

A hybrid encryption system for communication and financial transactions using RSA and a novel symmetric key algorithm

Prakash Kuppuswamy¹, Saeed Qasim Yahya Al Khalidi Al-Maliki², Rajan John³, Mohammad Haseebuddin³, Ahmed Ali Shaik Meeran⁴

¹Department of Computer and Network Engineering, College of CS and IT, Jazan University, Jazan, Kingdom of Saudi Arabia

²Department of Information science, King Khalid University, Abha, Kingdom of Saudi Arabia

³Department of Computer Science, College of CS and IT, Jazan University, Jazan, Kingdom of Saudi Arabia

⁴Department of Information Technology, College of CS and IT, Jazan University, Jazan, Kingdom of Saudi Arabia

Article Info

Article history:

Received Oct 10, 2022

Revised Nov 18, 2022

Accepted Nov 28, 2022

Keywords:

Cryptography

Data security

Hybrid encryption

Information security

Rivest Shamir Adleman

ABSTRACT

Today's digital data transmission over unsecured wired and wireless communication channels is making encryption algorithms an increasingly important tool for securing data and information. Hybrid encryption techniques combine encryption schemes of either two symmetric keys or both symmetric and asymmetric encryption methods, and that provides more security than public or private key single encryption models. Currently, there are many techniques on the market that use a combination of cryptographic algorithms and claim to provide higher data security. Many hybrid algorithms have failed to satisfy customers in securing data and cannot prevent all types of security threats. To improve the security of digital data, it is essential to develop novel and resilient security systems as it is inevitable in the digital era. The recommended algorithm scheme is a combination of the well-known Rivest Shamir Adleman (RSA) algorithm and a simple symmetric key (SSK) algorithm. The aim of this study is to develop a better encryption method using RSA and a newly proposed symmetric SSK algorithm. We believe that the proposed hybrid cryptographic algorithm provides more security and privacy.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Prakash Kuppuswamy

Department of Computer and Network Engineering

College of Computer Science and Information Technology, Jazan University

Al Maarefah Rd, Jazan, Kingdom of Saudi Arabia

Email: pperumal@jazanu.edu.sa

1. INTRODUCTION

Cryptography is a scrambled language that is called as art and science of secret writing, which cannot be achieved without the use of creative action and entrepreneurship [1]. It incorporates mathematical techniques as well as mechanisms related to information security or data security. Data security provides individual users' data privacy, confidentiality, data integrity, and data provenance authentication. Digital signatures, hash functions, message authentication codes, and encryption are four key cryptographic techniques used to achieve these goals [2]-[4]. In cryptography, encrypting mode is the content of a message that becomes unreadable format to outsiders. Once the message is encrypted, it is called ciphertext. The technical process of transforming the ciphertext into a readable format is called decryption. The standard method of encipher and decipher procedure comprises the use of a secret key, and decryption can be done only when the key is known by the authorized user.

There are numerous encryption algorithms used in the field of information security. They can be divided into symmetric (private) and asymmetric (public) encryption techniques. The term symmetric algorithm refers that, it uses of the same key to encrypt and decrypt. Asymmetric cryptosystem the method of enciphering and deciphering procedure uses encryption and decryption of two different keys [5], [6]. A symmetric algorithm is a mutual distribution of the collective secret between two users, such as the data encryption standard (DES) algorithm, which is the most important feature of any cryptosystem. In asymmetric cryptosystems, the encryption keys are public and the decryption keys are private. With asymmetric keys, asymmetric key encryption can solve the problem of key distribution. Both symmetric and public keys are used in this process. Public key is used for encryption and a private key is used for decryption [7], [8]. When asymmetric algorithms are used, there is no need to share secrets between the parties as they use different values for encryption procedures and revealing the text message. Asymmetric algorithms must each keep their own secret. The problem of key exchange in symmetric algorithms formed the basis for asymmetric algorithms known as public key cryptosystems. In 1976, Whitfield Diffie and Martin Hellman developed the first hybrid system [7], [9].

In recent years, technology and network tools have greatly changed the way people work and live [10]. The hybrid encryption algorithm is designed for secure and highly effective [11]. Also, it has chances of information theft. Simple encryption is not only very secure but also can be directly applied to encrypted financial data. With this method, the decryption output is similar to when the plaintext is processed directly, which is very convenient. In order to combine the advantages of the current research results for the encryption of users' private and financial data, a new hybrid encryption model is proposed [1]. In both private and public sectors, the malicious activities on cyber infrastructure are increasing every day, and thus the security requirements are also increasing [12], [13]. There may be many issues related to the security and protection of data during transmission [14], [15]. Hence, eventually required an efficient and robust approach to ensure the secure transmission of sensitive data along with its authentication over public networks [16], [17]. Combination of two different algorithms into a single hybrid algorithm is motivated by the possibility and it gives better performance and securities [18], [19]. Consequently, hybrid algorithm techniques provide a new class of algorithms [20], [21]. A hybrid scheme provides more data confidentiality which is to be achieved by this hybrid cryptosystem which contains all the interchangeable and dissimilar cryptography rules [22], [23]. In order to ensure safe communication and secure transactions, there are several factors to consider, including the type of channel used, the business model, and the associated security infrastructure. Security systems that are hybrid or new-model can only satisfy stakeholders' trust [23]-[25].

