Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 12, 2025

INFORMATION SECURITY OF PLAIN TEXT USING PUBLIC KEY CRYPTOSYSTEM

[*1]Muhammad Asif, [2]Ahsan Ali, [3]Muhammad Kashif Shafiq
[*1-3]Department of Mathematics, University of Management and Technology Sialkot Campus, Pakistan
[*1]muhammad.asif@math.qau.edu.pk [2]ahsan.ali@skt.umt.edu.pk [3]kashif.shafiq@skt.umt.edu.p

DOI: https://doi.org/10.5281/zenodo.20727278

Keywords
Cryptography, Files Encryption, Files Decryption, Public keys, Private keys, multi-prime numbers
Article History
Received on 28 Nov, 2025
Accepted on 25 Dec 2025
Published on 26 Dec 2025

Copyright @Author
Corresponding Author: Muhammad Asif

Abstract
Cryptography is the practice and considers the strategies for securing communication and information within the presence of adversaries. In this paper introduced the modified RSA for multiple prime numbers for data encryption. The strategy which is used in this cryptosystem is an asymmetric RSA algorithm. This method has two public and private keys. The proposed algorithm also implements on text data and also used six, eight, ten, and twelve prime numbers in place of four prime numbers to gain security and "n" prime numbers are not smoothly factorized and enhanced the efficiency. The objective of this technique is to improve the security of the modified RSA through decryption procedure by implementing a multiple prime numbers algorithm to find the value of the decryption key that will further enhance the security of the decryption process.

IEER
Institute for Excellence in Education & Research

1. Introduction

The RSA cryptosystem is a secure system which based on the factorization difficulties of large prime numbers [11], RSA algorithm is a secure method. By utilizing two cryptosystem keys in advanced method [6], in which we are going to be utilized multi-prime numbers, as well utilizing two public and private keys [8]. The proposed algorithm also implement on files. This system is built for secure communication of data are called cryptosystem. The objectives of advanced cryptography are secrecy, astuteness, verification and non-repudiation. Cryptography is the practice and considers the strategies for securing communication and information within the presence of adversaries. Utilized of cryptography for secure data in the different conditions like cash take from an ATM, Pay TV, e-mail, and record capacity utilizing [14]. Advance cryptography is extremely depend on numerical values and information technology. This system, also indicate through the acronym from the authors' names, the RSA cryptosystem has to be establish the verify the period to this day, which can be utilized in cryptographic implementation starting with keeping money, and email secure in online system [10]. In this paper, we describe the modified RSA for multiple prime numbers for file encryption. The strategy which is used in this cryptosystem is an asymmetric RSA algorithm. This method has two public and private keys. Computing is an important technique and which is concern with different algorithmic perspectives and computations measured. Every day an expansive sum of information shared through computer systems, arrange security has ended up exceptionally imperative viewpoint of organizing, to secure the information through a few measures whether they are computer program measures or the equipment. To perform modular exponentiation for data and files [13], security with a broad exponent and modulus. The cryptosystem needs extraordinary computational costs.

2. RSA Cryptosystem

In 1978, this RSA strategy was developed by Rivest, Shamir, and Adleman [1]. This strategy which narrate a public-keys cryptography, involve key generation and a public-key cipher, and it's secure system lies upon the assumed trouble of calculating integrability depend on prime factors. This work suggest that not one or the other the recipient nor the sender can deny erroneously which possess to sent an exact message [15]. The RSA cryptosystem is a secure system which depend on the factorization difficulties of large prime numbers [17]. RSA algorithm became secure. The development of RSA is continuously progressing day by day. By utilizing two cryptosystem keys in advanced method [7], in which we are going be utilized four prime numbers and obtain the both keys [6], as well utilizing two public and private keys. Different authors [18-23] proposed the different schemes for information security.

