Incorporating RSA with a New Symmetric-Key Encryption Algorithm to Produce a Hybrid Encryption System

Dr Prakash Kuppuswamy[1], Dr Saeed QY Al Khalidi[2], Dr Nithya Rekha Sivakumar[3]
prakashcnet@gmail.com, salkhalidi@yahoo.com, rekhasiva24@gmail.com
[1] Computer Networks Engineering Department, College of CS & IT, Jazan University, Jazan, KSA
[2] Department of Information science, King Khalid University, Abha, KSA
[3] Department of Computer Science & Engineering, Princes Nourah Bint Abdulrahman University, KSA

Abstract
The security of data and information using encryption algorithms is becoming increasingly important in today's world of digital data transmission over unsecured wired and wireless communication channels. Hybrid encryption techniques combine both symmetric and asymmetric encryption methods and provide more security than public or private key 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 proposed hybrid algorithm is a combination of the well-known 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.

Keywords:
Cryptography, Hybrid encryption algorithms, data security, information security, RSA.

1. Introduction

Cryptography is the art and science of secret writing, which cannot be achieved without the use of creative action and entrepreneurship [1-2][12]. It incorporates mathematical techniques as well as mechanisms related to information security, such as confidentiality, data integrity, entity authentication, and data provenance authentication [3] [10]. To achieve these goals, there are four major cryptographic techniques: Encryption, hash functions, Message Authentication Codes (MAC) and digital signatures [14,15]. Encrypting the content of a message so that it becomes unreadable to outsiders is called encryption. Once the message is encrypted, it is called ciphertext. The process of converting the ciphertext into plaintext is called decryption. The standard method of encryption and decryption involves the use of a key, and decryption can be done only when the key is known.

There are numerous encryption algorithms used in the field of information security. They can be divided into symmetric (private) and asymmetric (public) encryption techniques [9]. The encryption and decryption algorithms in a symmetric cryptosystem use the same key, while in an asymmetric cryptosystem the encryption and decryption algorithms use two different keys: an encryption key and a decryption key. Symmetric algorithms are cryptosystems in which a secret key is used for both encryption and decryption [4][11][17]. In symmetric cryptosystems, the algorithms are very resistant to possible attacks, but the brute force method to force the secret key is the major weakness. A symmetric algorithm is a shared distribution of the shared secret between two parties, such as the DES algorithm [4][5], which is the most important feature of any cryptosystem. [5].

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 private and public keys are used in this process. A public key is used for encryption and a private key is used for decryption [16]. When asymmetric algorithms are used, there is no need to share secrets between the parties as they use different values for encryption and decryption. 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 presented a method in which the sender and receiver did not have to share a secret. It was the first work on hybrid cryptosystems [3][17][6].

In recent years, technology and network tools have greatly changed the way people work and live. They are also exposed to significant risks 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 results are the same as 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 hybrid encryption method based on a new algorithm is proposed

Manuscript received January 5, 2024
Manuscript revised January 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.1.22

[12]. In both private and public sectors, the malicious activities on cyber infrastructure are increasing every day, and thus the security requirements are also increasing. There may be many issues related to security and protection of data during transmission. Therefore, we need an efficient and robust approach to ensure the secure transmission of sensitive data along with its authentication over public networks [13]. Combining two or more different algorithms into a single hybrid algorithm is motivated by the possibility that this new algorithm can perform better than any of its individual components. Consequently, hybrid algorithm techniques provide a new class of algorithms [23]. 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 [7] [22].

2. Related Study

Prakash Kuppuswamy, Dr. Saeed Q Y Al-Khalidi (2012) have proposed a new model of symmetric key algorithm. The purpose of this study is to investigate how to improve network security. It also aims to provide a better cryptographic mechanism for currently implemented techniques in a simple and powerful way. The researchers used module 37 and chose an arbitrary number. Then they used module 37 to calculate the inverse of the selected integer number. It is a necessity to distribute symmetric keys in a secure manner. The methods also studied the performance of the new SSK algorithm compared to other existing symmetric key algorithms [8].