2. RELATED STUDY

Manna *et al.* [6] propose a two-layer hybrid cryptosystem to avoid interception and protect the shared key. Accordingly, the authors have developed a hybrid cryptosystem that uses a private key encryption model and a public key combination model. The encryption of the private key disclosure itself was performed using Rivest Shamir Adleman (RSA) public key encryption. Despite the fact that the captured key may not be a valid one, the authors described the scheme as providing better security because the shared key is intercepted during the exchange between the sender and receiver. Data transmission and files can be handled by the proposed algorithm.

Research by Sajay *et al.* [20] security and the proper implementation of cloud computing over the network are the two most important issues related to cloud computing. There are five models of security in the cloud: confidentiality, authentication, accessibility, data recovery, and data integrity. In order to enhance data security in the cloud, encryption techniques should be applied during cloud data storage. A hybrid algorithm is proposed to develop cloud data security using encryption algorithms. It is primarily used to secure or store large amounts of data in cloud storage.

Research by Tariq *et al.* [11] a logarithmic-based image encryption structure is investigated for potential key leakages using a public key. Statistical analyses of entropy, correlation, and unified averaged changes in intensity were used to identify the scope of the security against various cryptographic outbreaks. To measure the unpredictability of the new encryption scheme, entropy and NIST chance suit experiments were adopted. These schemes are applied in the digital images to examine the outcomes. As a result of this encryption method, multimedia security seems quite reasonable.

Research by Hamdi [16], offers a modest and well-organized hybrid encryption that applies block cipher and stream cipher cryptographic systems. Using the chirikov standard map, this algorithm further minimizes the encryption time by using a chaotic system. Stream ciphers use two sequences, the first method generates pseudorandom blocks applied into stream cipher and the next method uses substitution and permutation sequence table are used. Different cryptographic tests and metrics are used to measure identify the scope, performance and security level of the new type of hybrid algorithm [14].

According to Yao and Su [1], focuses on securing hospital financial data. In the article, the author presented a hybrid encryption algorithm called the Noekeon algorithm. It uses the RSA cryptography scheme and the DES algorithm. According to the author, the message is encrypted twice in the encryption method. A large quantity of hospital financial data can be encrypted and decrypted efficiently and at high speeds with this scheme, according to the authors. Better performance and higher security are shown in the research article. It offers fast file transfers and security for files stored by Noekeon. By combining RSA with DES, the proposed model avoids the inefficient properties of the RSA algorithm to form a new Noekeon algorithm.

3. PROPOSED ALGORITHM

3.1. RSA and SSK tools

There are two ways to implement symmetric keys either stream ciphers or block ciphers. Block ciphers consist of fixed size of a variable is converted into ciphertext data of the same length. We know that a user ID will consist of a series of alphabetical characters, followed by a series of numbers, ranging from 0-9 respectively. We introduce synthetic data; the synthetic data value consists of equivalent values of alphabets and integers. Each alphabetical value is assigned as a numeric value, such as alphabet A is 1, B is 2, and so on. In addition to that, we consider integer value 0 to be known as 27 and 2 as 28, and finally, 9 is assigned 36, as well as the space value, which is 37. In Figure 1, the encrypt and decrypt procedure was as follows:

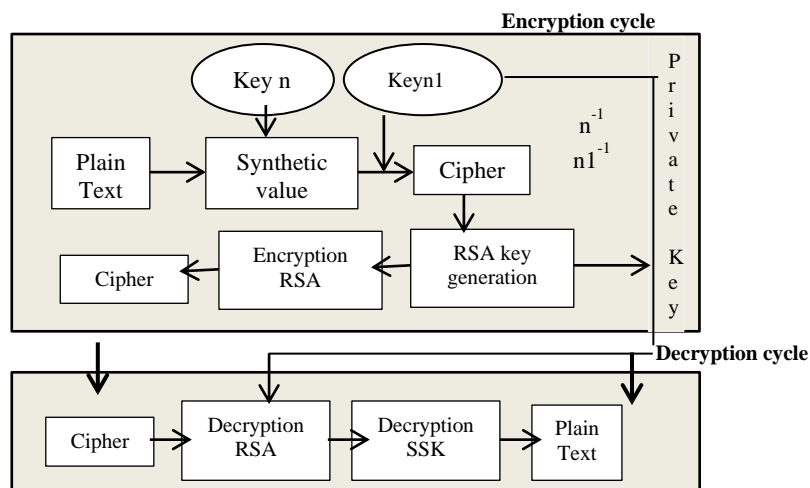


Figure 1. Encryption/decryption cycle

3.1.1. Generating the SSK keys

The modular multiplicative inverse is an integer ‘x’ such that.

$$a x \cong 1 \pmod{m} \tag{1}$$

The value of x should be in {1, 2, ... m-1}, i.e., in the range of integer modulo m. Multiplicative inverses of "a" modulo "m" only exist when "a" and "m" are relatively prime (i.e., when gcd(a, m)=1).

