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

[1]Prakash Kuppuswamy, [2]Q.Y. Saeed Al Khalidi and [3]Nithya Rekha Sivakumar

*[1]Department Computer Networks Engineering, College of CS and IT, Jazan University, Jazan, Kingdom of Saudi Arabia*

*[2]Department of Information Science, King Khalid University, Abha, Kingdom of Saudi Arabia*

*[3]Department of Computer Science and Engineering, Princes Nourah Bint Abdulrahman University, Kingdom of Saudi Arabia*

OPEN ACCESS

**Key Words**
Cryptography, hybrid encryption algorithms, data security, information security, RSA

**Corresponding Author**
Prakash Kuppuswamy
*Department of Computer Network and Engineering, College of CS and IT, Jazan University, Jazan, Kingdom of Saudi Arabia*

**Received:** 18 March 2022
**Accepted:** 25 March 2022
**Published:** 16 Aught 2022

**Citation:** Prakash Kuppuswamy, Q.Y. Saeed Al Khalidi and Nithya Rekha Sivakumar, 2023. Incorporating RSA with a New Symmetric-Key Encryption Algorithm to Produce a Hybrid Encryption System. Res. J. Applied Sci., 17: 7-14, doi: rjas.2022.7.14

## 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 combined encryption scheme of either two symmetric key or both of 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 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.

## 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[1-3]. It incorporates mathematical techniques as well as mechanisms related to information security or data security. Data security provides individual user's data privacy, confidentiality, data integrity and data provenance authentication[4,5]. To achieve these goals, there are four major cryptographic techniques: Encryption, hash functions, message authentication codes (MAC) and digital signatures[6,7]. In the cryptography, encrypting mode is the content of a message that it becomes unreadable format to outsiders. Once the message is encrypted, it is called ciphertext. The technical process of transforming the ciphertext into plaintext 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 to cryptosystems that use the same key to encrypt and decrypt. Asymmetric cryptosystem the method of encipher and decipher procedure uses two different key: An encryption key and a decryption key[8-10]. 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 mutual distribution of the collective secret between two users, such as the DES algorithm[8,11], which is the most important feature of any cryptosystem[11].

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. The encryption technique uses public key and a private key is used for decryption[12]. When asymmetric algorithms are used, there is no need to share secrets between the parties as they use different values for encryption procedure 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. Whitfield Diffie and Martin Hellman developed the first hybrid system in 1976 in which the sender and receiver did not have to share secrets. It was the first work on hybrid cryptosystems[3,4,10].

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 outputis the similar 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 new hybrid encryption model is proposed[13]. 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. Hence, eventually required an efficient and robust approach to ensure the secure transmission of sensitive data along with its authentication over public networks[14]. 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[15]. 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[16,17].

## RELATED STUDY

Schneier[18] have proposed a new model for symmetric key algorithms. The purpose of this study is to investigate ways to improve network security. It also aims to provide a simple and powerful cryptographic mechanism for currently implemented techniques. Module 37 was used and an arbitrary number was chosen by the researchers. Using module 37, they calculated the inverse of the selected integer number. Providing symmetric keys in a secure manner is essential. In addition, the article evaluated the enactment of the new Simple Symmetric key algorithm against other existing symmetric key algorithms.

William[19] discuss the design of a new hybrid encryption system as a grouping of public-key and private-key cryptosystems. Asymmetric cryptosystems (with the public keys) have several performance problems such as computational weakness, memory waste, energy consumption and deployment limitations for a large amount of data but they are fairly reliable and secure when exchanging keys over insecure remote communication channels. Despite their efficiency (private keys), symmetric cryptosystems are not capable of providing non-repudiation, false secret key changes, forged ciphertext changes and authentication of both parties' origins.

Manna *et al.*[20] 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. Encryption of the private key disclosure itself was performed using 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 sender and receiver. Data transmission and files can be handled by the proposed algorithm.

To improve aviation security between moving objects and ground objects, the authors propose a hybrid combination of AES and ElGamal encryption schemes. The purpose of their study was to demonstrate the effectiveness of the hybrid model's security. By stating that their new hybrid encryption algorithms take less time than other hybrid encryption algorithms, the authors defend the use of their new hybrid encryption algorithms. An analysis of comparative results on the proposed system is presented in this research article. In order to evaluate the hybrid encryption scheme, comparisons were made and evaluated with the existing algorithms. These algorithms included AES encryption, Elgamal encryption and the AES encryption scheme. In this performance evaluation, we compare the encrypting and decrypting times and memory consumption using Java language. Finally, the authors believe that the hybrid scheme provides greater security than previous versions[21].

This study discusses how to prevent message leakage, smartphone theft and jamming of mobile communications. The researchers developed a hybrid algorithm known as SM2, which uses public key algorithms and SM4, which uses symmetric key algorithms. In the study, the authors demonstrate that messaging is more secure and key sharing is more effective[22].

