MINAR International Journal of Applied Sciences and Technology
ISSN: 2717-8234
Article type: Research Article

Received: 02/09/2023 **Accepted:** 25/10/2023 **Published:** 01/12/2023

A STUDY ON MODIFIED RSA CRYPTOSYSTEM

Dua M. GHADI[1]
Ministry of Education, Iraq

Abstract

Cryptography is the technique of turning information into an unreadable form in order to safeguard it. It is used to prevent unwanted data access. The RSA Algorithm offers robust encryption; however, it is computationally demanding. The RSA algorithm, has a vulnerability related to integer factorization for small numbers. The researchers want to improve the RSA cryptosystem's security and efficiency by presenting and comparing various modifications that attempt to improve the key generation, encryption, and decryption procedures. This paper explains how to extend and modify the RSA algorithm for better security and performance, then gives brief description of their output**.**

Keywords: *Cryptosystem; Decryption; Encryption; RSA; Modified RSA*.

Introduction

One important part of communication is keeping the data and messages safe while they travel over networks, and cryptography has an integral role here. Before providing a communication over a public network, cryptography entails converting it into an unreadable form, known as encryption. The encryption of data secures it against any unlawful entry to decrypt it and, only the holders of the corresponding keys may [1].

Classic cryptography is a kind of symmetric key cryptography where the encryption and decryption procedures are carried out using the same key — it means that a single key is used for both the encryption and decryption processes— the key is identical or private, like in ancient Egyptian hieroglyphs, Greek's scytale or Rome's Caesar's this cryptography works in such a way that the key must remain unknown but cryptography nowadays is based on asymmetric key system, where one has two keys separate ones for decryption and encryption. The inbuilt benefit of such asymmetric systems is a greater secure guarantee than symmetric when it's understood that two separate keys protect message privacy. On the other hand, modern crypto employs asymmetric key cryptographic system where there

http://dx.doi.org/10.47832/2717-8234.17.5

[1] mdua1093@gmail.com

are two separate keys used for encrypting as well as decrypting thus making one more secure. Some of these systems that one might encounter as an Undergraduate are “the Diffie- Hellman (DH) Key Exchange Protocol, RSA, and Multi-Prime RSA”. [2].

RSA encryption, with number theory at its foundation, which uses prime factorization as part of its security model, is commonly adopted. This is a public-key (asymmetric) crypto system that was introduced back in 1978 where till date it’s one of the most popular systems used for digital signature and secure communication [3]. Its power comes from the fact that the factorization of this problem is difficult and mathematicians have struggled with it for decades. RSA uses 2 keys: The public key is utilized for encrypting the data, while the private key is utilized for decrypting it, so to maintain secure communication private key not be distributed and only can use with private secret number or we can say this will never share [4].

This paper presents four sections. Section 2 presents the standard RSA algorithm. Thereafter follows the review of the modified RSA approach and its sub-sections in Section 3. It then continues with Section 4, which presents a comparison between standard RSA and modified RSA. Lastly, Section 5 is the conclusion.

1. Standard RSA Algorithm

The RSA algorithm is popular with public key cryptosystems, but it has challenges involving factorizing large numbers. Three phases are in the RSA algorithm. The private key and public key are both created in key generation stage. The encryption is to convert normal letters into some random letters with the help of a public key and decrypt to again turn those random letters into normal letters using a private key. This algorithm allows for secure communication because only your communication can be viewed and decrypted by the intended recipient [5].

2.1. Key Generation

RSA is a method of asymmetric encryption based on the utilize of a public key and corresponding private key to encode and decode messages. It’s about multiplying two primes together and secreting their constituent parts to secure communications. To decrypt requires knowledge of prime factors; to decode you must have the key.

The RSA's keys are generated using the following process:

Algorithm_1: Key Generation for RSA [3]	
Input: p and q	***// "p, q is distinct prime numbers"***
Output: K_1 (e, n), K_2 (d, n)	***// "K_1 is public key, K_2 is private key"***
1. Choose two random prime numbers, p and q.	***//"should have a similar bit length"***
2. $n \leftarrow p\,q$.	***// "n is a modulus for both the public and private keys"***
3. $\Phi(n) \leftarrow (p-1)(q-1).$	***// "Φ is Euler's totient function"***
4. Choose an integer **e** such that 1 < e < $\Phi(n)$ and gcd of (e, $\Phi(n)$) =1	
5. $d \leftarrow e^{-1} \bmod \Phi(n)$	***// "d is the multiplicative inverse of $e \bmod \Phi(n)$"***
6. Public key = K_1 (e, n), Private key = K_2 (d, n).	