The creation of two distinct public and private keys will alter the RSA algorithm [16]. Due to the large number of keys, the RSA modified algorithm takes longer to compute, yet it is still more secure than the regular technique. For encryption and decryption, this method [4] used two public and private keys and four prime numbers. which are divided into three stages: encryption, decryption, and key creation.

3. Generation of Key in RSA Algorithm

The common use of this strategy is to enhancement the usage of the method and build it further fast and diminish the strategy of decryption [12]. By utilizing four prime numbers, and Chinese remainder theorem [2], with two time encryption for each message, in this algorithm. RSA is a block cipher and the plaintext and ciphertext are numbers between 0 and *n-1*.

4. Existing Technique

Step 1

Select different prime numbers randomly say u,v and w,x.

Step 2

Calculate the value of (n, m), $n = uv$, $m = wx$.

Step 3

Calculate the Euler phi function of n and m.

Step 4

Choose two prime numbers "e" and "g" randomly, where e *and* g which are greater than 1 and less than respectively and $gcd(e, \varphi(n)) = 1$, $gcd(g, \varphi(m)) = 1$.

Step 5

Compute t, d such that $tg \equiv 1 mod \varphi(m)$, $de \equiv 1 \ mod \ \varphi(n)$.

Step 6

Public Key { g, e, m, n }, and Private Key { t, d, n, m}.

Following the creation of many public and private keys using the key generation procedure. The message will be encrypted using the public keys. The correctness must be further differentiated using four modified RSA

numbers because we are using the encryption method twice.

Encryption

We will select the message "M" and primary public key "e" for encryption.

$C_1 = M^e \bmod n$

with "C_1" the other key is "g" we calculate the cipher text by using, $C = C^g \bmod m$

Decryption 1

We utilized d and t for the decryption of cipher text,

$m_1 = C^t \bmod m$

After that, we get the plain text by using the other private key d, $M = m^d \bmod n$

5. Proposed Cryptosystem 1

The proposed techniques increase the RSA algorithm with the use of multiple prime numbers with two public keys. The use of multiple prime numbers will increase the security and speed of the encryption technique. The proposed algorithm also implement on files. We are using six, eight, ten, and twelve prime numbers in place of four prime numbers to gain security, and "n" numbers are not smoothly factorized and enhanced the efficiency.

5.1 Objectives

By using a multiple prime numbers approach to determine the value of the decryption key, this technique aims to increase the security of the modified RSA decryption process. Because this approach uses several keys, it takes longer to compute, but its security is [3] higher than that of modified RSA. Two types of keys are used in the modified RSA computation [7] with two public keys; additionally, two public and private keys are used for encryption and decryption [9]. Their attack is not defenseless due to these three stages.

Step 1. Key generation.
Step 2. Encryption.
Step 3. Decryption.

Steps for Securing of Files

Modified RSA using multiple prime numbers [5], for secure file transmission algorithm is divided into four parts.

Step 1. Selecting a file for transmission.
Step 2. Encrypt the choose file.
Step 3. Transmission of the encrypted file.
Step 4. The decryption of files at other ends.

5.2 Key Generation of the Proposed Technique

During this method we will use multiple prime numbers [4] and generate different public and private keys which show the sender and receiver. Private keys also called secret keys. Secure RSA file transmission algorithm can be summarized as follows.

Step 1

Select multi-prime numbers randomly say $u,v,z...n$ and $w,x,y...n$.

Step 2

Find the value $n = uvz...n$, $m = wxy...n$.

Step 3

Compute the Euler phi function as,

$\varphi(n) = (u-1)(v-1)(z-1)...(n-1)$ *and*

$\varphi(m) = (w-1)(x-1)(y-1)...(n-1)$.

Step 4

Select two prime numbers "e" and "g" where,

$\gcd(g, \varphi(m)) = 1$, $\gcd(e, \varphi(n)) = 1$.

Step 5

Compute the value of t, d.

Step 6

Key {e, g, n, m} for public, and Key {d, t, n, m} for private. The creation of many public and private keys using the key generation procedure. We use the public keys to encrypt the message.

