**Iraqi Journal of Communications and Computer Networks**
**e-ISSN: 3105-9252, p-ISSN: 3105-9244**
**Vol. (1), Iss. (1), September 2025**
**DOI: https://doi.org/10.58564/IJCCN.1.1.2025.6**

https://ijccn.net/ **Research Article**

# Reliable RSA Cryptosystem Using the Path Tracing Method

Ruma Kareem K. Ajeena [1*], Ban Jasim Kadim [2]

[1] Prof. Dr., Department of Computer Science, College of Education for Pure Science Ibn Al- Haitham, University of Baghdad & Scientists Foundation for Development, Baghdad, Iraq
[2] Researcher, Department of Mathematics, College of Education for Pure Science, University of Babylon, Babil, Iraq

***Corresponding Author:** ruma.k.kh@ihcoedu.uobaghdad.edu.iq, scientists.ffd2019@gmail.com

**Citation:** Ruma Kareem K. Ajeena, & Ban Jasim Kadim. (2025). Reliable RSA Cryptosystem Using the Path Tracing Method. Iraqi Journal of Communications and Computer Networks (IJCCN), 1(1), 52–61.

ARTICLE INFO

Received: 03 Mar. 2025
Revised: 15 May 2025
Accepted: 22 Jun. 2025

ABSTRACT

The reliability theory has many applications in different areas, in mathematics, engineering, manufacturing the devices, computer scinace and cryptography as well . A reliable cryptosystem: type RSA has been proposed in 2 dimension. The plaintext $M$ has been divided into two parts $m_1$ and $m_2$ in the proposed reliable RSA cryptosystem (R-RSA). Sub-ciphertexts ($C_1$, $C_2$) and ($C_1$', $C_2$') form two paths which are corresponding to the parts $m_1$ and $m_2$ respectively. The encrypted plaintext is designed as a reliable system which considers a new main point in this work. The encryption and decryption processes on the proposed R-RSA cryptosystem are done uses the path tracing method (PTM) and parallel series reduction method (PSRM). A study case of the R-RSA cryptosystem is discussed as a new experimental result. The security issues on R-RSA cryptosystem are determined. A more secure R-RSA cryptosystem has been designed for communication in compare to other previous cryptosystems.

**Keywords:** Cryptography, RSA cryptosystem, Reliability, R-RSA, Security.

## INTRODUCTION

Cryptography is employed to protect the information based on the various techniques. Some techniques are depended on Algebra, especially matrix algebra or linear algebra or abstract algebra [1-4]. Another direction of methods focuses on using Diophantine equations especially elliptic curves [5-8]. The graph and optimization theories also are used to design several cryptographic schemes [9,10]. On the other hand, some encryption schemes are formed using the reliability theory. The reliability [11] is the probability that a system performs satisfactorily for a time period with some conditions.

## LITERATURE REVIEW

For information transmission, the integral aspects are reliability and security. Several researchers in their work to increase these aspects. Some coding theory and cryptographic techniques are achieved with largely reliability [12]. In 2014, S. Xiao et al. [13] introduced the evaluation and estimation of the performance of key management schemes (KMSs) based on the reliability theory. The analysis of reliability showed the KMSs concentrate on postponing the key theft as well as possible directions to improve the reliability of KMSs. In 2017, S. Subramanian et al. [14] presenting two block ciphers which are used for authenticated encryption algorithms. In 2023, B. Kadim and R. Ajeena [15] proposed the reliable El-Gamal cryptosystem (R-EPKC) using the PTM. Also, in 2024, the same authors [16] used the modified decomposition method (M-DM) to design reliable Rabin cryptosystem (R-RPKC).

This work proposes using the PTM for computing the proposed R-RSA public key cryptosystem. On the proposed cryptosystem, the plaintext $M$ is divided into parts. The ciphertext $C$ of $M$ is done and represents as two paths

$C_1$ and $C_2$ using the PTM. The decryption process is computed to recover the original plaintext based on the series-parallel reduction method (SPRM).

The outline of this work includes: Some reliability systems which are series, parallel and parallel-series systems. Also, some reliable methods of the complex system is discussed, especially the PTM and SPRM. The R-RSA public key cryptosystem is proposed as a new contribution in this work. A study case of R-RSA cryptosystem has been presented as a new experimental result. The R-RSA cryptosystem security issue is determined. The conclusions of this research work is drown.