The public key is used to encrypt data, while the private key is used to decrypt it. The public key is widely known, but the private key is kept private and only known to the user who has it. Anyone can send data using the public key, whereas only the user can decrypt it.

2.2. Encryption

Alice shares her public key (n, e) with Bob, while he keeps his private key. In order to transmit a message M to Alice, Bob can use Alice's public key to encrypt the message, ensuring that only Alice, with her private key, can decrypt and read the message as mentioned in above, that approach is an important concept in public key cryptography.

Algorithm_2: RSA Encryption [3]	
Input: M, K_1 (e, n)	***// "M is the message (plaintext), K_1 Public Key from Algorithm_1"***
Output: c	***// "c is ciphertext"***
1. $c \leftarrow M^e \bmod n$	***// "Encrypt message in ciphertext"***
2. Alice sends the ciphertext **c** to Bob	

In the context of RSA encryption, the text explains that the message M is encrypted as C using a public key and can only be decoded by the recipient using their private key. The private key is kept secret, and the public key is available publicly. But with longer messages m, the efficacy of such keys decreases. The multiple values of m can produce the same ciphertext — but this happens very rarely in practice.

2.3. Decryption

The decryption process is much the same as encryption. Once you know the values of p and q, to decrypt and decipher RSA you just need the ciphered message (encrypted text)

and return the unmodified plaintext. Decryption can be performed with either the public or private keys, offering some flexibility.

Algorithm_3: RSA Decryption [3]	
Input: c, K_2 (d, n)	***// "c is ciphertext , K_2 Private Key from Algorithm_1"***
Output: M	***// "M is message (plaintext)"***
1. $M \leftarrow c^d \pmod n$	***// "Decryption ciphertext in plaintext"***
2. Bob can read the original message M (plaintext)	

It defines how the RSA algorithm is being decrypted by the algorithm. The recipient, Bob, in turn, needs his private key (d) and the modulus (n) to calculate the original message (M) utilizing the formula M = $c^d \ mod \ n$. Enable Bob to see the message that was sanded by the recipient — Alice.

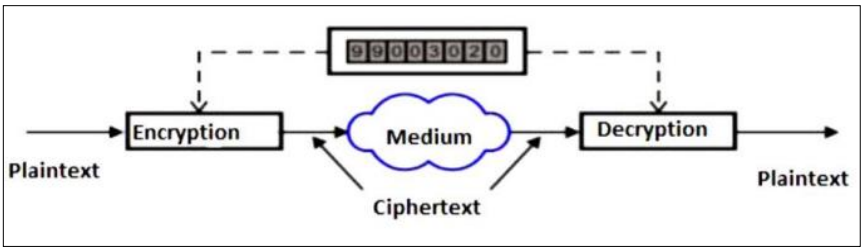

Figure 1: Encryption and Decryption System *[6]*.

2. Literature Review on Modified RSA Approach

In this section we concentrate on presenting modifications to improve the RSA for security. The RSA algorithm is popularly used in network security and has issues of factorization for small numbers. The scientists suggest improvements to create novel methods towards increase security and efficient cryptosystem of RSA by optimizing key-generation, encryption and decryption process.

In [7] Hashim H. R. describes an alteration on the RSA cryptosystem which improves its security with multiple distinct secret keys. This change is geared towards implementing this method on matrices with particular attention paid to those used for images. With more private keys the RSA system is strengthened to make secure the public key cryptography.

Mezher A. E. [4] propose a solution to improve the security of RSA algorithm utilizing multiple public /private key pairs. In embedding the variance in the keys, the security of RSA becomes stronger such that now its reliability doesn't just depend on the size of the key but rather depends on the variance in multiple keys.

Islam M. et al [8] suggested a much-improved RSA based on "n" number of different prime numbers such that, finding a factor for N will become more difficult; hence improving the security of the RSA. It is based on 2 separate public, secret key pairs of N, that generate

after creating two greatest factors and making an increase encryption, decoding operation of 2 that increase in effectiveness, privacy, and resilience to a break of a single point. Results of our experiments show that this method takes longer to generate keys, analyses the data, encryption and decryption than the traditional RSA.

Al_Barazanchi et al. [9], new security frameworks for secure data are discussed, focusing on RSA algorithm development and stronger encryption keys to increase security in applications Paper 3 proposes to include challenges About RSA algorithm by key. The findings show that the suggested algorithm with 3 keys has a lower error rate in receiving the encrypted text.