Step 7

We encrypt the message.

Step 8

We decrypt the message.

The flow chart of the proposed algorithm is shown in figure 1.

Flow Chart

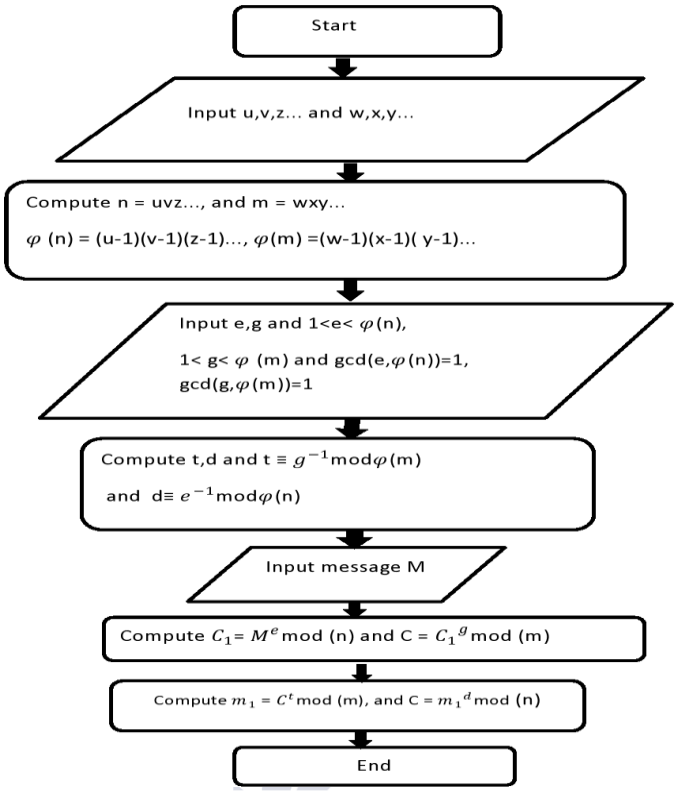


Figure 1. Flow chart for files encryption and decryption

5.3 Illustration of the Proposed Scheme

Consider the plaintext as "**FOLDER**" then encrypt and decrypt by using modified RSA for twelve prime numbers.

Step 1.

Randomly choose twelve prime numbers *u,v,z,a,c,e* and *w,x,y,b,d,f*.

u = 15643 *v* = 15601 *z* = 15139 *a* = 13963
c = 14071 *e* = 14293
w = 15359 *x* = 15413 *y* = 15511 *b* = 13879
d = 13709 *f* = 14759

Step 2.

Calculate:

$n = uvzace = 15643\times15601\times15139\times13963\times14071\times14293$

n = 10375206 896023944 811906753

$m = wxybdf = 15359\times15413\times15511\times13879\times13709\times14759$

m = 10311237 772006350 409445113

Step 3.

Find the euler phi function:

$\varphi(n) = (u-1)(v-1)(z-1)(a-1)(c-1)(e-1)$

$\varphi(n)$ =(15643-1)(15601-1)(15139-1)(13963-1)(14071-1)(14293-1)

$\varphi(n)$ = 10370987 706075438 169728000

$\varphi(m) = (w-1)(x-1)(y-1)(b-1)(d-1)(f-1)$

$\varphi(m)$ = (15359-1)(15413-1)(15511-1)(13879-1)(13709-1)(14759-1)

$\varphi(m)$=10307039 640465054 792856320

Select the "*e*" which satisfy, 1<e< $\varphi(n)$ and gcd(e, $\varphi(n)$)=1.

We choose e = 131, gcd(131,10370987 706075438 169728000)=1 and 1<g< $\varphi(m)$, gcd(g,$\varphi(m)$)=1.

