1, e_2, p) // To be announced publicly
Private_key $\leftarrow$ d // To be kept secret
return Public_key and Private_key
}

Figure 5: Pseudo-code key generation stage: encryption and decryption

6. Methodology

Methodology of our proposed system is by Hybrid /blended of two algorithms namely: (i.e. AES with RSA) and (i.e. AES with ECC), also (i.e. AES with ElGamal). The enhancement of security performance for developing and comparing an excellent result in milliseconds unit by Java programing language. Hence, there are an indirect relation between the performance-security and time- consume in milliseconds unit. The Figure 6 show indirect relation between performance-security and time-consume. The creation of web Ecommerce and secured by one of the blended algorithms as a methodology and protect the website. As mentioned, that before the protection of website should be by one of the algorithms.

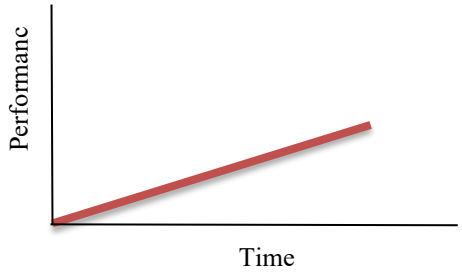

Figure 6: Time

Nevertheless, the performance analysis is an important part of our proposed system by Hybrid techniques between two algorithms and show that the best performance with less time unit and explained in Table below. The Table 2- show all file types with Hybrid algorithms of AES-RSA performance analysis. The main purpose of our proposed system is mixing two algorithms and test the six types of files such as: jpg, txt, pdf, pptx, mp3, mp4 with different file size over Hybrid AES-RSA. The Encryption time and throughput of all types that show it in Table 2 by blended AES and RSA

Table 2: Hybrid AES-RSA Encryption Performance Comparison: Encryption Time and Throughput

File Type	Text size (In Kb)	Encryption Time	Encryption Throughput
JPG	9328	120	71746.15
TXT	3765	55	68436.36
PDF	1136	25	45400.0
PPTX	1743	31	56193.54
MP3	57531	709	81142.45
MP4	4555	60	75900.0
Average Time		166.66	66469.75

The Hybrid techniques between two algorithms and show that the best performance with less time unit and explained in Table below. The Table 3 show all file types with Hybrid algorithms of AES-RSA performance analysis. The main purpose of our proposed system is mixing two algorithms and test the six types of files such as: jpg, txt, pdf, pptx, mp3, mp4 with different file size over Hybrid AES-RSA.

The decryption time and throughput of all types that show it in Table 3 by blended AES and RSA.

Table 3: Hybrid AES-RSA Decryption Performance Comparison: Decryption Time and Throughput

File Type	Text size (In Kb)	Decryption Time	Decryption Throughput
JPG	9328	179	52106.14
TXT	3765	75	50186.66
PDF	1136	50	22700.0
PPTX	1743	47	37063.82
MP3	57531	722	79681.44
MP4	4555	99	46000.0
Average Time		195.33	47956.34

The Hybrid techniques between two algorithms and show that the best performance with less time unit and explained in Table below. The Table 4 show all file types with Hybrid algorithms of AES- ECC performance analysis. The main purpose of our proposed system is mixing two algorithms and test the six types of files such as: jpg, txt, pdf, pptx, mp3, mp4 with different file size over Hybrid AES- ECC.

The Encryption time and throughput of all types that show it in Table 4 by blended AES and ECC.

Table 4: Hybrid AES- ECC Encryption Performance Comparison: Encryption Time and Throughput

File Type	Text size (In Kb)	Encryption Time	Encryption Throughput
JPG	9328	735	12689.79
TXT	3765	608	6190.78
PDF	1136	585	1940.17
PPTX	1743	595	2927.73
MP3	57531	1570	36643.31
MP4	4555	648	7027.77
Average Time		790.166	11236.59

The Hybrid techniques between two algorithms and show that the best performance with less time unit and explained in Table below. The Table 5 show all file types with Hybrid algorithms of AES- ECC performance analysis. The main purpose of our proposed system is mixing two algorithms and test the six types of files such as: jpg, txt, pdf, pptx, mp3, mp4 with different file size over Hybrid AES- ECC.