## SOME RELIABILITY SYSTEMS

This section presents some fundamental facts and concepts related to the reliability systems. There are several reliability systems, some of them are discussed as follows.

### Series Systems

The success or failure of full system can be determined based on the components of it. With the failure of one or more than one component in the system and the result is a failure then the system is named by series system (SS) [18], see Figure (1).


**Figure 1.** A series system.

This means that, all components of the system work, so the system success to perform the function that designed for it. Let SS has n mutually independent components. The failure of one component, with mutually independence property, is not affecting on the life of the rest components. The parameters that can be used are: $S_i$ is the event (path) with component i that is operational, S is the path of the system, R(t) is the system reliability and Ri(t) indicates to the reliability of component *i*. The system reliability is determined based on the probability by

$$R= P(S) = P(S_1 \cdot S_2 \cdot \dots \cdot S_n). \quad (1)$$

Since the components are independent, so

$$R= P(S) = P(S_1) \cdot P(S_2) \cdot \dots \cdot P(S_n) = \prod_{i=1}^{n} R_i. \quad (2)$$

The system reliability is

$$R = R_0^n, \quad (3)$$

when all n components be identical to the reliability $R_o$.

### Parallel Systems

If the failure of full system occurred depending on the failure that obtained all components of the system, then there is a parallel system (PS) [18] that is shown in Figure (2).

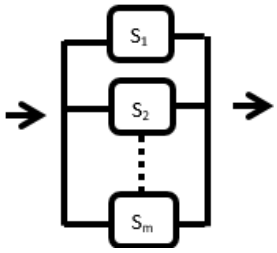



**Figure 2.** A Parallel System (PS).

In general, the reliability of a PS can be computed as follows. With m components of a parallel system which are mutually independent components. The system unreliability F (failure probability) is expressed by

$$F = P(\bar{S}) = P(\bar{S}_1 \cdot \bar{S}_2 \cdot \dots \cdot \bar{S}_m), \quad (4)$$

where is the complement element of S. Since the event (path) are mutually impendent then F in Equation (4) is rewritten by

$$F = P(\bar{S}) = P(\bar{S}_1) \cdot P(\bar{S}_2) \cdot \dots \cdot P(\bar{S}_m) = \prod_{i=1}^{m}(1 - R_i). \quad (5)$$

The unreliability components system gives the reliability system, namely

$$R = \prod_{i=1}^{m}(1 - R_i). \quad (6)$$

The identical of all components m leads to

$$R = 1 - (1 - R_i)^m \quad (7)$$

### Parallel–Series System

The parallel connection of the n disjoint paths with path i has mi connected components in series for $1 \le i \le n$ forms a parallel–series system (PSS) [17]. The diagram of PSS reliability is shown in Figure (3).

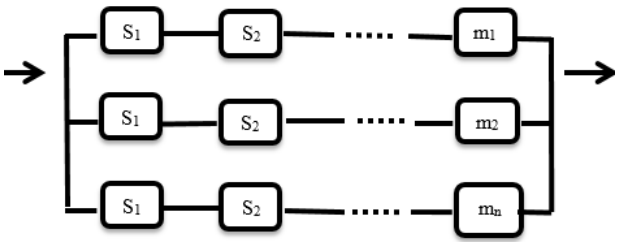



**Figure 3.** A PSS.

In the PSS, the components are not in common are available in n minimal paths. Each path reliability considers as a function of its component reliabilities.

- $p_{ij}$ : reliability of component j in path i, $1 \le i \le n$, $1 \le j \le m_i$
- $q_{ij}$: $1 - p_{ij}$, $1 \le i \le n$, $1 \le j \le m_i$

The reliability of path i is

$$P_i = \prod_{j=1}^{m_i} P_{ij}, i = 1, \dots, n. \quad (8)$$

The PSS reliability is

$$R_s = 1 - \prod_{i=1}^{n}(1 - P_i) = 1 - \prod_{i=1}^{n}(1 - \prod_{j=1}^{m_i} P_{ij}). \quad (9)$$

The system's reliability is

$$R_s = 1 - (1 - P_m)^n, \quad (10)$$

with the distributed components are independent and identically and they have reliability pi j = p as well as the components number in each path is constant, namely $m_i = m$.