3.1.2. Generating the RSA keys

It is important that the chosen prime numbers are large so that someone will have trouble figuring them out. Calculate $n = (x, x, y)$

Use *totient* function to find out the value of $\phi(n) = (x - 1)(y - 1)$ (2)

Select an integer *e*, such that *e* is *co-prime* to $\phi(n)$ and $1 < e < \phi(n)$ (3)

The pair of numbers (n,e) makes up the public key.

$$\text{Identify 'd' with using extended Euclidean algorithm that } e \cdot d = 1 \bmod \phi(n) \quad (4)$$

The pair (n,d) marks up the private key [19].

3.1.3. Encryption

For the encryption process, the RSA algorithm required plain text as well as e and n . The message was assigned to integers from 1 to 26 based on the alphabet. Given plaintext P , represented as a number, the ciphertext C is calculated as (5):

$$C = Pe \bmod n \quad (5)$$

3.1.4. Decryption

With the use of a private key, the decryption process is exactly the reverse of encryption. For the decryption of RSA algorithm required cipher text as well as d and n . Using the following equation, the plaintext or sender's message can be determined.

$$P = Cd \bmod n \quad (6)$$

3.2. Key generation procedure of RSA and SSK

A key assumption behind the RSA algorithm scheme is that integer factorization is a challenging task. It means that given a large value n , it is hard to identify the prime factors that makeup n . It is the most popular asymmetric key algorithm.

3.2.1. SSK

The process of simple symmetric key generation (SSK) is straightforward. Pick two integer numbers, one positive and one negative, with $n=37$ because it is a fixed number of modulus. The key generation processing steps are listed in sequence from a to c.

- Select any two integer numbers likely one positive and negative say as $n, n1$
- Find the inverse of the 'n' on modulo 37(key 1) say k .
- Again calculate the inverse of $n1$ on modulo 37 say as $k1$.

3.2.2. RSA

The process of RSA key generation is easy and vibrant. Pick two large integers, p and q , with n being the product of p multiplied by q . It is not a fixed number of modulus. The key generation processing steps are listed in sequence from a to e.

- Choose two very large random prime integers p and q
- Compute n and $\phi(n): n=p \cdot q$ and $\phi(n)=(p-1)(q-1)$
- Choose an integer e , $1 < e < \phi(n)$ such that: $\gcd(e, \phi(n))=1$
- Compute d , $1 < d < \phi(n)$ such that: $e \cdot d \equiv 1 \pmod{\phi(n)}$
- Public key is (n, e) and the Secret key or private is (n, d)

3.3. Encryption method

The hybrid method is a combination of simple symmetric key and RSA algorithm. The first process of C =Cipher Text is derived from SSK and the second process of $C1$ =Cipher Text1 is derived from RSA. The encryption processing steps are listed in sequence from a to d.

- An alphabetical equivalent integer synthetic value assigned to user message 'M'
- Multiply synthetic value with random selected integer number $n, n1$
- Evaluate with modulo 37, $C=(M \cdot n \cdot n1) \bmod 37$
- Ciphertext $C1=C^e \pmod{n}$, Now the encrypted text is "C1"

3.4. Decryption method

The hybrid decryption process is a straightforward method. The first process of C =Cipher Text is derived from SSK and the second process of M =Plain Text or Message or Revealed text is derived from RSA. The decryption processing steps are listed in sequence from a to d.

- Use key1 and key then multiply with the received text.
- Then calculate the identified value with modulo 37
- Remainder is $C=(C1 \cdot n^{-1} \cdot n1^{-1}) \bmod 1$
- Revealed plain text or message $M=C^d \pmod{n}$

4. IMPLEMENTATION

4.1. Algorithm

The algorithm is a step-by-step procedure that defines a set of protocol that must be carried out in a specific order to produce the desired result. Hybrid security algorithm steps are described in the following sections. In sections 4.1.1 and 4.1.2, the algorithm steps for SSK and RSA are presented. In section 4.1.3, the encryption/decryption process is explained.

4.1.1. Using SSK

The implementation protocol of simple symmetric encryption (SSK) is very easy and it is based on two variables, one positive integer and another negative integer. The encryption process of SSK processing steps is listed below from a to d.

- Choose any random negative or positive integer $\rightarrow n, n1$
- Inverse of $n, n1 \pmod{37} \rightarrow k, k1$ // SSK Key generation
- Plaintext $\rightarrow M$
- $C \rightarrow (M * n * n1) \pmod{37}$ // SSK Encryption

4.1.2. Using RSA

The implementation protocol of RSA is moderate and it is based on two large prime numbers. There are many mathematical calculations such as GCD, inverse, Euler's phi theorem and congruent functions are used. The encryption process of RSA processing steps is listed below from a to h.