The Decryption time and throughput of all types that show it in Table 5 by blended AES and ECC

Table 5: Hybrid AES- ECC Decryption Performance Comparison: Decryption Time and Throughput

File Type	Text size (In Kb)	Encryption Time	Encryption Throughput
JPG	9328	186	50145.16
TXT	3765	100	37640.0
PDF	1136	65	17461.53
PPTX	1743	69	25246.37
MP3	57531	802	71733.16
MP4	4555	117	38923.07
Average Time		790.166	11236.59

The Hybrid techniques between two algorithms and show that the best performance with less time unit and explained in Table below. The Table 3 show all file types with Hybrid algorithms of AES-ElGamal performance analysis. The main purpose of our proposed system is mixing two algorithms and test the six types of files such as: jpg, txt, pdf, pptx, mp3, mp4 with different file size over Hybrid AES- ElGamal.

The Encryption time and throughput of all types that show it in Table 6 by blended AES and ElGamal.

Table 6: Hybrid AES- ElGamal Encryption Performance Comparison: Encryption Time and Throughput

File Type	Text size (In Kb)	Encryption Time	Encryption Throughput
JPG	9328	877	10635.11
TXT	3765	788	4776.64
PDF	1136	769	1475.942
PPTX	1743	763	2283.09
MP3	57531	1787	32193.62
MP4	4555	805	5657.14
Average Time		964.83	9503.59

The Hybrid techniques between two algorithms and show that the best performance with less time unit and explained in Table below. The Table 7 show all file types with Hybrid algorithms of AES- ElGamal performance analysis. The main purpose of our proposed system is mixing two algorithms and test the six types of files such as: jpg, txt, pdf, pptx, mp3, mp4 with different file size over Hybrid AES- ElGamal.

The Decryption time and throughput of all types that show it in Table 7 by blended AES and ElGamal.

Table 7: Hybrid AES- ElGamal Decryption Performance Comparison: Decryption Time and Throughput

File Type	Text size (In Kb)	Decryption Time	Decryption Throughput
JPG	9328	300	31090.0
TXT	3765	150	25093.33
PDF	1136	115	9869.56
PPTX	1743	127	13716.53
MP3	57531	1170	49170.94
MP4	4555	174	26172.41
Average Time		339.33	25852.12

In order to achieve more information from previous comparability between three performance which are: Hybrid algorithm of (AES-RSA, AES-ECC, AES- ElGamal). The Table below shows performance analysis for several Hybrid Encryption algorithm, in respect of the average time and throughput. encryption time and Encryption throughput are two parameters that complete and been blended together. In the context of the

presented data information. The three Hybrid /OR blended algorithms are explained below:

- Hybrid AES-RSA: The result blended AES-RSA Encryption algorithms by average time is 166.66 milliseconds. Nevertheless, an encryption time of throughput of blended AES-RSA is 66469.75 milliseconds. The encryption throughput for this Hybrid approach is much higher and more notable. this combination between two algorithms namely Hybrid AES-RSA, thus the Encryption Time and Encryption Throughput is much less than the other blend algorithms (Hybrid AES-ECC and Hybrid AES- ElGamal). However, the Hybrid AES-RSA is outcome is much better and fewer than the others blended algorithms, which are; Hybrid AES-ECC and Hybrid AES- ElGamal. All result is show in Table 8.

Table 8: Average Time Encryption and Throughput of AES-Based Hybrid Cryptosystems with RSA, ElGamal, and ECC in milliseconds

Average Time	Encryption Time	Encryption Throughput
Hybrid AES-RSA	166.66	66469.75
Hybrid AES-ECC	790.166	11236.59
Hybrid AES-ElGamal	964.83	9503.59

In order to achieve more information from previous comparability between three performance which are: Hybrid algorithm of (AES-RSA, AES-ECC, AES- ElGamal). The Table below shows performance analysis for several Hybrid decryption algorithm, in respect of the average time and throughput. decryption time and decryption throughput are two parameters that complete and been blended together. In the context of the presented data information. The three Hybrid /OR blended algorithms are explained below:

- Hybrid AES-RSA: The result blended AES-RSA decryption algorithms by average time is 195.33 milliseconds. Nevertheless, an Encryption time of throughput of blended AES-RSA is 47956.34 milliseconds. The decryption throughput for this Hybrid approach is much higher and more notable. this combination between two algorithms namely Hybrid AES-RSA, thus the Decryption Time and Decryption Throughput is much less than the other blend algorithms (Hybrid AES-ECC and Hybrid AES-ElGamal). However, the Hybrid AES-RSA is outcome is much better and fewer than the others blended algorithms, which are; Hybrid AES-ECC and Hybrid AES- ElGamal. All result is show in Table 9.