## SOME RELIABIE METHODS

Two reliable methods are discussed as follows.

### Path Tracing Method

On PTM [18], each path from a starting into an ending can be considered. From one end to the other in the reliability block diagram at least one path available. As well, from the beginning of the path to the end of it at least one path is available that the success of a system determines. So, it does not failed system is available as given in Figure (4)

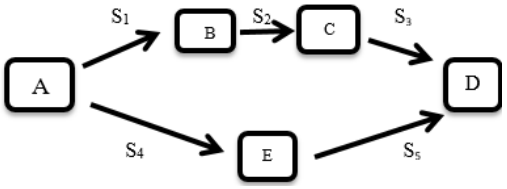



**Figure 4.** A complex system.

that has two paths which cannot fail as given in Figure (5).

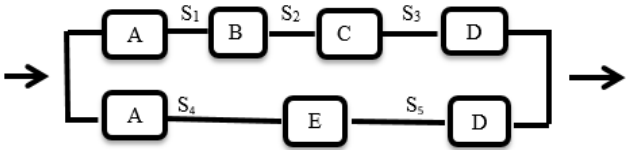



**Figure 5.** Parallel-series system.

The paths in Figure (5) are: $P_1 = S_1\text{-}S_2\text{-}S_3$ and $P_2 = S_4\text{-}S_5$. The series paths reliability $Rs_j$ with j=1,2 is calculated based on the reliability Ri of subsystems $S_i$ for i=1,...,5. So, the reliability is

$$Rs_j = \prod_{j=1}^{n} R_j, \text{ where n is the subsystems number } S_i \text{ in path } P_j.$$

Using Figure (5), series paths reliabilities are

$$Rs_1 = R_1R_2R_3 \text{ and } Rs_2 = R_4R_5.$$

The parallel system reliability $R_p$ is

$$R_p = 1 - \prod_{j=1}^{m}(1 - Rs_j), \text{ with the paths number is m.}$$

$Rs = 1\text{-}[(1\text{-}Rs_1)\ (1\text{-}Rs_2)]$

$= 1\text{-}[1\text{-}(R_1R_2R_3)(1\text{-}R_4R_5)]$

$= R_4R_5 + R_1R_2R_3 - R_1R_2R_3R_4R_5.$

## Series-Parallel Reduction Method

The complex system reliability in Figure (4) can be described as a SPS by

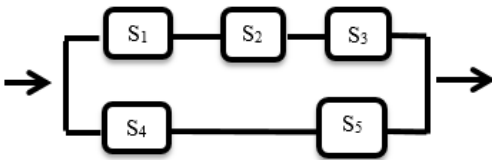



**Figure 6.** A series-parallel system.

In Figure (6), five components $S_i$, for i = 1,...,5 are available. The component S reliability $R_i$. The system reliability can be evaluated using the SPRM. Based on Figure (6), a super-component $S_a$ has $S_1$, $S_2$ and $S_3$ components which form a series subsystem. The super-component reliability is given by

$$R_a = R_1\ R_2R_3.$$

Another series subsystem of a super-component $S_b$ has been formed by the components $S_4$ and $S_5$. The super-component reliability is

$$R_b = R_4R_5.$$

The series reductions in Figure (6) based on the super-components $S_a$ and $S_b$ can be expressed in Figure (7).

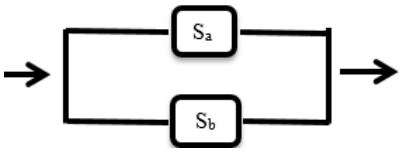



**Figure 7.** The $S_a$ and $S_b$ as series reductions.

The parallel system reliability Rs of $S_a$ and $S_b$ is computed by

$$R_s = 1 - \prod_{j=1}^{m}(1 - Rs_j), \text{ where m is the paths number.}$$

The super-components $S_a$ and $S_b$ form a parallel subsystem $S_c$. The reliability $R_c(t)$ is

$R_c = 1-[(1-R_a)(1-R_b)]$

$= R_a + R_b - R_aR_b = R_1R_2R_3 + R_4R_5 - R_1R_2R_3R_4R_5.$

Figure (8) shows the parallel reduction reliability that given in Figure (7).