- Choose two prime numbers $N \rightarrow pq$ // RSA Key generation
- Calculate $\phi(N) \rightarrow (p-1) * (q-1)$ (Euler's totient function)
- Randomly pick e so that $\gcd(e, \phi(N)) \rightarrow 1$
- Validate e and $\phi(N)$ is relatively prime
- Identify d such that $e * d \rightarrow 1 \pmod{\phi(N)}$
- Verify, d is the multiplicative inverse of e
- Public key is $\rightarrow (e, N)$
- Private key is $\rightarrow (d, N)$

4.1.3. Encryption and decryption

The hybrid encryption and decryption process is a quite simple method. A message encrypted using SSK and RSA produces C and $C1$, respectively. The initial decryption process of C =Cipher Text is derived from SSK. The second process of M =Plain Text or Message or Revealed text is derived from RSA. The decryption processing steps are listed below in sequence of a to c.

- Encrypt $C1 \rightarrow C^e \pmod{N}$ // RSA Encryption
- Decrypt $(C) \rightarrow C1^d \pmod{N}$ // RSA Decryption
- Plaintext $M \rightarrow (C * k * k1) \pmod{37}$ // SSK Decryption

The encryption technique is known as scrambling programs. When plaintext or message are unscrambled, it is very easy to identify by the intruder even in the binary format of the message, so that is required scrambled encryption mode. There are lot of security issues are happen transmitting messages between sender and receiver. Message interception and modification has commonly appeared in premature cryptography algorithm. So, that integrity and confidentiality are significant features of a well efficient algorithm. It is the basis of the protocol that enables us to provide security while accomplishing an incredibly vital system. In order to better understand the proposed hybrid technique, plaintext "CRYPTO2022" was chosen for experimental purposes as shown in Table 1.

Table 1. Plain text message

Message	C	R	Y	P	T	O	2	0	2	2
Equivalent integers	3	18	25	16	20	15	29	27	29	29

4.2. Key generation of SSK

We chose $n=3$ and its inverse number= 25 as the experimental key generation number. In this case, the second number is -8 and its inverse is 23 . These two inverse numbers are securely shared with the recipient for the purpose of decryption. The key generation of SSK processing steps is listed below from a to d.

- Selecting random integer number $n=3$
- Then inverse of $3=25$ (verification $3 \times 25 \pmod{37}=1$) So, Key1= 25
- Again, selecting random negative numbers $n1=-8$

d. Then the inverse of -8 is known as 23 (verify $-8 \times 23 = -184 \pmod{37} = 1$) So, $Key_2 = 23$, Here is the encryption process using SSK shown in Table 2.

Table 2. Encryption process of SSK

Plain Text	Integer Value	CT=(M*n) mod 37	CT=(CT*n1) mod 37	Cipher Text
C	3	9	2	B
R	18	17	12	L
Y	25	1	29	2
P	16	11	23	W
T	20	23	1	A
O	15	8	10	J
2	29	13	7	G
0	27	7	18	R
2	29	13	7	G
2	29	13	7	G

4.3. Key generation of RSA

In an experiment to generate RSA keys, we selected the first prime number $p=3$ and the second prime number $q=11$. Based on the chosen p and Q , we derived n and ϕ 'n'. In addition, a randomly chosen e and its inverse d based on the modulo n is needed to generate the key. The key generation process for RSA is mentioned below.

$P=3; q=11; \text{Therefore, } n=33 \text{ and } \phi n=20$

Selecting 'e'=7 then inverse of 'e' or $d=3$ (verification $7 \times 3 \pmod{20} = 1$)

Public key is $e, n=7, 33$

Private key 'd'=3

4.4. RSA encryption

From above Table 2, we receive the ciphertext message "BL2WAJGRGG", which is equivalent to integer values 2, 12, 29, 23, 1, 10, 7, 18, 7, 7. In the first column the cipher text is mentioned, and in the second column its equivalent integer values are placed. The third column uses RSA encryption, the fourth column refers to remainder values, and the derived value is assigned an alphanumeric value. The encryption result is shown in Table 3, and it is encrypted with RSA public and private keys $((m)^e \pmod n)$.

Table 3. Encryption process of RSA

Cipher Text	Integer value	RSA encryption	Remainder value	Equivalent alphanumeric
B	2	$(2)^7 \pmod{33} = 29$	29	2
L	12	$(12)^7 \pmod{33} = 12$	12	L
2	29	$(29)^7 \pmod{33} = 17$	17	Q
W	23	$(23)^7 \pmod{33} = 23$	23	W
A	1	$(1)^7 \pmod{33} = 1$	1	A
J	10	$(10)^7 \pmod{33} = 10$	10	J
G	7	$(7)^7 \pmod{33} = 28$	28	1
R	18	$(18)^7 \pmod{33} = 6$	6	F
G	7	$(7)^7 \pmod{33} = 28$	28	1
G	7	$(7)^7 \pmod{33} = 28$	28	1

4.5. Decryption process of RSA and SSK

Encrypted messages received from the sender are shown in the Table 3. For the decryption process to retrieve the original message, we applied the SSK and RSA algorithms mentioned in the Tables 4 and 5. In the first column the cipher text is mentioned, and in the second column its equivalent integer values are placed. The third column uses RSA encryption, the fourth column refers to remainder values, and the derived value is assigned an alphanumeric value in fifth column of Table 4. In the second stage, we applied the SSK algorithm shown in Table 5, in the first column cipher text stage 2 obtained from Table 4. In the second column, equivalent integer values are assigned. This is followed by the SSK decryption process mentioned in column 3 and finally revealed cipher text or original message shown in column 4 of Table 5. The decryption process of the hybrid scheme is described in Tables 4 and 5, where the private key $((m)^d \pmod n)$ and the inverse of $n, n1$ is called $k1, k2$.