Alia and Yahya[3] 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 amount 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.

## PROPOSED ALGORITHM

**RSA and SSK tools:** There are two ways to implement symmetric keys: Block ciphers or stream ciphers. 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 asnumeric value, such as alphabet A is 1, B is 2 and so on. In addition to that, we consider integer value 0 is known as 27 and 2 is 28 and finally 9 is assigned 36, as well as the space value, which is 37. In Fig. 1, the encrypt and decrypt procedure were as follows:

**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).

**Generating the RSA keys:** It is important that the chosen prime numbers are large so that someone will have trouble figuring them out:

$$\text{Calculate } n = (x\times y)$$

Use totient function to find out the value of:

$$\varphi(n) = (=x-1)(y-1) \tag{2}$$

Select an integer e, such that e is:

$$\text{co-prime to } \varphi(n) \text{ and } 1<e<\varphi(n) \tag{3}$$

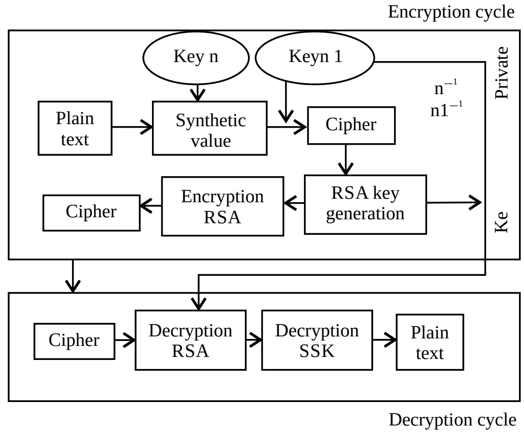

Fig. 1: Encryption/decryption cycle

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

Identify ‘d’ with using extended Euclidean algorithm that:

$$e.d = 1 \bmod \varphi(n) \tag{4}$$

The pair (n,d) marks up the private key[23]

**Encryption:** Given a plaintext P is represented as a number, the ciphertext C is calculated as:

$$C = P^{e} \bmod n \tag{5}$$

**Decryption:** The plaintext or sender’s message can be obtained using the private key (n,d):

$$P = C^{d} \bmod n \tag{6}$$

**Key generation procedure of RSA and SSK:** The RSA algorithm scheme is constructed on the assumption that integer factorization is a difficult problem. It means that given a large value n, it is hard to identify the prime factors that make up n. It is most popular asymmetric key algorithm.

**SSK:**

- Select any two integer number likely one positive and negative say as n, n1
- Find the inverse ofthe ‘n’ onmodulo 37(key 1) say k
- Again calculate the inverse of n1 on modulo 37 say as k1

**RSA:**

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

**Encryption method:**

- An alphabetical equivalent integer synthetic value assigned to user message‘M’
- Multiply syntheticvalue with random selected integer number n, n1
- Evaluate with modulo 37, C = (M*n*n1) mod 37
- CiphertextC1 = $C^{e}$ (mod n), Now Encrypted text is “C1”

**Decryption method:**

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

## IMPLEMENTATION

**Algorithm:** Following is a description of the Symmetric Key Algorithm based on integer numbers and the RSA algorithm.

**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

**Using RSA:**

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

**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 technique is known as scrambling programs. When plaintext or message are unscrambled, it is very easy to identified by the intruder even in binary format of the message, so that is required scrambled encryption mode. They are then called ciphertext or enciphered text. The usage of encrypting the text on security professionals can virtually reverse the value of an interception and the possibilities of effective alteration and fabrication of sender’s message. 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. Computer security can also be assured through encryption procedures that support availability and 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 |

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 |

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 |

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 |

**Key generation of SSK:**

- Selecting random integer number n = 3
- Then inverse of 3 = 25(verification 3×25 mod 37 = 1) So, Key1 = 25
- Again, selecting random negative numbers n1 = -8
- Then the inverse of -8 is known as 23(verify -8×23 = -184 mod 37 = 1) So, Key2 = 23, Here is the encryption process using SSK shown in Table 2.