Step 4

Choose g =151 and gcd(g, $\varphi(m)$) = gcd (151,10307039 640465054 792856320) = 1

$tg \equiv 1 \bmod \varphi(m)$

$t \equiv g^{-1} \bmod \varphi(m) \equiv 151^{-1} \bmod 10307039\ 640465054\ 792856320$ t = 9829229 855807734 371995431

Step 5

Determine "d " then $de \equiv 1 \bmod \varphi(n)$.

$d \equiv e^{-1} \bmod \varphi(n) \equiv 131^{-1} \bmod 10370987\ 706075438\ 169728000$

d= 5383413 465749082 408713771

Step 6.

First Public key:

(e , n) = (131, 10375206 896023944 811906753)

2nd public key:

(g , m) = (151,10311237 772006350 409445113)

First private key:

(t , m) = (9829229 855807734 371995431 , 10311237 772006350 409445113)

2nd private key:

(d , n) = (5383413 465749082 408713771 , 10375206 896023944 811906753)

Encryption

Consider the plaintext is "**FOLDER**", M = 051411030417. The string broke into four-digit blocks 0514 1103 0417. Plaintext should be less than n.

Cipher text:

For 1st block

$C_1 \equiv M^e \bmod n$

$C_1 \equiv 0514^{131} \bmod 10375206896023944811906753$

and

$C \equiv C_1{}^g \bmod m$

$C \equiv 4123129\ 651900687\ 548417199^{151} \bmod 10311237\ 772006350\ 409445113$

C = 8019283 613824690 807698042

For 2nd block

$C_1 \equiv M^e \bmod n \equiv 1103^{131} \bmod 10375206896023944\ 811906753$

C_1= 6313820 362245416 548285929

and

$C \equiv C_1{}^g \bmod m$

$C \equiv 631382036224541654828592^{151} \bmod 10311237\ 772006350\ 409445113$

C = 3198320 161830539 310495010

For 3rd block

$C_1 \equiv M^e \bmod n \equiv 0417^{131} \bmod 10375206896023944\ 811906753$

$C_1 \equiv 9966338\ 587442060\ 599558932$

And $C \equiv C^g \bmod m$

$C \equiv 9966338\ 587442060\ 599558932^{151} \bmod 10311237\ 772006350\ 409445113$

C=3615520 352943577 354482019

Decryption For 1st block

$M_1 \equiv C^t \bmod m$

$M_1 \equiv 8019283\ 613824690\ 807698042^{9829229\ 855807734\ 371995431} \bmod 10311237772006350409445113$

M_1= 4123129 651900687 548417199

$M \equiv M^d \bmod n$

$M \equiv 4123129\ 651900687\ 548417199^{5383413\ 465749082\ 408713771} \bmod 10375206\ 896023944\ 811906753$

M = 514, Message "**FO**".

For 2nd block

$M_1 \equiv C^t \bmod m$

$M_1 \equiv 3198320\ 161830539\ 310495010^{9829229\ 855807734\ 371995431} \bmod 10311237772006350409445113$

M_1 = 6313820 362245416 54828592

$M \equiv M^d \bmod n$

$M \equiv 631382036224541654828592^{9}{}^{538341346574908240871377} \bmod 10375206\ 896023944\ 811906753$

M=1103, Message "**LD**".

For 3rd block

$M_1 \equiv C^t \bmod m$

$M_1 \equiv 3615520352943577354482019^{98292298558077343719954} \bmod 10311237772006350409445113$

M_1 = 9966338 587442060 599558932

$M \equiv M^d \bmod n$

$M \equiv 9966338587442060599558932^{5383413465749082408713771} \bmod 10375206\ 896023944\ 811906753$

M= 0417, Message "**ER**".

Hence, the plaintext is "**FOLDER**".

6. Comparison

MRSA	Secured Files using MRSA with multiple prime numbers
Use two public keys.	Use two public keys.
Medium communication elevated.	High communication elevated.
Security increased.	Deliver strong security.
Less porous against brute force attack.	Little penetrable to against brute force attack.
Required large time for files security.	Required more time for files security.