**Figure 8.** The $S_a$ and $S_b$ as parallel reduction.

## THE RELIABLE CRYPTOSYSTEM: TYPE RSA

The 2-dimension cryptosystem: type RSA (R-RSA) has proposed. First user selects the domain parameters: $p_i$ and $q_i$ for i =1,2 are large secret primes and $e$ is a public encryption exponent with the property that gcd(e,($p_i$-1)($q_i$-1))=1. The public modulo $N_i$ and Ø($N_i$), $i$=1,2, namely $N_i = p_iq_i$ are computed. So, Ø($N_i$) = ($p_i$-1)($q_i$-1). First user sent ($N_1$, $N_2$, $e$) as a public key to second user.

To encrypt the plaintext M of second user, so it divides into two parts M=($m_1$,$m_2$), where $m_1$,$m_2$ ∈[1,N-1]. The ciphertext C = ($C_1$,$C_2$) of M = ($m_1$,$m_2$) is calculated below. For m1, the ciphertext is

$$C_1 = m_1^e (\text{mod } N_1).$$

While, the ciphertext of $m_2$ is

$$C_2 = m_2^e (\text{mod } N_2).$$

The ciphertext is C = ($C_1$,$C_2$) has been received by first user. The network system of the ciphertext and public $N_1$, $N_2$ in the R-RSA cryptosystem is shown in Figure (9).

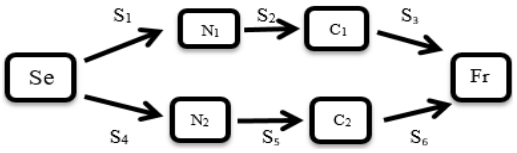



**Figure 9.** Network system of $C$ and $N_1$, $N_2$ in the R-RSA cryptosystem.

Two paths of the R-RSA cryptosystem consists of $N_1$, $C_1$ of $m_1$ and $N_2$, $C_2$ of $m_2$ respectively. The proposed cryptosystem reliability is determined depending on the PTM [25]. The sets are {$S_1$,$S_2$,$S_3$} and {$S_4$,$S_5$,$S_6$} are minimal path sets. So, a parallel-series system of the proposed cryptosystem is shown in Figure (10).

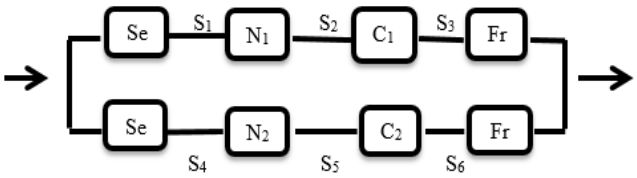



**Figure 10.** The R-RSA cryptosystem as a parallel-series system.

In this system, the paths are: $P_1$= $S_1$-$S_2$-$S_3$ and $P_2$ = $S_4$-$S_5$-$S_6$. The series paths reliability $Rs_j$ with j=1,2 is calculated depends on the reliability $R_i$ of subsystems $S_i$ for i=1,...,6. So,

$$Rs_j = \prod_{i=1}^{n} R_i, \text{ where the number of subsystems } S_i \text{ in path } P_j \text{ is equal to n.}$$

The parallel system reliability Rs is

$$R_p = 1 - \prod_{j=1}^{m}\left(1 - Rs_j\right), \text{ with the paths number is m.}$$

The decryption is done as follows. Computing first $\emptyset(N_i) = (p_i-1)(q_i-1)$, for i=1,2. So, $ed_i \equiv 1 \bmod (p_i-1)(q_i-1)$ can be solved, namely

$$d_1 \equiv e^{-1} \ (mod\ \emptyset(N_1)) \text{ and } d_2 \equiv e^{-1} \ (mod\ \emptyset(N_2)).$$

First user also calculates

$$m_1 \equiv C_1^{d_1} (\bmod N_1) \text{ and } m_2 \equiv C_2^{d_2} (\bmod N_2).$$

The original plaintext is ($m_1$,$m_2$). For encrypting the messages, new technique has been proposed based on the reliable method which is named by parallel-series reduction method (PSRM) that employs also to decrypt the ciphertext and recover the original plaintext. In Figure (11), the reliability system has two paths with six components.