Table 4. Decryption process of RSA

Cipher text	Integer value	RSA decryption	Remainder	Equivalent alphanumeric
2	29	$(29)^3 \text{ mod } 33=2$	2	B
L	12	$(12)^3 \text{ mod } 33=12$	12	L
Q	17	$(17)^3 \text{ mod } 33=29$	29	2
W	23	$(23)^3 \text{ mod } 33=23$	23	W
A	1	$(1)^3 \text{ mod } 33=1$	1	A
J	10	$(10)^3 \text{ mod } 33=10$	10	J
1	28	$(28)^3 \text{ mod } 33=7$	7	G
F	6	$(6)^3 \text{ mod } 33=18$	18	R
1	28	$(28)^3 \text{ mod } 33=7$	7	G
1	28	$(28)^3 \text{ mod } 33=7$	7	G

Table 5. Decryption process of SSK

Cipher text	Integer value	$PT=(M*k1*k2) \text{ mod } 37$	Plain text
B	2	3	C
L	12	18	R
2	29	25	Y
W	23	16	P
A	1	20	T
J	10	15	O
G	7	29	2
R	18	27	0
G	7	29	2
G	7	29	2

5. RESULTS AND DISCUSSION

The proposed method in hybrid security is the combination of the familiar RSA and a novel simple symmetric key algorithm. We have compared our results with popular algorithms of 3DES, AES (Rijndael), Elliptic curve, and Robin method. As part of this comparison, different metrics are provided and performance is evaluated by encrypting input files containing different contents and message sizes. The algorithms were implemented in JAVA using their standard specifications and were tested using 300 bits of message length. Different algorithms require different memory spaces to perform the operation. Input data size and number of rounds determine how much memory an algorithm consumes.

Our study compares the proposed hybrid scheme to various existing algorithms on various metrics such as processing speed, encryption duration, decryption duration, key generation, number of rounds, and block size. The comparison metrics are given in Table 6. In addition, Table 7 demonstrates the encipher and decipher stages of SSK and RSA algorithms. Based on the metrics of 300-bit plain text size, the key generation analysis chart mentioned in Figure 2, the encryption comparison chart mentioned in Figure 3, and the decryption comparison graph are shown in Figure 4. The encryption chart demonstrates a novel hybrid technique that takes about the same amount of time to complete as RSA. It is superior to other schemes such as 3DES, AES, and Robin.

The advantage of this hybrid algorithm is that it is flexible and offers higher security than any other algorithm. It is a novel hybrid scheme with a robust RSA algorithm, so it is basically providing more security. Normally, any type of cryptography scheme depends on key management and the number of bits. There are many algorithms that provide effective security, but they do not satisfy the time consumption of applications. Therefore, RSA and elliptic curve cryptography (ECC) are still in use today and are used in many applications. Our proposed hybrid also provides the same sort of service with higher security.

Table 6. Comparison table

	3DES	AES	Robin method	Elliptic curve	RSA	RSA+SSK (Hybrid)
Key Generation (mSec)	8	14	16	12	6	7
Message length (bit)	300	300	300	300	300	300
Encryption (mSec)	9	7	9	7	6	6.5
Decryption (mSec)	8	7	12	6	5	5.5
Security	3	3.5	2.5	4	4	4.5
Key length (bit)	56 bits	128	256	112-256	4- 512	4-512
Block size	64 bits	128 bits	Variable	Variable	Variable	Variable

Table 7. Encryption/decryption analysis

	Encryption analysis		Decryption analysis	
Symmetric key	Key (3, -8)	BL2WAJGRGG	$(C)^3 \text{ mod } 33$	BL2WAJGRGG
RSA	$(P)^7 \text{ mod } 33$	2LQWAJ1F11	Key (25, 23)	CRYPTO2022