Abdeldaym, R. S., et al. [10], they propose to use 4-prime numbers instead of one in the RSA algorithm. Instead of sending 1-public key, 2-public keys are sent to the recipient. However, RSA decryption uses the Chinese memory theorem to increase decryption speed to address the speed issue.

Mojisola, F. O. et al. [11] Their study introduces encryption algorithms that aim to enhance the safety of the well-known RSA algorithm (with a key duration of 1024) in opposition to numerous assaults. The observe compares the safety evaluation and experimental consequences of the proposed set of rules, called RBMRSA, with the classical RSA set of rules. The outcomes indicate that RBMRSA offers stepped forward security however might also require greater execution time compared to classical RSA.

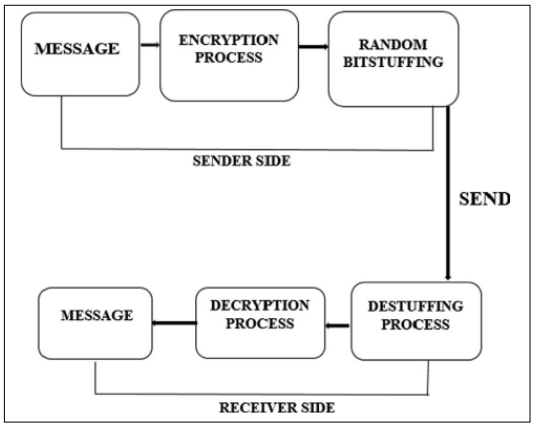

Figure 2: RBMRSA Algorithm *[11]*

Lizy, R. F. S. [12] Their paper discusses the encryption of an image in the Aadhaar card using the RK-RSA algorithm, which provides enhanced protection and confidentiality. The performance of the RK-RSA algorithm is evaluated depended on factors like: “Avalanche Effect, Speed, Throughput, and Power Consumption” is presented with improved outcome. The paper further presents a thorough mathematical explanation on the RK-RSA algorithm.

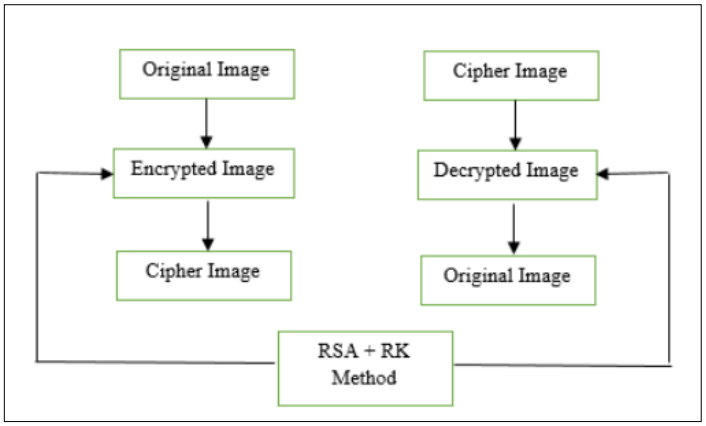

Figure 3: RK-RSA Algorithm *[12]*

Lizy, R. [13] they propose using the Euclidean approach instead of changing the RSA algorithm so as to improve its results. The proposed technique is more effective on "speed, throughput, power dissipation, and noise enhancement factor". The authors not only provide empirical evidence but also derive mathematical logic in support of their proposed approach.

Sarjiyus O. et al. [14] Their research aims to develop a new RSA scheme to improve network data security. The scheme will generate robust secret keys using a new functionality, making it difficult to guess the private key or factorize certain values. This approach uses a number within a specific interval to tie encryption and decryption keys.

Gupta, Chiradeep, and NV Subba Reddy [15], They propose a strategy for fusing the "DH key exchange protocol and the public-key RSA encryption system" to defend against the MITM attack. In order to assess the efficacy of their suggested strategy, the researchers contrast its performance with that of the original DH Key Exchange technique and the RSA Cryptosystem.

The following **Table 1** provided A summary of Modified RSA methods and the time that consuming

Table 1: summary of Modified RSA.