Ijaz Ali Shoukat, Kamalrulnizam Abu Bakar, Subariah Ibrahim (2013) This study proposes a generic hybrid encryption system (HES) under a mutual committee of symmetric and asymmetric cryptosystems. Asymmetric cryptosystems (with public key) have several performance problems such as computational weakness, memory wastage, energy consumption and deployment limitations for large amount of data, but are quite secure and reliable in exchanging keys over insecure remote communication channels. Symmetric cryptosystems (private keys) are 100 times more efficient, but they are unable to account for non-repudiation, false secret key changes, forged ciphertext changes, and authentication of both parties' origins when exchanging information [9].

Sarbajit Manna, Mohit Prajapati, Ayan Sett, Kallol Banerjee, Saurabh Dutta (2017) To avoid interception of messages and the shared key in the middle, the authors have proposed a two-layer hybrid cryptosystem. So, the authors have introduced a hybrid cryptosystem which uses private key encryption model and public key combination model. The private key disclosure itself was encrypted using RSA public key encryption. The authors describe the advantages of the proposed scheme as better security since the shared key is intercepted during the exchange between sender and receiver, even if the intercepted key is not a valid key. The proposed algorithm is suitable for application to files and data transmission[19].

Maksim Iavich, Sergiy Gnatyuk, Elza Jintcharadze, Yuliia Polishchuk, Roman Odarchenko (2018), The authors propose to use a new hybrid combination model of AES and ElGamal encryption schemes to improve aviation security between ground and moving objects. Their goal was to demonstrate the effectiveness of the security of the new hybrid model. The authors defend the use of the new hybrid encryption algorithms by stating that the time required for data encryption is less than other hybrid encryption algorithms. This research article shows a comparative analysis and experimental results on the proposed system. They have evaluated the performance of AES encryption scheme, Elgamal encryption scheme and hybrid encryption scheme. The performance evaluation is done using Java language and compares the processing time of encryption and decryption with memory consumption. Finally, the authors believe that the newly proposed hybrid scheme provides more security than the previous versions [20].

Wang Z, Dong H, Chi Y, Zhang J, Yang T, Liu Q (2020) In this research article, the authors addressed mobile communication security to prevent message leakage, smartphone theft, and jamming. They developed a new hybrid model called SM2, a public key algorithm, and SM4, a symmetric key algorithm that provides double encryption. Based on their research, the paper shows better message security and effective key sharing [21].

Fei Yao (2021) The author focused on securing the financial data of the hospital sector. The author presented a hybrid encryption technique called Noekeon algorithm. It is based on RSA public key encryption method and DES algorithm. The author proposes that the message is encrypted twice in the encryption method. The algorithm is characterized by fast encryption speed, high encryption intensity and efficient encryption and decryption of a large amount of hospital financial data. The results are shown in the research article, better performance and higher security. Noekeon's model provides fast transfer and security of storage files. The author believes that the proposed model tries to avoid the inefficient properties of RSA algorithm when combined with DES to form a new Noekeon algorithm [12].

3. Proposed Algorithm

3.1 RSA & SSK tools

The symmetric key is implemented in two ways either as a block cipher or stream cipher. Block cipher transforms a fixed-length block of plaintext say a fixed size of 64 data into a block of ciphertext (encrypted text) 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. Here, in the newly developed symmetric key algorithm,
we introduce synthetic data, which is based on the user ID. Normally the synthetic data value consists of equivalent values of alphabets and numbers. Each alphabetical value is assigned an integer number, such as A = 1, B = 2, etc. Therefore, we consider integer value 0 to be 27 and 1 to be 28....9 to be 36, as well as the space value, which is 37. In Figure 1, the encryption and decryption processing structures are shown.

3.1.1 Generating the SSK keys

The modular multiplicative inverse is an integer 'x' such that.