**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

**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).

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

## RESULTS AND DISCUSSION

The proposed method in hybrid security is the combination of the familiar RSA and Novel simple symmetric key algorithm. We have compared our

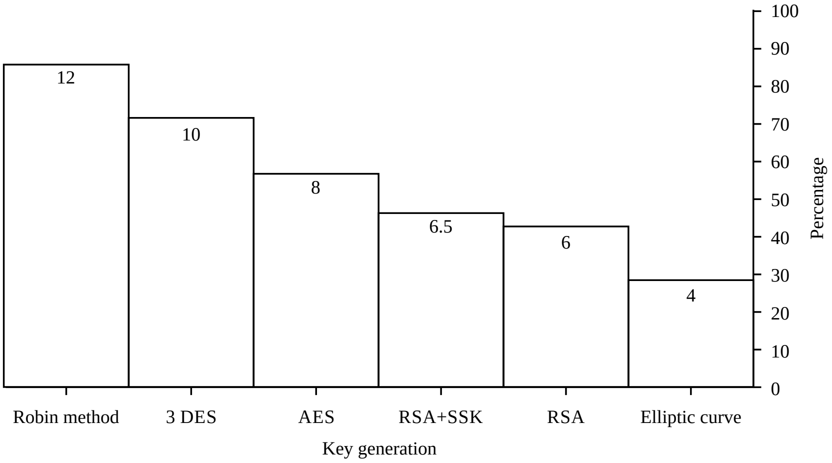

Fig. 2: Key generation comparison

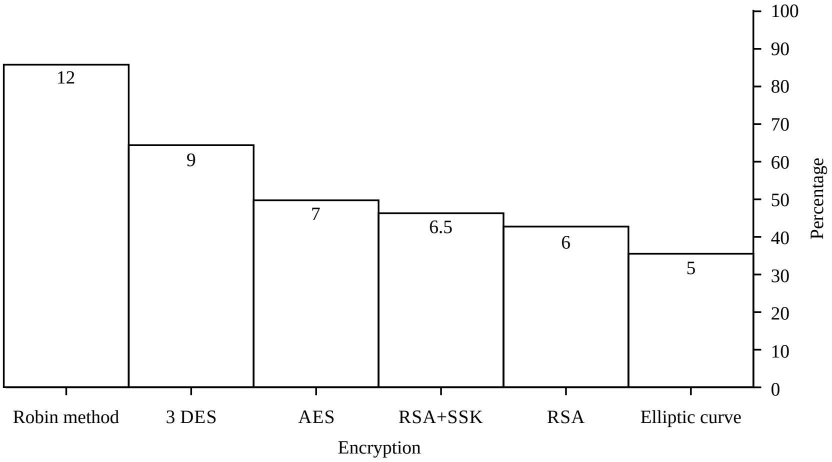

Fig. 3: Encryption duration comparison

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 |

Table 7: Encryption/decryption analysis

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

results with popular algorithms of 3DES, AES (Rijndael), Elliptic curve, 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 Fig. 2, encryption comparison chart mentioned in Fig. 3 and decryption comparison graph is shown in Fig. 4. The

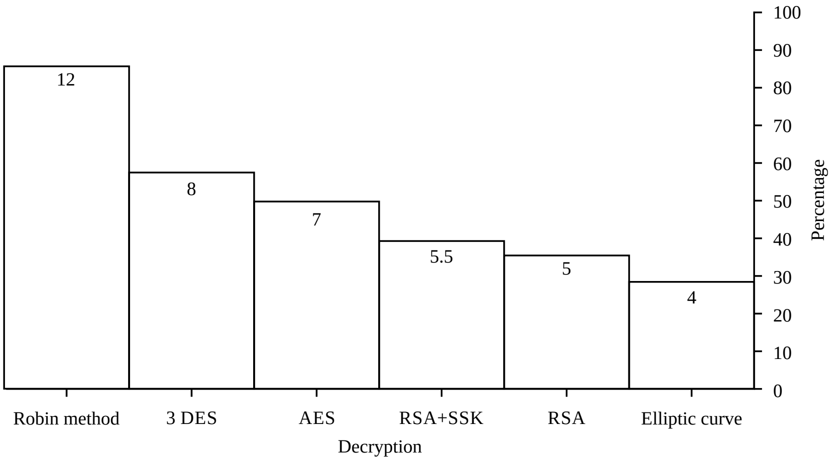

Fig. 4: Decryption duration comparison

Table 8: Number 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 |

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 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.

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. The 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, Elliptic Curve Cryptography (ECC) has progressively developed in reputation recently because of its smaller key size and potential to maintain security. The 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 math involved in taking a discrete logarithm is actually much older. 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.

## CONCLUSION

Public key cryptography and private key cryptography are combined in the hybrid cryptosystem. The concept of combining two or more algorithms to enhance performance was developed as part of a hybrid algorithm technique. A sample of message bits chosen for the experiment was used to demonstrate how better solutions can be achieved in less time. This study proposes a hybrid cryptosystem that uses both symmetric keys and asymmetric cryptography. Any 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 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 the experimental results, we identified several conclusive points. According to the results, security and performance analysis as shown in Table 7, the proposed method consumes a reasonable amount of encryption and decryption time with better security than other alternative methods.