Ref.	Title	Approach/Method	Input tex size	Time	
				Encryption	***Decryption***
[7]	"A new modification of RSA cryptosystem based on the number of the private keys'	suggest "k" "number o distinct private keys"	plain matrices	-	
[4]	"Enhanced RSA Cryptosystem based on Multiplicity of Public and Private Keys"	incorporating the multiplicity of keys	12	347.049 ms	
[8]	"A modified and secured RSA public key cryptosystem based on "n" prime numbers".	n distinct prime number RSA	4096 bits	Encryption: 56.87 ms	Decryption: 19,983.37 ms
[9]	"Modified RSA-based algorithm: a double secure approach"	"complexity to the encryption and decryption process using 3 keys (3k)"	100 bytes	0.035638 s	
[10]	"Modified RSA algorithm using two public key and chinese remainder theorem'	RSA using Multi Keys	1136 bits	113	
. [11]	"An improved random bit-stuffing technique with a modified RSA algorithm for resisting attacks in information security (RBMRSA)"	RBMRSA method	60 bytes	Encryption: 3.49 ms	Decryption: 17.01 ms
[12]	"Image Encryption Using RK-RSA Algorithm in Aadhaar Card"	RK-RSA for textimage	289 bytes	Encryption: 19.2005 s	Decryption: 31.8459 s
[13]	"Improvement of RSA Algorithm Using Euclidean Technique"	RSA algorithm is modified by incorporating the Euclidean technique	289 bytes	0.882420 s	
[14]	"New RSA Scheme for Improved Security "	uses a number within a specific interval to tie encryption and decryption keys	-	-	

[15]	"Enhancement of Security o Diffie-Hellman Key Exchange Protocol using RSA Cryptography"	"public-key RSA with DH key exchange"	-	0.0056461 s

The Table lists some methods that prior researchers have suggested to increase the security, effectiveness, and speed of the RSA system. These strategies change the prime number and key size. The security of the system is increased by increasing the complexity of the scheme and the size of the key. In the next section, we will explain and compare these methods with the standard RSA.

3.1. Modified RSA based on Keys

The RSA, as mentioned before, is a well-liked asymmetric cryptography method. It has been found that the value of private keys is vulnerable to factorization attacks based on the modulus 'n' and the public key. Some studies describe changes to the RSA algorithm influenced by keys. These studies focus on enhancing security by modifying the equation of the keys during the encryption and decryption process.

Nivetha A., et al. [3]**,** They suggested enhancing the RSA algorithm by incorporating 4-prime numbers in the public and private key combination. Their modifications increase the complexity of the factor variables, which simplifies the analysis process with the help of tools and equipment Their algorithms focus on increasing the speed of the calibration work by reducing the computational steps and complexity on, leading to easier calculations and reduced time constraints.

Ayele A. & Sreenivasarao V. [16] Proposed an algorithm to implement RSA public-key crypto system using two separate public keys. This approach increases security by preventing an attacker from gaining detailed knowledge of the encryption key and decrypting the message. However, it is important to note that this approach may result in slower performance speeds compared to other RSA implementations.

Mansour, A. H. [17]**,** Based on the Gordon method, they suggested system employs a formula where primes are written as 2^(2p0 + 1) and 2^(2q0 + 1). By streamlining the prime multiplication procedure, which depends on the likelihood of the strong primes, this strategy seeks to enhance the basic generation's performance.

Shukla A. K., & Kapoor V. [18]**,** A modified version of the RSA algorithm is introduced in public key cryptography. The RSA algorithm generates two keys: one for encryption and another for decryption. Yet, brute force assaults can be used to exploit the method. They propose using n prime numbers and several public keys to boost security and raise the likelihood of a breach. The discrete logarithm issue serves as the mathematical foundation for the RSA algorithm's application, particularly when it comes to integer multiplication.

Mezher, A. E., [4]**,** A proposed new RSA algorithm for encryption and decryption schemes. Their scheme to enhance the security of the RSA algorithm by utilizing multiple public and private keys. This algorithm enhances the security of RSA by using more public keys to encrypt the message and generating more private keys to decrypt it. This makes it harder for attackers to decrypt the message because they would have to search for all of the private keys instead of just one.

3.2. Modified RSA Based on Prime Number

The algorithm used in this case uses large prime numbers, represented by the variables p, q, r, which are difficult to parse into specific variables for increased security, algorithm stores variables in separate database tables, changing values than e and d during encryption and decryption, from the beginning of the process and storing the previous key offline [19].

The method utilizes Number Theory to establish secure communication between Alice and Bob. Bob generates private, secret, and public keys, with the public key being shared publicly. The private key is kept secret by Bob, and additional keys are shared secretly with Alice to enhance security. Alice can then encrypt a plaintext message into ciphertext using the provided keys, and Bob can decrypt the ciphertext back into the original message [2] . Encryption, encryption, and decryption using keys, show in the following algorithm, [2]:

Algorithm_3: Prime Number Algorithm.