6.1 Files Encryption Analysis

Analyzed and studied two public keys cryptography, compared the modified RSA algorithm and modified RSA using multiple prime numbers achieved a basic process for file encryption and decryption, provided effective protection to document security. We find that

the modified RSA technique can be used for file encryption by analyzing the display situation of the program. When high-security file transfer is necessary in public forums, the modified RSA technique can be utilized.

7. Conclusion

The proposed technique of modified RSA in which using multiple prime numbers is favorable for files securing. To extend the security of files, secret keys and multi-prime numbers are used in this algorithm. Expressed the comparison between modified RSA for four prime numbers and for multiple prime numbers for the security of files. By utilizing multi-prime RSA calculation, the effectiveness of the decryption is progressed when compared to the modified RSA for four prime numbers makes a difference through split the files for security purposes. Although it takes longer to execute than the original RSA, the Chinese Remainder Theorem improves the performance of modified RSA with multi-prime integers and makes it more safe utilizing the advanced RSA model (two public and private keys). We can utilize modified RSA with multi-prime numbers to increase security and ensure file transmission safety. Because there are more keys in modified RSA, the computation time is longer, but the security is higher. The RSA cryptosystem's security is predicated on two mathematical challenges: the challenge of factoring big numbers, which is known as a mathematical attack, and the challenge of attempting every conceivable private key, which is known as a brute force attack. Thus, the security was improved by this approach. Because it is an asymmetric-key cryptosystem, two keys a public key and a private key are needed for communication. Data division aids in preventing hackers from viewing the complete file. Additionally, even if the hacker managed to view the saved file, he might not be able to identify its contents because it is encrypted. Compared to using split files for four prime numbers, this solution demonstrates its security. In order to effectively address the core issue of security, this study proposes file security. Data privacy is ensured by splitting the file and encrypting it using an unbreakable method. This approach can be investigated and applied in the future.

8. References

[1] Abdulkader, H., Samir, R., & Hussien, R. (2019). Improved RSA security using Chinese remainder theorem and multiple keys. Future Computing & Informatics Journal, 4(1), Art.1. 51-64.

[2] Balaji, V. S. (2010). Secure transmission of data using Chinese remainder theorem and RSA. Journal of Global Research in Computer Science, 1(1), 33-35.

[3] Dhakar, R. S., Gupta, A. K., & Sharma, P. (2012). Modified RSA encryption algorithm. International Conference on Advanced Computing & Communication Technologies, 7(2-3-4), 426-429.

[4] Gannon, J. (2001). Stealing secrets, telling lies: How spies and code breakers helped shape the twentieth century. University of Nebraska, 1st edition, 30-31.

[5] Hinek, M. J. (2008). On the security of multi-prime RSA. Journal of Mathematical Cryptology, 2(2), 117-147.

[6] Ivy, B. P. U., Mandiwa, P., & Kumar, M. (2012). A modified RSA cryptosystem based on `n' prime numbers. International Journal of Engineering & Computer Science, 1(2), 63-66.

[7] Jahan, I., Asif, M., & Rozario, L. J. (2015). Improved RSA cryptosystem based on the study of number theory and public-key cryptosystems. American Journal of Engineering Research, 4(1), 143-149.

[8] Kapoor, V. (2013). Data encryption and decryption using modified RSA cryptography based on multiple public keys and `n' prime number. International Journal of Scientific Research in Network Security & Communication, 1(2), 35-38.

[9] Mollin, R. A. (2005). Codes: the guide to secrecy from ancient to modern times. CRC Press. Richard A. Mollin, Chapman & Hall/CRC, 1st edition, 679.

[10] Saraireh, S. (2013). A secure data communication system using cryptography and steganography. International Journal of Computer Networks & Communications 5(3), 125-137.