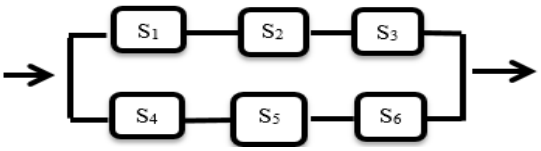
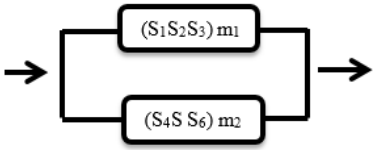



**Figure 11.** The plaintext paths form a parallel-series block.

The components $S_1$, $S_2$, $S_3$, and $S_4$, $S_5$, $S_6$, in Figure (11), form the series subsystems which are recreated using the super-components that are indicated into $m_1$ and $m_2$ respectively. The super-components reliabilities are $m_1$= $R_1R_2R_3$ and $m_2$= $R_4R_5R_6$. The series reductions in Figure (11) have been represented into Figure (12).

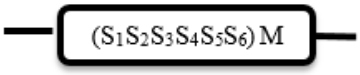



**Figuer 12.** The plaintext paths as a parallel block diagram.

A parallel subsystem has been formed based on the components $m_1$ and $m_2$ given in Figure (12) and that can be reformed by a super-component for referring into M. The super-component M has reliability computed by

$$R_p = 1 - \prod_{j=1}^{k}\left(1 - Rs_j\right), \text{ where the number of the paths } P_j \text{ equal to k.}$$

In Figure (12), the parallel reductions are converted into Figure (13).




**Figuer 13.** The plaintext system.

## RESULTS AND DISCUSSION

### Study Case on the R-RSA Cryptosystem

First user selects $p_1$=11, $p_2$=89, $q_1$=13 and $q_2$=5 as secret prime numbers. The parameter e=71 is selected also as a public encryption exponent with the property that gcd(e,($p_i$-1)($q_i$-1))=1, i=1,2. She/He computes her/his public modulo Ni. Computing Ø($N_i$) is done with $N_1= p_1q_1= 11\times13 =143$ and $N_2= p_2q_2 = 89\times5=445$ so, the values of

$$Ø(N_1) = (p_1-1)( q_1-1) =10\times12 = 120 \text{ and } Ø(N_2) = (p_2-1)(q_2-1) = 88\times4 = 352.$$

The public key of the first user is ($N_1$, $N_2$, e) = (143, 445, 71).

To encrypt the plaintext M. Second user divided M into two parts m1 and m2 ,where M = ($m_1$,$m_2$) = (43,59) such that M ∈ [1, N-1]. Second user uses a public key ($N_1$, $N_2$, e) to compute the ciphertext C = ($C_1$,$C_2$) for $m_1$ and $m_2$. For $m_1$, the ciphertext is computed by

$$C_1 = m_1^e (\text{mod } N_1) \equiv 20^{71} (\text{mod } 143) = 10.$$

While, the ciphertext of $m_2$ is

$$C_2 = m_2^e (\text{mod } N_2) \equiv 32^{71} (\text{mod } 445) = 439.$$

So, the ciphertext is ($C_1$,$C_2$) = (10,439) has been received by the first user. The network system of the ciphertext public parameter $N_1$ and $N_2$ in the R-RSA cryptosystem is shown in Figure (14).

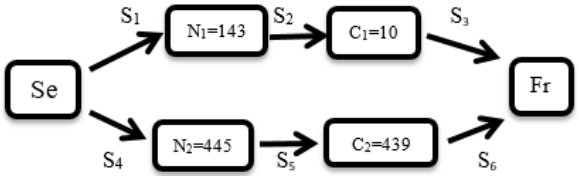



**Figure 14.** Network system of the ($C_1$,$C_2$), $N_1$ and $N_2$ in the R-RSA cryptosystem.

On the R-RSA cryptosystem, the paths of $N_i$ and $C_i$ of $m_i$ for i =1,2 are formed. The reliability is calculated based on the PTM. The {$S_1$,$S_2$,$S_3$}and {$S_4$,$S_5$,$S_6$}are minimal path sets. Figure (15) shows a parallel-series system of R-RSA cryptosystem.