$a\ x \cong 1 \pmod{m}$……………… ………..…………… (1)

The value of x should be in {1, 2, … m-1}, i.e., in the range of integer modulo m. The multiplicative inverse of "a modulo m" exists if and only if a and m are relatively prime (i.e., if gcd(a, m) = 1).

3.1.2 Generating the RSA keys

Select two large prime numbers, x and *y*. The prime numbers need to be large so that they will be difficult for someone to figure out.
Calculate $n = (x \text{ x } y)$.
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.
Use extended Euclidean algorithm to find *d* such that
$e.d{=}1 mod\ \phi(n)$………………………………............ (4)
The pair (*n*,*d*) makes up the private key [18].

3.1.3 Encryption

Given a plaintext *P*, represented as a number, the ciphertext *C* is calculated as:
$C{=}P^e$
$mod\ n$…………………………..…………………..(5)

3.1.4 Decryption

Using the private key (*n*,*d*), the plaintext can be found using:
$P{=}C^d\ mod\ n$……………………………..……………… (6)

Prime Generation and Integer Factorization
Modular Exponentiation and Roots

3.2 Key generation procedure of RSA and SSK

The RSA algorithm is based on the assumption that integer factorization is a difficult problem. This means that given a large value *n*, it is difficult to find the prime factors that make up *n*. It is most popular asymmetric key algorithm**.**

3.2.1 SSK

1) Select any two integer number likely one positive and negative say as n, n1
2) Find the inverse of the 'n' on modulo 37(key 1) say k.
3) Again find the inverse of n1 on modulo 37 say as k1.

3.2.2 RSA

1. Choose two very large random prime integers p and q
2. Compute n and φ(n):n = p*q and φ(n) = (p-1)(q-1)
3. Choose an integer e, 1 < e < φ(n) such that: gcd (e, φ(n)) = 1
4. Compute d, 1 < d < φ(n) such that: e*d ≡ 1 (mod φ(n))
5. Public key is (n, e) and the private key is (n, d)

3.3 Encryption method

1) Assign synthetic value for user message 'M'
2) Multiply synthetic value with random selected integer number n, n1
3) Calculate with modulo 37, C = (M* n*n1) mod 37
Ciphertext C1 = C^e (mod n), Now Encrypted text is "C1"

3.3 Decryption method

1) Multiply received text with key1 & key2
2) Calculate with modulo 37
3) Remainder is C = $(C1{*}n^{-1}{*}n1^{-1})$ mod 1
4) Revealed plain text or Message **M=** C^d (mod n)

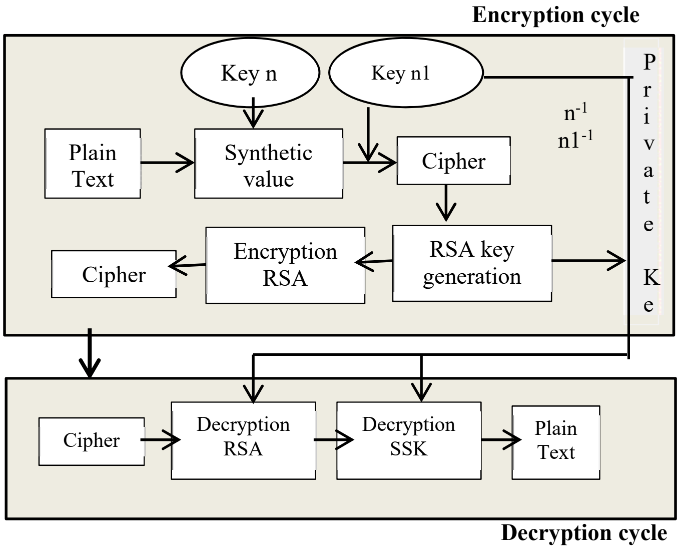

Figure 1. Encryption/Decryption cycle

4. Implementation

4.1 Algorithm

The procedure of Simple symmetric key algorithm and RSA algorithm is given below

4.1.1 Using SSK

Choose any random negative or positive integer → n, n1
Inverse of n, n1 mod 37→ k, k1 // SSK Key generation
Plaintext → M
C → (M *n *n1) mod 37 // SSK Encryption