## REFERENCES

1. Willett, M., 1982. Cryptography old and new. Comput. Secur., 1: 177-186.
2. Lin, H.S., 1998. Cryptography and public policy. J. Gov. Inform., 25: 135-148.
3. Alia, M.A. and A.A. Yahya, 2010. Public–key steganography based on matching method. Europ. J. Sci. Res., 40: 223-231.
4. Kumar, S. and T. Wollinger, 2006. Fundamentals of Symmetric Cryptography. In: Embedded Security in Cars., Lemke, K., C. Paar and M. Wolf, (Eds.)., Springer-Verlag, Berlin/Heidelberg, ISBN-10: 3540283846, pp: 125-143.
5. Burke, J., J. McDonald and T. Austin, 2000. Architectural support for fast symmetric-key cryptography. ACM SIGARCH Comput. Architecture News, 28: 178-189.
6. Mohapatra, P.K., 2000. Public key cryptography. XRDS: Crossroads, ACM Mag. Students, 7: 14-22.
7. Palanisamy, V. and A.J. Mary, 2011. Hybrid cryptography by the implementation of RSA and AES. Int. J. Curr. Res., 3: 241-244.
8. Kuppuswamy, P. and D.S.Q.Y. Al-Khalidi, 2012. Implementation of security through simple symmetric key algorithm based on modulo 37. Int. J. Comput. Technol., 3: 335-338.
9. Shoukat, I.A., K.A. Bakar and S. Ibrahim, 2013. A generic hybrid encryption system (HES). Res. J. Applied Sci., Eng. Technol., 5: 2692-2700.
10. Praphul, M.N. and K.R.Nataraj, 2013. FPGA implementation of hybrid cryptosystem. Int. J. Emerg. Sci. Eng., 1: 14-19.
11. Singh, A., M. Marwaha, B. Singh and S. Singh, 2013. Comparative study of DES, 3DES, AES and RSA. CIRWOLRD, Int. J. Comput. Technol., 9: 1162-1170.
12. Yao, F., 2021. Hybrid encryption scheme for hospital financial data based on noekeon algorithm. Secur. Commun. Networks, Vol. 2021. 10.1155/2021/7578752.
13. Ali, T.S. and R. Ali, 2020. A novel medical image signcryption scheme using TLTS and henon chaotic map. IEEE Access, 8: 71974-71992.
14. Sujithra, M., G. Padmavathi and S. Narayanan, 2015. Mobile device data security: A cryptographic approach by outsourcing mobile data to cloud. Procedia Comput. Sci., 47: 480-485.
15. Akomolafe, O.P. and M.O. Abodunrin, 2017. A hybrid cryptographic model for data storage in mobile cloud computing. Comput. Net. Inf. Secur., 6: 53-60.
16. Taha, A.A., D.S.A. Elminaam and K.M. Hosny, 2018. An improved security schema for mobile cloud computing using hybrid cryptographic algorithms. Far East J. Electrons. Commun., 18: 521-546.
17. Schneier, B., 1996. Applied Cryptography. 2nd Edn., John Wiley & Sons, New York, ISBN-10: 0471128457, Pages: 1027.
18. William, H.J.F., 2010. A Collection of Examples of the Applications of the Calculus of Finite Differences. J. Smith and Sold by J. Deighton & Sons, California, ISBN-10: 0341908185, Pages: 171.
19. Manna, S., M. Prajapati, A. Sett, K. Banerjee and S. Dutta, 2017. Design and Implementation of a Two-Layered Hybrid Cryptosystem. 2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), November 03-,December 05, 2017, IEEE, India, pp: 327-331.
20. Iavich, M., S. Gnatyuk, E. Jintcharadze, Y. Polishchuk and R. Odarchenko, 2018. Hybrid Encryption Model of AES and ElGamal Cryptosystems for Flight Control Systems. 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC), October 16-,December 18, 2018, IEEE, Ukraine, pp: 229-233.
21. Wang, Z., H. Dong, Y. Chi, J. Zhang, T. Yang and Q. Liu, 2020. Research and Implementation of Hybrid Encryption System Based on SM2 and SM4 Algorithm. Proceedings of the 9th International Conference on Computer Engineering and Networks, Springer Singapore, Singapore, pp: 695-702.
22. Thillaiarasu, N., S.C. Pandian, G.N. Balaji, R.M.B. Shierly, A. Divya and G.D. Prabha, 2018. Enforcing Confidentiality and Authentication over Public Cloud Using Hybrid Cryptosystems. International Conference on Intelligent Data Communication Technologies and Internet of Things (ICICI) 2018, October 21-21, 2018, Springer, Cham, pp: 1495-1503.
23. Malek, M. and M. Guruswamy, 1989. A hybrid algorithm technique. University of Texas at Austin Computer Science Dept. Taylor Hall 2.124 Austin, TXUnited States, https://dl.acm.org/doi/10.5555/898987.