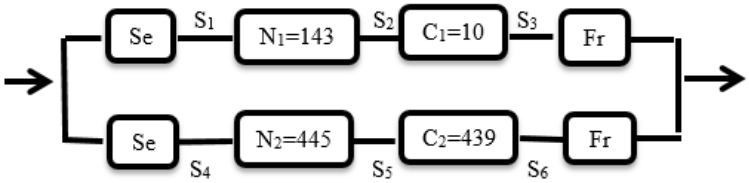



**Figure 15.** The proposed R-RSA cryptosystem as a parallel-series system.

In Figure (15), the paths are: $P_1$= $S_1$-$S_2$-$S_3$ and $P_2$ = $S_4$-$S_5$-$S_6$. Computing the series paths reliability $Rs_j$ for j=1,2 is done by

$$Rs_j = \prod_{i=1}^{n} R_i, \text{ where n is the number of subsystems } S_i \text{ in path } P_j.$$

So, it is possible to determine

$$Rs_1= R_1R_2R_3 \text{ and } Rs_2= R_4R_5R_6.$$

The parallel system reliability Rs is

$$R_p = 1 - \prod_{j=1}^{m} (1 - Rs_j), \text{ with the paths number m.}$$

$Rs_j = 1-[(1- Rs_1) (1- Rs_2)]$

$= 1-[(1- R_1R_2R_3)(1- R_4R_5R_6)]$

$= R_1 R_2R_3 + R_4R_5R_6 - R_1 R_2R_3 R_4R_5R_6.$

Upon first user receives the ciphertext $(C_1,C_2) = (10,439)$, she/he does the following computations:

$$\emptyset(N_1) = 120 \text{ and } \emptyset(N_2) = 352.$$

So, she/he computes

$$d_1 \equiv e^{-1} (mod\ \emptyset(N_1)) \equiv 71^{-1}(mod\ 120) = 71$$

and

$$d_2 \equiv e^{-1} (mod\ \emptyset(N_2)) \equiv 71^{-1}(mod\ 352) = 119.$$

She/ He calculates

$$m_1 \equiv C_1^{d_1}(\text{mod } N_1) \equiv 10^{71} (mod\ 143) = 43$$

and

$$m_2 \equiv C_2^{d_2}(\text{mod } N_2) \equiv 439^{119} (mod\ 445) = 59.$$

The original plaintext of the $(m_1, m_2) = (43,59)$. For encrypting the messages, new technique has been proposed based on the PSRM that employs also for decrypting the ciphertext. In Figure (16), the reliability system has two paths with six components.

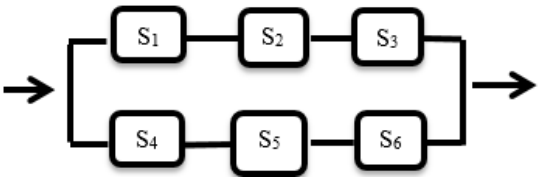



**Figure 16.** The plaintext paths form a parallel-series block.

The components $S_1$, $S_2$, $S_3$, and $S_4$, $S_5$, $S_6$, in Figure (16), form the series subsystems which are recreated using the super-components that are indicated into $m_1$ and $m_2$ respectively. The super-components reliabilities are $m_1 = R_1R_2R_3$ and $m_2 = R_4R_5R_6$. The series reductions in Figure (16) have been represented into Figure (17).

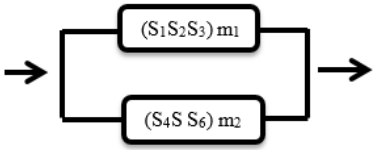



**Figure 17.** The plaintext paths in the parallel block diagram.

A parallel subsystem has been formed based on the components m1 and m2 given in Figure (17) and that can be recreated using the super-component for referring into M. Computing the reliability of super-component M is done by

$$R_m = 1 - (1 - R_{m_1})(1 - R_{m_2}) = R_{m_1} + R_{m_2} - R_{m_1}R_{m_2}.$$

In Figure (17), the parallel reductions are converted into Figure (18).