4.1.2 Using RSA

Choose two prime numbers N→pq // RSA Key generation
Calculate φ(N) → (p-1) * (q-1) (Euler's totient function)
Randomly pick e so that gcd(e,φ(N)) → 1
validate e and φ(N) is relatively prime
identify d such that e*d →1 (modφ(N))
verify, d is the multiplicative inverse of e.
public key is → (e, N)
private key is → (d, N)

4.1.3 Encryption and Decryption

Encrypt C1 → C^e mod N // RSA Encryption
Decrypt (C) →$C1^d$ mod N // RSA Decryption
Plaintext M →(C*k*k1) mod 37 // SSK Decryption

Encryption is the formal name for scrambling programs. When plaintext or cleartext are unscrambled, they are transformed so that they are unintelligible to the outside observer. They are then called ciphertext or enciphered text. Using encryption security professionals can virtually nullify the value of an interception and the possibilities of effective modification and fabrication. Encryption is clearly addressing the need for confidentiality of data. Furthermore, it can be used to guarantee data integrity, that the data cannot be easily read or changed in a meaningful way. It is the basis of the protocol that enables us to provide security while accomplishing an incredibly vital system or network task. A protocol is an agreed-on sequence of actions that leads to desirable results. For example, some operating system protocols ensure the availability of resources as different tasks and users request them. Thus, encryption can also be thought of as supporting availability. That is, encryption is at the heart of methods for ensuring all aspects of computer security. 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

1) We are selecting random integer number n=3
2) Then inverse of 3=25(verification 3x25 mod 37=1) So, Key1=25
3) Again we are selecting random negative numbers n1= -8
4) Then inverse of –8 = 23 (verify -8 x 23=-184 mod 37 = 1) So, Key2 = 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 order to generate keys for the RSA algorithm, follow these steps
P=3; q=11; Therefore, n = 33 and Øn =20
Selecting 'e' =7 then inverse of 'e' or d =3 (verification 7*3 mod 20 =1)
Public key is e, n = 7, 33
Private key 'd' = 3

4.4 RSA Encryption

From the 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. The encryption result is shown in table 3, and it is encrypted with RSA public and private keys ($(m)^e$ mod n).

Table 3. Encryption process of RSA

B	2	$(2)^7$ mod 33 = 29	29	2
L	12	$(12)^7$ mod 33 = 12	12	L
2	29	$(29)^7$ mod 33 = 17	17	Q
W	23	$(23)^7$ mod 33 = 23	23	W
A	1	$(1)^7$ mod 33 = 1	1	A
J	10	$(10)^7$ mod 33 = 10	10	J
G	7	$(7)^7$ mod 33 = 28	28	1
R	18	$(18)^7$ mod 33 = 6	6	F
G	7	$(7)^7$ mod 33 = 28	28	1
G	7	$(7)^7$ mod 33 = 28	28	1

4.5 Decryption process of RSA & SSK

The decryption process of the hybrid scheme is described in Tables 4 and 5, where the private key ($(m)^d$ mod n) and the inverse of n, n1 is called k1, k2.

Table 4. Decryption process of RSA

2	29	$(29)^3$ mod 33 = 2	2	B
L	12	$(12)^3$ mod 33 = 12	12	L
Q	17	$(17)^3$ mod 33 = 29	29	2
W	23	$(23)^3$ mod 33 = 23	23	W
A	1	$(1)^3$ mod 33 = 1	1	A
J	10	$(10)^3$ mod 33 = 10	10	J
1	28	$(28)^3$ mod 33 = 7	7	G
F	6	$(6)^3$ mod 33 = 18	18	R
1	28	$(28)^3$ mod 33 = 7	7	G
1	28	$(28)^3$ mod 33 = 7	7	G

Table 5. Decryption process of SSK

Cipher Text	Integer Value	PT=(M*k1*k2) 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 & Discussion

The proposed method in hybrid security is the combination of the familiar RSA and Novel simple symmetric key algorithm. We have compared our results with popular algorithms such as 3DES, AES (Rijndael), Elliptic curve, Robin method, and proposed Hybrid encryption, which is all implemented, and their performance is compared by encrypting input files of varying contents and 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. The memory space required by any algorithm is determined on the basis of input data size and the number of rounds etc.