Table 9: Average Time Decryption and Throughput of AES-Based Hybrid Cryptosystems with RSA, ElGamal, and ECC in milliseconds

Average Time	Decryption Time	Decryption Throughput
Hybrid AES-RSA	195.33	47956.34
Hybrid AES-ECC	223.16	40191.54
Hybrid AES-ElGamal	339.33	25852.12

However, the two pi-chart below give more information regarding our proposed system average Time Encryption and throughput of AES-Based Hybrid Cryptosystems with RSA, ElGamal, ECC. the Figure 7 show the best performance Hybrid AES-RSA over (Hybrid AES-ECC and Hybrid AES- ElGamal).

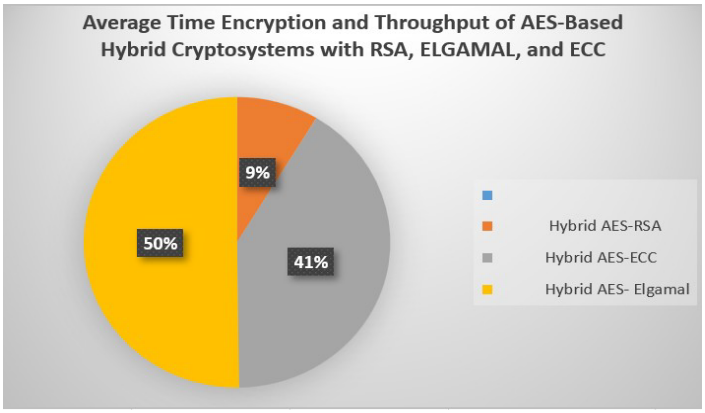

Figure 7: Average Time Encryption and Throughput (Hybrid AES-ECC and Hybrid AES- ElGamal)

The Hybrid AES-RSA Encryption method demonstrates an average Decryption time of 195.33 milliseconds, achieving a throughput of 47956.34 decrypts per second. In comparison, Hybrid AES-ECC exhibits a slightly longer decryption time of 223.16 milliseconds with a throughput of 40191.54 decrypts per second. Hybrid AES- ElGamal, on the other hand, has a higher Decryption time of 339.33 milliseconds and a throughput of 25852.12 Decrypts per second. which Mentioned and explained clearly in Table 9, by of information in Table 9 created a pie-chart Figure 8.

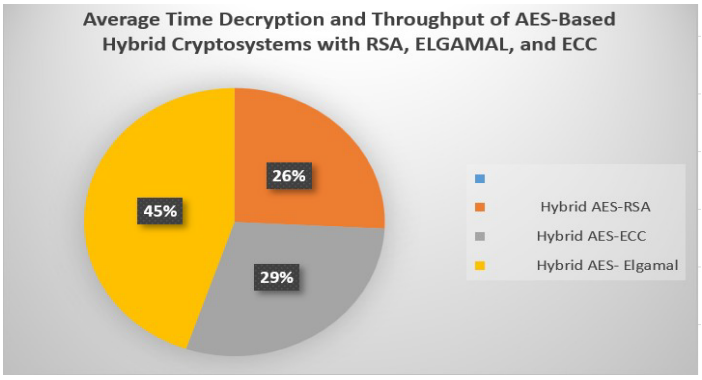

Figure 8: Average Time Decryption and Throughput (Hybrid AES-ECC and Hybrid AES- ElGamal)

7. Conclusion

In conclusion, the data analysis declared that the performance variations among the three Hybrid encryption methods namely

Hybrid AES-RSA, Hybrid AES-ECC, and Hybrid AES- ElGamal. The Hybrid AES-RSA proves superior speed in both schemes' encryption and decryption processes. This mean that making its an optimal choice for applications requiring swift data protection. Furthermore, it achieved the highest throughput for encryption and decryption and underlining its efficiency. Nevertheless, Hybrid AES-ECC and Hybrid AES-ElGamal exhibit slower encryption and decryption time-consume that is why making them less suitable for time-sensitive tasks. Although both are offer certain cryptographic advantages to reduced throughput may limit their applicability.

Eventually, the selection of an encryption scheme should be based on a careful consideration of security requirements and performance requirements. The speed is important for Hybrid AES-RSA stands out as the most favorable option, while Hybrid AES-ECC and Hybrid AES- ElGamal may be more appropriate in situations where performance is less critical, and specific security features are prioritized.