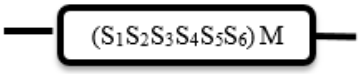



**Figure 18.** The original plaintext system.

## SECURITY ISSUES

Another version of RSA cryptosystem is proposed to enhance the security. On new proposed cryptosystem which is named by R-RSA cryptosystem, two parameters N1 and N2 of public key are generated based on secret primes p1q1 and p2q2 respectively. So, we are working with two integer factorization problems which are considered as hard mathematical problem to solve by attackers with large choice of primes. Thus, it is more difficult to get these primes that the attacker can be used to recover two parts of the plaintext

## CONCLUSION

In this work, a modified algorithm for RSA with enhanced security has been proposed through the connection for computing the complex system reliability. The security has been increased based on the hardness solving of the two integer factorization problems through choosing the secert large primes pi and qi for i =1,2 to generate the moduls N1 and N2. Rcovering the original plaintext which is divied into two parts by attackers became is more difficult. No doubt time complexity is increased, but it is negligible in compare to security level and protection of plaintext which is more important in information security.

## REFERENCES

[1] Z. Y. Karatas, E. Luy and B. Gonen, "A public key cryptosystem based on matrices," Int. J. Comput. Appl, 182, 47-50, 2019.
[2] M. Maxrizal, "Public Key Cryptosystem Based on Singular Matrix," Trends in Sciences, 19(3), 2147-2147, 2022.
[3] K. Prasad, H. Mahato and M. Kumari, "A novel public key cryptography based on generalized Lucas matrices," arXiv preprint arXiv:2202.08156, 2022.
[4] R. K. K. Ajeena, "Integer matrix size 2× 2 sub-decomposition method for elliptic curve cryptography," Computer Science, 18, No. 4, (2023), pp. 599-606.
[5] S. J. Yaqoob and R. K. K. Ajeena, "The Multi-Primes Lanstra's Elliptic Curve Factorization Algorithm," In 2020 6th International Engineering Conference "Sustainable Technology and Development" (IEC), (IEEE, 2020), pp. 141-145.
[6] R. K. K. Ajeena and H. Kamarulhaili, "On the distribution of scalar k for elliptic scalar multiplication," In AIP Conference Proceedings, (AIP Publishing, 2015), 1682, No. 1.
[7] T. Fujita, "Analytical study on Ultrafilter in Digraph: Directed Tangle and Directed Ultrafilter," Asian Research Journal of Mathematics 21, No. 5 (2025), pp. 132-146.
[8] T. Fujita, "Linear-branch-decomposition of digraph,"Theory and Applications of Graphs, submitted (2025).
[9] H. Aljader and R. Ajeena, "The optimized Diffie-Hellman key exchange using the graphical method," Journal of Discrete Mathematical Sciences & Cryptography, 2022.
[10] W. Kuo and M. J. Zuo, "Optimal reliability modeling: principles and applications," John Wiley & Sons, 2003.
[11] H. Fazlollahtabar and S. T. A. Niaki, Reliability models of complex systems for robots and automation. CRC Press, 2017.
[12] S. Xiao, W. Gong, D. Towsley, Q. Zhang and T. Zhu, "Reliability analysis for cryptographic key management," in 2014 IEEE International Conference on Communications (ICC), (IEEE, 2014), pp. 999-1004.
[13] S. Subramanian, M. Mozaffari-Kermani, R. Azarderakhsh and M. Nojoumian, "Reliable hardware architectures for cryptographic block ciphers LED and HIGHT," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 36(10), 1750-1758, (2017).
[14] A. R. Akhatov, M. Sabharwal, F. M. Nazarov, A. Rashidov, "Application of cryptographic methods to blockchain technology to increase data reliability," In 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), (IEEE, 2022), pp. 642-647.
[15] B. J. Kadim and R. K. K. Ajeena, "Reliable Public Key Cryptosystem Type El-Gamal," In 2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI), (IEEE,

2023), pp. 1-6.
[16] B. J. Kadim and R. K. K. Ajeena, “Reliable Rabin cryptosystem using the modified decomposition method,” In AIP Conference Proceedings, 3122, No. 1, (AIP Publishing, 2024).
[17] G. Yang, “Life cycle reliability engineering,” John Wiley & Sons, 2007.
[18] A. A. AL-Ali, “Reliability of complex system”, Basra J. science, 16(1),115-112, Basra, Iraq, 1998.