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 bit	128	256	112-256	4- 512	4-512
Block size	64 bit	128 bit	Variable	Variable	Variable	Variable

We compare the efficiency of the proposed hybrid scheme with various metrics such as processing speed, encryption duration, decryption duration, key generation, number of rounds, and block size with various existing algorithms. The comparison metrics are given in table 6. In addition, the encryption and decryption stages of SSK and RSA algorithms are shown in table 7. Based on the metrics of 300-bit plain text size, the key generation analysis chart mentioned in figure 3, encryption comparison chart mentioned in figure 3 and decryption comparison graph is 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.

Table 7. Encryption/Decryption analysis

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

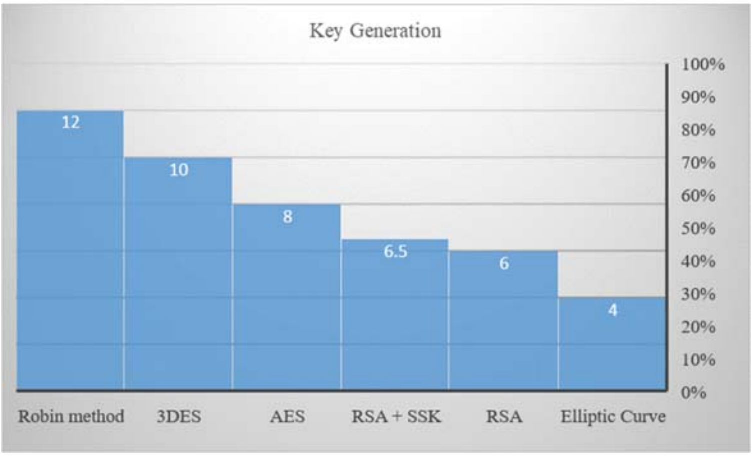

Figure 2. Key generation comparison

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 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.