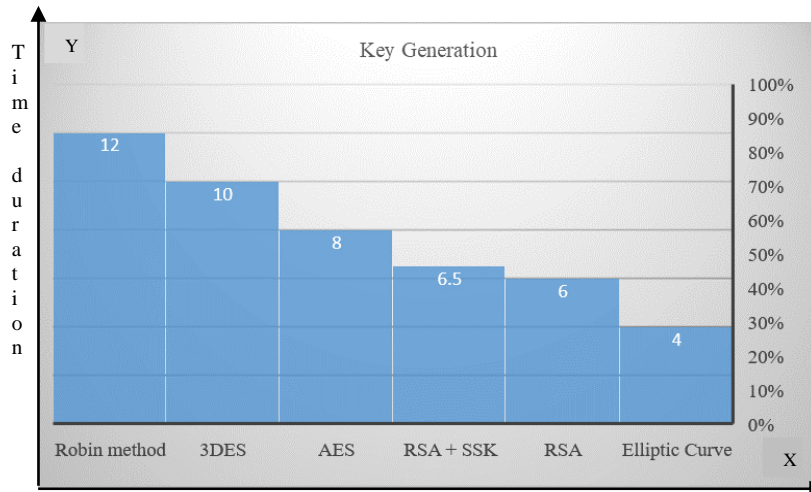


Figure 2. Key generation comparison

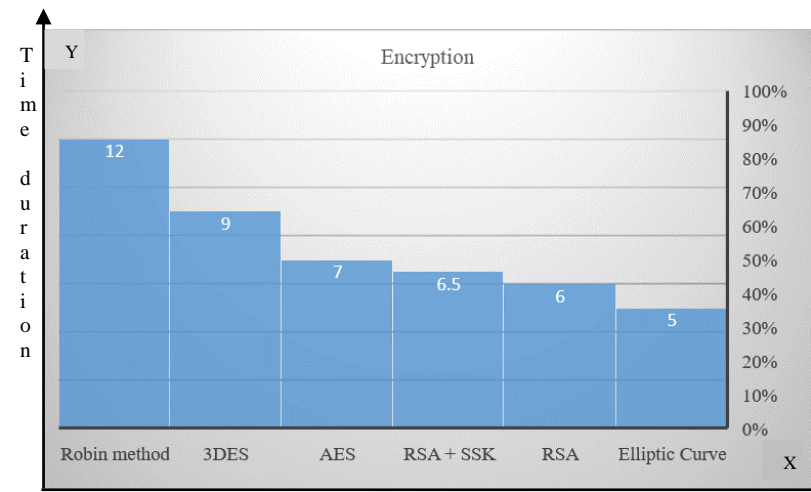


Figure 3. Encryption duration comparison

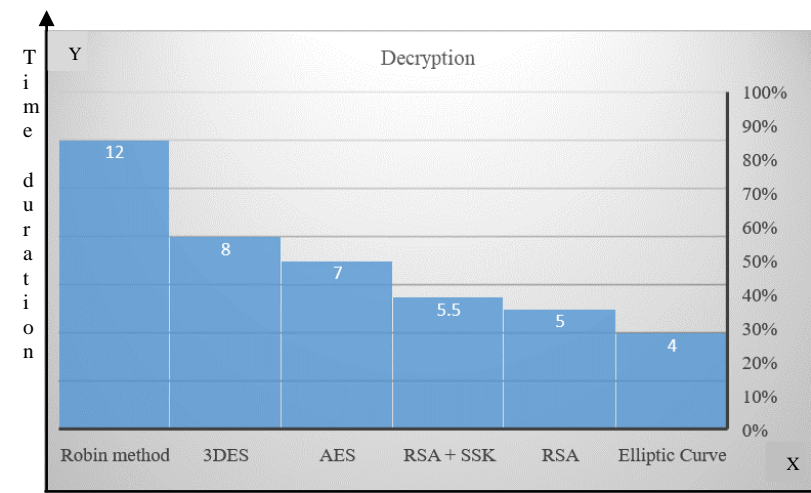


Figure 4. Decryption duration comparison

It is considered to be the most efficient algorithm that uses a small amount of memory, fast processing, and security. The security of our algorithm is strengthened by the standard RSA algorithm with a

symmetric key algorithm able to increase the template security strength. Cryptography is commonly constructed as a composition of primitives, like high generation, RSA, SHA-2, and AES. They are normally producing $(2)^{900}$ instances more than the other primitives, so it takes more processing time and security. 3DES algorithm that makes use of 48 sequences in its calculation using transpositions and substitutions with a key size of 168 bits. AES 128 makes use of 10 rounds, AES 192 makes use of 12 rounds, and AES 256 makes use of 14 rounds. Since there are more rounds, the encryption becomes more complicated, resulting in AES 256 being the most invulnerable AES version. Rabin method will realize it with a likelihood of $3/4$ at every round, so the common variety of Miller-Rabin rounds for a single non-prime subscription is $1+(1/4)+(1/16)+\dots=4/3$. For the 300 values, this ability is about 400 rounds of Miller-Rabin, relying on the chosen n .

As an alternative to elliptic curves, RSA boasts high numbers of its own. However, ECC has progressively developed in reputation recently because of its smaller key size and potential to maintain security. RSA is slow at 128-bit protection levels, which makes it more likely that a key operation such as signature era will not be successful. ECC uses a finite field to calculate the results. Because of this, elliptical curves are very recent developments, but the mathematical calculation involved in taking a discrete logarithm of older scheme. Most of these algorithms are simplified versions of factoring algorithms. In the proposed hybrid algorithm, 128 bits are processed in a single round, which produces similar results. Comparative analysis is presented in Table 8 in which RSA, ECC, and proposed hybrid schemes are shown as single-round algorithms.