[11] Shinde, G. N., & Fadewar, H. S. (2008). Faster RSA algorithm for decryption using Chinese remainder theorem. International Conference on Computational & Experimental Engineering & Sciences, 5(4), 255-262.

[12] Rai, A., & Jain, S. (2017). Modified RSA cryptographic system with two public keys and

Chinese remainder theorem. International Journal of Computer Science & Engineering, 4(7), 22-25.

[13] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[14] Saraireh, S. (2013). A secure data communication system using cryptography and steganography. International Journal of Computer Networks & Communications 5(3), 125-137.

[15] Shinde, G. N., & Fadewar, H. S. (2008). Faster RSA algorithm for decryption using Chinese remainder theorem. International Conference on Computational & Experimental Engineering & Sciences. 5(4), 255-262.

[16] Sony, K., Shaik, D., Sri, B. D., & Anitha, G. (2015). Improvised asymmetric key encryption algorithm using MATLAB. IOSR Journal of Electronics & Communication Engineering, 10(2), 31-36.

[17] Suganya, N., M. E. Boopal, and M. Naveena. "Implementing Multiprime RSA Algorithm to Enhance the Data Security in Cloud Computing." International Journal of Innovative Research in Science, Engineering and Technology 4, no. 1 (2015): 2347-6710.

[18] Bahaddad, A., Asif, M., Ashraf, U. M., Asiri, Y., & Alkhalaf, S. (2024). The security of text data based on cyclic codes over algebraic structure. Thermal Science, 28(6 Part B), 5205-5215.

[19] Mahboob, A., Siddique, I., Asif, M., Nadeem, M., & Saleem, A. (2024). Construction of highly non linear component of block cipher based on mclaurin series and mellin transformation with application in image encryption. Multimedia Tools and Applications, 83(3), 7159-7177.

[20] Mahboob, A., Asif, M., Zulqarnain, R. M., Saddique, I., Ahmad, H., & Askar, S. (2023). A Mathematical Approach for Generating a Highly Non-Linear Substitution Box Using Quadratic Fractional Transformation. Computers, Materials & Continua, 77(2).

[21] Mahboob, A., Asif, M., Zulqarnain, R. M., Siddique, I., Ahmad, H., Askar, S. S., & Pau, G. (2023). An Innovative Technique for Constructing Highly Non-Linear Components of Block Cipher for Data Security against Cyber Attacks. Comput. Syst. Sci. Eng., 47(2), 2547-2562.

[22] Mahboob, A., Asif, M., Nadeem, M., Saleem, A., Eldin, S. M., & Siddique, I. (2022). A cryptographic scheme for construction of substitution boxes using quantic fractional transformation. IEEE Access, 10, 132908-132916.

[23] Asif, M., Asamoah, J. K. K., Hazzazi, M. M., Alharbi, A. R., Ashraf, M. U., & Alghamdi, A. M. (2022). A novel image encryption technique based on cyclic codes over Galois field. Computational Intelligence and Neuroscience, 2022(1), 1912603.

[24] Khan, M., Jamal, S. S., Hazzazi, M. M., Ali, K. M., Hussain, I., & Asif, M. (2021). An efficient image encryption scheme based on double affine substitution box and chaotic system. Integration, 81, 108-122.

[25] Alanazi, A. S., Munir, N., Khan, M., Asif, M., & Hussain, I. (2021). Cryptanalysis of novel image encryption scheme based on multiple chaotic substitution boxes. IEEE Access, 9, 93795-93802.

[26] Asif, M., Mairaj, S., Saeed, Z., Ashraf, M. U., Jambi, K., & Zulqarnain, R. M. (2021). A novel image encryption technique based on Mobius transformation. Computational intelligence and neuroscience, 2021(1), 1912859.

[27] Asif, M., & Shah, T. (2019). BCH Codes with computational approach and its applications in image encryption. Journal of Intelligent & Fuzzy Systems, 37(3), 3925-3939.Science Engineering and Technology 4(1), 2347-6710.