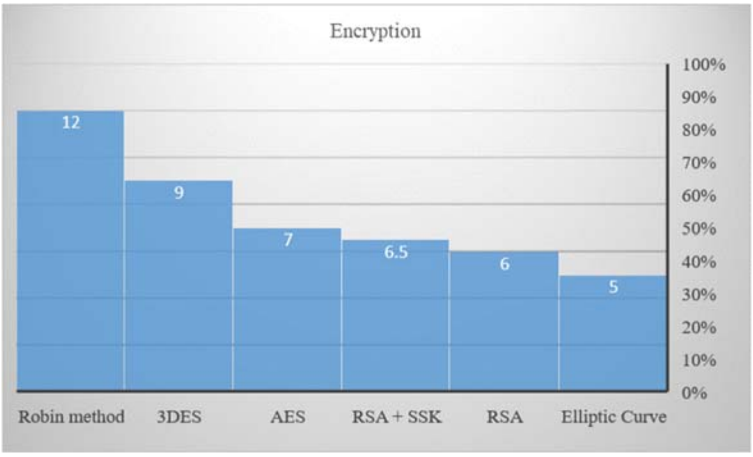

Figure 3. Encryption duration comparison

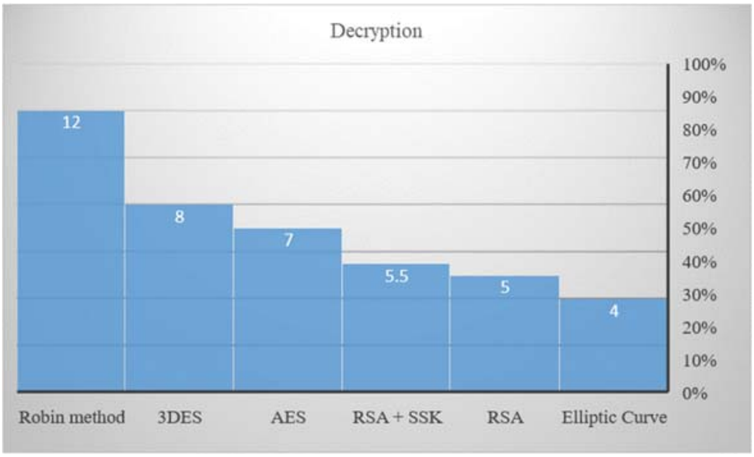

Figure 4. Decryption duration comparison

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 or Triple DES, however, was later changed to AES, which proved to be the strongest algorithm. 3DES is a block cipher that makes use of 48 rounds in its computation using transpositions and substitutions with a key size of 168 bit. 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)+... = 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 steadily grown in reputation over the past few years because of its smaller key size and potential to maintain security. When it comes to overall performance at 128-bit protection levels, RSA is typically stated to be slower than ECC for personal key operations such as signature era or key management. The hassle of ECC makes use of a finite field. Thus, the elliptical curves themselves are relatively new, but most of the math involved in taking a discrete logarithm over the area is older. In fact, most of the algorithms used are pretty minor editions of factoring algorithms. The proposed hybrid algorithm also produces similar results with 128 bit processing in a single round. Comparative analysis is presented in table.8 in which RSA, ECC, and proposed hybrid schemes are shown as single-round algorithms.

Manuscript received January 5, 2024
Manuscript revised January 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.1.22

Table 8. No. of processing round

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

6. Conclusion

The hybrid cryptosystem is a combination of public and private key cryptography. A novel hybrid algorithm technique based on the idea of mixing two or more algorithms for improved performance was developed. The goal of achieving better solutions in less time was demonstrated by using a sample of message bits chosen for the experimental result. This work proposes a hybrid cryptosystem that utilizes the benefit of both symmetric key and asymmetric cryptographic methods. For encryption and decryption of any data, a secure key is required. Satisfying security requirements is one of the most significant goals for cryptography system security designers. In this research article, the proposed scheme has been designed for securing transactions by using the well-known public key RSA algorithm and symmetric key algorithm, which is based on simple integer numbers. Experimental results show that the new hybrid method improves both the interacting performance and the security service for desired data communication transactions. Several points can be concluded from the experimental results. Based on the results, security, and performance analysis with various metrics as shown in table 7, it has been concluded that the proposed method consumes a reasonable amount of encryption and decryption time with better security than alternative methods.

References

(1) Journal:

[1] Willett M, "Cryptography old and new", *Science Direct Computers & Security*, pp. 177-186, 1982.

[2] Lin H S, "Cryptography and Public Policy", *Journal of Government Information*, pp. 135–148, 1998.

[3] Alia M.A, Yahya A, "Public–Key Steganography Based on Matching Method", *European Journal of Scientific Research*, pp. 223-231, 2010.

[4] Kumar S, Wollinger T, "Fundamentals of Symmetric Cryptography", *Embedded Security in Cars*, pp. 125-143, 2006.

[5] Burke J, McDonald J, Austin T, "Architectural support for fast symmetric-key cryptography", *Association for Computing Machinery*, Volume 34, pp 178–189, 2000.

[6] Mohapatra,P.K, "Public-Key Cryptography", *XRDS: Crossroads, The ACM Magazine for students*, Vol.7, 2000.

[7] Palanisamy V, Jeneba Mary A, "Hybrid cryptography by the implementation of RSA and AES", *International Journal of Current Research,*Vol. 33, Issue, 4, pp.241-244, April, 2011.

[8] Prakash Kuppuswamy, Saeed Q Y Al-Khalidi, "Implementation of security through simple symmetric key algorithm based on modulo 37", *Council for Innovative Research, International Journal of Computers & Technology*, www.ijctonline.com,ISSN:2277-3061, Volume 3 No. 2, OCT, 2012.