Table 8. No. of processing round

Algorithm	128 bits (processing) (Round)
DES	16
3DES	48
AES	10
Robin	16
RSA	1
ECC	1
RSA+SSK	1

6. CONCLUSION

Public key cryptography and private key cryptography are combined in the hybrid cryptosystem. Combining two or more algorithms to enhance performance was developed as part of a hybrid algorithm technique. The sample of message bits chosen for the experiment was used to demonstrate how better solutions can be achieved in less time. This work proposes a hybrid cryptosystem that uses both symmetric keys and asymmetric cryptography. Any type of data that needs to be encrypted or decrypted requires a secure key. Among the most significant goals for cryptography system security designers is to satisfy security requirements. We propose a scheme for securing transactions based on the well-known public key RSA algorithm and a symmetric key algorithm, which are computed on simple integer numbers. Our results show that the hybrid method improves both the interacting performance and the security service of the desired data communication transactions. Based on experimental results, we identified several conclusive points. According to the results, security, and performance analysis discussed in the previous section, the proposed method consumes a reasonable amount of encryption and decryption time with better security than other alternative methods.





REFERENCES

- [1] F. Yao and J. Su, "Hybrid Encryption Scheme for Hospital Financial Data Based on Noekeon Algorithm," *Sec. and Commun. Netw.*, vol. 2021, Jan. 2021, doi: 10.1155/2021/7578752.
- [2] T. S. Ali and R. Ali, "A Novel Medical Image Signcrypton Scheme Using TLTS and Henon Chaotic Map," *IEEE Access*, vol. 8, pp. 71974–71992, 2020, doi: 10.1109/ACCESS.2020.2987615.
- [3] M. Sujithra, G. Padmavathi, and S. Narayanan, "Mobile Device Data Security: A Cryptographic Approach by Outsourcing Mobile Data to Cloud," *Procedia Computer Science*, vol. 47, pp. 480–485, Jan. 2015, doi: 10.1016/j.procs.2015.03.232.
- [4] A. Singh, M. Marwaha, B. Singh, and S. Singh, "Comparative Study of DES, 3DES, AES and RSA," *International journal of computers and technology*, vol. 9, no. 3, Jul. 2013, doi: 10.24297/ijct.v9i3.3342.
- [5] O. P. Akomolafe and M. O. Abodunrin, "A Hybrid Cryptographic Model for Data Storage in Mobile Cloud Computing," *International Journal of Computer Network and Information Security(IJCNIS)*, vol. 9, no. 6, pp. 53–60, Jun. 2017, doi: 10.5815/ijcnis.2017.06.06.
- [6] S. Manna, M. Prajapati, A. Sett, K. Banerjee, and S. Dutta, "Design and implementation of a two-layered hybrid cryptosystem," in *2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, Nov. 2017, pp. 327–331, doi: 10.1109/ICRCICN.2017.8234529.