References

[1] P. Patil and R. Bansode, "Performance Evaluation of Hybrid Cryptography Algorithm for Secure Sharing of Text & Images," International Research Journal of Engineering and Technology 2020

[2] K. H. A. Faraj, A. B. Kanbar, J. Gul-Mohammed, W. M. Hmeed, and S. F. Karim, "Cloud Computing Loading Time Over Different Operating Systems," Science Journal of University of Zakho, **8**(4):154–159, 2020, DOI: https://doi.org/10.25271/sjuoz.2020.8.4.756

[3] Z. C. Oleiwi, W. A. Alawsi, W. C. Alisawi, A. S. Alfoudi, and L. H. Alfarhani, "Overview and Performance Analysis of Encryption Algorithms," J. Phys. Conf. Ser., **1664**(1), 2020, DOI: https://doi.org/10.1088/1742-6596/1664/1/012051

[4] P. Chinnasamy, S. Padmavathi, R. Swathy, and S. Rakesh, "Efficient Data Security Using Hybrid Cryptography on Cloud Computing," Lect. Notes Networks Syst., **145**(September):537–547, 2021, DOI: https://doi.org/10.1007/978-981-15-7345-3_46

[5] F. Maqsood, M. Ahmed, M. M. Ali, and M. A. Shah, "Cryptography: A Comparative Analysis for Modern Techniques," Int. J. Adv. Comput. Sci. Appl., **8**(6):442-448, 2017, DOI: https://doi.org/10.14569/IJACSA.2017.080659

[6] P. Verma, J. Shekhar, P. Preety, and A. Asthana, "A Survey for Performance Analysis Various Cryptography Techniques Digital Contents," International Journal of Computer Science and Mobile Computing, **4**(1):522–531, 2015

[7] N. Bisht and S. Singh, "A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms," International Journal of Innovative Research in Science, Engineering and Technology, **4**(3):1028-1031, 2015, DOI: https://doi.org/10.15680/IJIRSET.2015.0403043

[8] S. Chandra and S. Paira, "A Comparative Survey of Symmetric and Asymmetric Key Cryptography," in 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), 2014, 1-4, DOI: https://doi.org/10.1109/ICECCE.2014.7086640

[9] P. Kuppuswamy and S. Q. Y. Al-Khalidi, "Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm," Manage. Inf. Syst. Rev., **19**(2):1-13, 2014, DOI: https://doi.org/10.6131/MISR.2014.1902.01

[10] P. Verma, P. Guha, and S. Mishra, "Comparative Study of Different Cryptographic Algorithms," Int. J. Emerg. Trends Technol. Comput. Sci., **5**(2):58-63, 2016

[11] R. Harkanson and Y. Kim, "Applications of Elliptic Curve Cryptography: A Light Introduction to Elliptic Curves and a Survey of Their Applications," in 12th Annual Cyber and Information Security Research Conference, USA, 2017, 1-7

[12] K. Keerthi and B. Surendiran, "Elliptic Curve Cryptography for Secured Text Encryption," in International Conference on Circuits Power and Computing Technologies, India, 2017

[13] S. C. Iyer, R. R. Sedamkar, and S. Gupta, "A Novel Idea on Multimedia Encryption Using Hybrid Crypto Approach," in 7th International Conference on Communication, Computing and Virtualization, 2016, **79**:293-298

[14] S. C. Iyer, R. R. Sedamkar, and S. Gupta, "An Efficient Multimedia Encryption Using Hybrid Crypto Approaches," Int. J. Recent Trends Eng. Res., **2**:442-452, 2016

[15] S. Sharma and V. Chopra, "Analysis of AES Encryption with ECC," in Proceedings of International Interdisciplinary Conference on Engineering Science & Management, 2016, 195

[16] D. Ameta and S. Upadhyay, "A Hybrid Approach for Image Encryption Using Different Number Iterations in ECC and AES Techniques," Int. J. Comput. Appl., **175**(3), 2017, DOI: https://doi.org/10.5120/ijca2017915469

[17] N. Mathura and R. Bansode, "AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection," in Proc. 7th Int. Conf. Commun., Comput., Virtualization, 2016, 131-135, DOI: https://doi.org/10.1016/j.procs.2016.03.131

[18] F. Yousif, "Encryption and Decryption of Audio Signal Based on RSA Algorithm," Int. J. Eng. Technol. Manage. Res., **5**(7):259-264, 2018, DOI: https://doi.org/10.29121/ijetmr.v5.i7.2018.259

[19] O. A. Imran, S. F. Yousif, I. S. Hameed, W. N. Al-Din Abed, and A. T. Hammid, "Implementation of El-Gamal Algorithm for Speech Signals Encryption and Decryption," Procedia Comput. Sci., **167**:1028–1037, 2020, DOI: https://doi.org/10.1016/j.procs.2020.03.402

Copyright: This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-SA) license (https://creativecommons.org/licenses/by-sa/4.0/).