[9] Ijaz Ali Shoukat, Kamalrulnizam Abu Bakar, Subariah Ibrahim, "A Generic Hybrid Encryption System (HES)", *Research Journal of Applied Sciences, Engineering and Technology* 5(9): 2692-2700, ISSN: 2040-7459; e-ISSN: 2040-7467 Maxwell Scientific Organization, 2013.

[10] Praphul M.N, Nataraj K.R, "FPGA Implementation of Hybrid Cryptosystem", *International Journal of Emerging Science and Engineering (IJESE)* ISSN: 2319–6378, Volume-1, Issue-8, June 2013.

[11] Amritpal Singh, Mohit Marwaha, Baljinder Singh, Sandeep Singh , "Comparative Study of DES, 3DES, AES and RSA", *Council for Innovative Research International Journal of Computers & Technology*, Vol 9, No 3 www.cirworld.com, July 25, 2013.

[12] Fei Yao, "Hybrid Encryption Scheme for Hospital Financial Data Based on Noekeon Algorithm", *Security and Communication Networks*, Published 19 October 2021.

[13] Ali TS, Ali R, "A Novel Medical Image Signcryption Scheme Using TLTS and Henon Chaotic Map", in *IEEE Access*, vol. 8, pp. 71974-71992, 2020.

[14] Sujithra M, Padmavathi G, Narayanan S, "Mobile device data security: A cryptographic approach by outsourcing mobile data to cloud", *Procedia Computer Science*, vol. 47, pp. 480-485, 2015.

[15] Oladeji P. Akomolafe, Matthew O. Abodunrin, "A Hybrid Cryptographic Model for Data Storage in Mobile Cloud Computing", *I. J. Computer Network and Information Security*, Vol.6, pp. 53-60, 2017.

[16] Ali Abdulridha Taha, Diaa Salama Abd Elminaam, Khalid M. Hosny Far, "An improved security scheme for mobile cloud computing using Hybrid cryptographic algorithms", *East Journal of Electronics and Communications*, Volume 18, Number 4, 2018, Pages 521-546, 2018.

(2) Books:

[17] Schneier B, "Applied Cryptography", *New York: John Wiley & Sons*, 1996.

[18] Herschel, John Frederick William (1820), Book: "Part III. Section I. Examples of the Direct Method of Differences". A Collection of Examples of the Applications of the Calculus of Finite Differences. *Cambridge, UK: Printed by J. Smith, sold by J. Deighton & sons*. pp. 1–13 [5–6]. Accessed on 26/12/2021.

(3) Conference Proceedings:

[19] Sarbajit Manna, Mohit Prajapati, Ayan Sett, Kallol Banerjee, Saurabh Dutta, "Design and implementation of a two-layered hybrid cryptosystem", *International Conference on Security for Information Technology and Communications SECITC*, pp 85-96, 2017.

[20] Maksim Iavich, Sergiy Gnatyuk, Elza Jintcharadze, Yuliia Polishchuk, Roman Odarchenko, "Hybrid Encryption Model of AES and ElGamal Cryptosystems for Flight Control Systems", *IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control* (MSNMC), 2018.

[21] Wang Z, Dong H, Chi Y, Zhang J, Yang T, Liu Q, "Research and Implementation of Hybrid Encryption System Based on SM2 and SM4 Algorithm", Proceedings of the 9th International Conference on computer Engineering and Networks, *Advances in Intelligent Systems and Computing* Vol.1143, Springer July 2020.

[22] Thillaiarasu N, Chenthur Pandian S, Naveen Balaji G, Benitha Shierly M, Divya A, Divya Prabha G, "Enforcing Confidentiality and Authentication over Public Cloud Using Hybrid Cryptosystems", *International Conference on Intelligent Data Communication Technologies and Internet of Things* (ICICI), pp 1495-1503, 2018.

(4) Reports:

[23] Miroslaw Malek, Mohan guruswamy, Howard Owens, Minhir pandya, "A Hybrid Algorithm Technique" *Technical Report* -89-06, March 1989.