- [7] K. Hosny, A. Taha, and D.-D. Salama, "An improved security schema for mobile cloud computing using hybrid cryptographic algorithms," *Far East Journal of Electronics and Communications*, vol. 18, no. 4, pp. 521–546, Apr. 2018, doi: 10.17654/EC018040521.
- [8] M. N. Praphul and K. R. Nataraj, "FPGA Implementation of Hybrid Cryptosystem," *International Journal of Emerging Science and Engineering (IJESE)*, vol. 1, no. 8, pp. 14–19, 2013.
- [9] Z. Wang, H. Dong, Y. Chi, J. Zhang, T. Yang, and Q. Liu, "Research and Implementation of Hybrid Encryption System Based on SM2 and SM4 Algorithm," in *Proceedings of the 9th International Conference on Computer Engineering and Networks*, Singapore, 2021, pp. 695–702, doi: 10.1007/978-981-15-3753-0_68.
- [10] Ü. Çavuşoğlu, S. Kaçar, A. Zengin, and I. Pehlivan, "A novel hybrid encryption algorithm based on chaos and S-AES algorithm," *Nonlinear Dyn*, vol. 92, no. 4, pp. 1745–1759, Jun. 2018, doi: 10.1007/s11071-018-4159-4.
- [11] S. Tariq, M. Khan, A. Alghafis, and M. Amin, "A novel hybrid encryption scheme based on chaotic Lorenz system and logarithmic key generation," *Multimed Tools Appl*, vol. 79, no. 31, pp. 23507–23529, Aug. 2020, doi: 10.1007/s11042-020-09134-8.
- [12] I. A. Shoukat, K. A. Bakar, and S. Ibrahim, "A Generic Hybrid Encryption System (HES)," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 5, no. 9, 2013, doi: 10.19026/rjaset.5.4793.
- [13] J. F. W. Herschel and S. F. O. LaCroix, "A Collection of Examples of the Applications of the Calculus of Finite Differences," UK: Nabu Press, 2011.
- [14] M. Iavich, S. Gnatyuk, E. Jintcharadze, Y. Polishchuk, and R. Odarchenko, "Hybrid Encryption Model of AES and ElGamal Cryptosystems for Flight Control Systems," in *2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC)*, Oct. 2018, pp. 229–233, doi: 10.1109/MSNMC.2018.8576289.
- [15] P. Li, J. Li, Z. Huang, C. Z. Gao, W. B. Chen, and K. Chen, "Privacy-preserving outsourced classification in cloud computing," *Cluster Computer*, vol. 21, pp. 277–286, 2018, doi: 10.1007/s10586-017-0849-9.
- [16] M. Hamdi, J. Miri, and B. Moalla, "Hybrid encryption algorithm (HEA) based on chaotic system," *Soft Comput*, vol. 25, no. 3, pp. 1847–1858, Feb. 2021, doi: 10.1007/s00500-020-05258-z.
- [17] S. Farooq, D. Prashar, K. Jyoti, "Hybrid Encryption Algorithm in Wireless Body Area Networks (WBAN)," *Advances in Intelligent Systems and Computing*, pp. 401–410, 2018, doi: 10.1007/978-981-10-5903-2_41.
- [18] N. Thillaiarasu, S. Chentur Pandian, G. Naveen Balaji, R. M. Benitha Shierly, A. Divya, and G. Divya Prabha, "Enforcing Confidentiality and Authentication over Public Cloud Using Hybrid Cryptosystems," in *International Conference on Intelligent Data Communication Technologies and Internet of Things (ICICI) 2018*, Cham, 2019, pp. 1495–1503, doi: 10.1007/978-3-030-03146-6_175.
- [19] Z. Cao and O. Markowitch, "Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 2, pp. 392–393, 1 Feb. 2021, doi: 10.1109/TPDS.2020.3021683.
- [20] K. R. Sajay, S. S. Babu, and Y. Vijayalakshmi, "Enhancing the security of cloud data using hybrid encryption algorithm," *J Ambient Intell Human Comput*, Jul. 2019, doi: 10.1007/s12652-019-01403-1.
- [21] P. Kuppuswamy and S. Q. Y. Al-Khalidi, "Implementation of security through simple symmetric key algorithm based on modulo 37," *International Journal of Computers and Technology*, vol. 3, no. 2, pp. 335–338, Oct. 2012, doi: 10.24297/ijct.v3i2c.2896.
- [22] F. Giacon, E. Kiltz, B. Poettering, "Hybrid Encryption in a Multi-user Setting," *Springer*, vol. 10769, pp. 159–189, 2018, doi: 10.1007/978-3-319-76578-5_6.
- [23] G. Viswanath, P. V. Krishna, "Hybrid encryption framework for securing big data storage in multi-cloud environment," *Evolution Intelligent*, vol. 14, pp. 691–698, 2021, doi: 10.1007/s12065-020-00404-w.
- [24] S. Bojjagani, V. N. Sastry, C. M. Chen, S. Kumari, M. K. Khan, "Systematic survey of mobile payments, protocols, and security infrastructure," *Journal of Ambient Intelligence and Humanized Computing*, 2021, doi: 10.1007/s12652-021-03316-4.
- [25] Y. -C. Chen, T. -H. Hung, S. -H. Hsieh and C. -W. Shiu, "A New Reversible Data Hiding in Encrypted Image Based on Multi-Secret Sharing and Lightweight Cryptographic Algorithms," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3332–3343, Dec. 2019, doi: 10.1109/TIFS.2019.2914557.

BIOGRAPHIES OF AUTHORS






Dr. Prakash Kuppuswamy     Department of Computer Engineering and Networks in Jazan University, KSA. Ph.D awarded by Dravidian University. He has published 30 International Research journals/Technical papers and participated in many international Conferences in Maldives, Libya and Ethiopia. His research area includes Cryptography, Bio-informatics and E-commerce security etc. Corresponding author. College of Computer Science and Information system, Jazan University. He can be contacted at email: pperumal@jazanu.edu.sa.






Dr. Saeed Bin Qasim Bin Yahya Al-Khalidi Al-Maliki     is a Professor, Department of Management Information System, at King Khalid University, Abha, KSA. He published many National and International papers, Journals. Also, he participated as a Reviewer in many international conferences worldwide. His research interests include: Information System development, approaches to systems analysis and the early stages of systems development process, IT/IS evaluation practices, E-readiness assessment. Doctor of Philosophy in Information Systems, 2006, College of Computer Science, University of East Anglia - Norge, UK. He can be contacted at email: salkhalidi@kku.edu.sa.






Dr. Rajan John    is Assistant Professor, Department of Computer Science, Jazan University, KSA. Ph.D awarded by Karunya University. He has published 20 International Research journals/Technical papers and participated in many international Conferences. He can be contacted at email: jose_rajana@yahoo.com



Mohammad Haseebuddin    Department of Computer Science, College of CS and IT, Jazan University, Jazan, KSA. Master Degree obtained from Osmania University, Hyderabad, India. Specialized in Cloud Computing and IoT. He can be contacted at email: mhaseebuddin@jazanu.edu.sa.



Ahamed Ali Shaik Meeran    Department of Information Technology, College of CS and IT, Jazan University, Jazan, KSA. Master Degree obtained from Andhra University, Visakhapatnam, A.P, India. Specialized in networks and Server Administration. He can be contacted at email: ameeran@jazanu.edu.sa.