Key Generation

1. $n \leftarrow p.q^r$ *// "Bob selects three or more prime numbers, such as p, q, r, and so on. then multiplies these prime numbers together to obtain the modulus, n, which is used for both the public and private key in cryptographic algorithms like RSA".*
2. $\Phi(n) \leftarrow (p-1)(q-1)(r-1).$ *// "computes the Euler's Totient of n".*
3. $1 < e < \Phi(n)$ and gcd of (e, $\Phi(n)$)=1 *// "Bob chooses the Encryption exponent e which satisfying the condition".*
4. $d.e \leftarrow 1(mod\ e\ \Phi(n))$ *// "computes the decryption exponent d"*

Encryption

1. $c \leftarrow (am+b)^e\ (mod\ n)$ *// "Alice converts a message or plaintext into a numerical code labeled as 'm' and then encrypts it into ciphertext 'c'. The process involves transforming the original message using cryptographic algorithms to ensure its confidentiality and security during transmission or storage".*

//" then Alice transmits the encrypted message, represented as ciphertext c, to Bob"

Decryption

// "Bob is decrypting a ciphertext using the modified Multi-prime RSA algorithm. He computes the decryption by performing calculations involving modular arithmetic. This process allows him to retrieve the plaintext message from the ciphertext".

1. $m_p \leftarrow \frac{c^d\ (mod\ p)-b}{a}$
2. $m_q \leftarrow \frac{c^d\ (mod\ q)-b}{a}$
3. $m_r \leftarrow \frac{c^d\ (mod\ r)-b}{a}$

.
.
.

// "Applying the Chinese residue theorem and Fermat's minor theorem, Bob is able to recover the original plaintext message denoted by 'm'. These mathematical techniques allow for the decryption process, allowing Bob to recover the original message from the cipher text".

4. $m = m_p = m_q = m_r = \ldots..$

Multi-prime RSA provides better security compared to standard RSA. "Factoring attacks", "small private exponent attacks", and "Chinese remainder theorem attacks" are the three primary multi-prime RSA attacks. Multiplication Attacks occur when parameters

product of primes are small so the use of large parameters is necessary to prevent simple multiplication “Small private component attacks” and “Chinese remainder theorem attacks” both target the private key, but what cuts to it breaks modulus into chunks of primes [2], [20].

3.3. Modified RSA Based on Diffie-Hellman Key

The DH algorithm is a key exchange method that allows 2-parties to share a secret key without prior knowledge. It uses RSA keys as input, generating a secure cipher text. Encryption and decryption involve XOR operations, ensuring easy message transmission and reception for users.

Bhattacharjee C. A. et al. [21]**,** describes a combined approach of the Diffie-Hellman and RSA algorithms, where the session key from Diffie-Hellman is used in the RSA cryptosystem. This approach enhances security by multiplying the session key with prime numbers and replacing the multiplied value with the RSA 'N' variable. This technique makes it more challenging for attackers to perform mathematical factorization attacks on the RSA cryptosystem.

Alice and Bob would like to exchange their messages securely. They declare that they shall encode their public key so that only them can be in a position of reading other parts of the message. To achieve this, the proposed model mixes up the RSA algorithm with the DH Key Exchange algorithm. They use the RSA protocol, where random numbers are generated and a public-private key calculated. Then the encrypted public key is exchanged and decrypted with their own private store, which makes it difficult for an attacker to break the encryption without knowledge of the over primes involved [15].

This procedure differs due to using the DH algorithm instead of keys exchange, as well as the XOR operation instead of RSA relying on modular exponentiation and prime number factorization. In the RSA cryptosystem DH algorithm is used to generate the session key. It increases security through replacement of the multiplied ‘session key’ and the ‘RSA N’ with a prime number. The basic objective of this method is to complicate any attempts at the mathematical factorization attack against the RSA cryptosystem.

Table 2: Modification Technique with their Features

Author Ref. year	Modification Technique						Feature of the Modification
	Keys	n Prime Number	Diffie-Hellman	Signature	Euclidean	Random bit-stuffing	
Ayele A. & Sreenivasarao V., [16], 2013							Features of this modified RSA algorithm include: 1. The conversion uses instead two public key pairs rather than one. 2. This change entails encoding and decoding the e key with mathematical logic. 3. Doing this will prevent attackers from reaching out to the e value which eventually leads them to decrypting the message through d value. 4. A tweaked algorithm aims at delivering an encrypted-decrypted approach that preserves data security but remains efficient.
Shukla, A. K., & Kapoor, V., [18], 2014							The modified RSA combines the usage of multiple public keys with the n prime technique. The inclusion of these additional features increases the difficulty for a hacker to figure out how to crack the encryption process. To further hinder others' ability to analyze the data, the implementation additionally includes discrete-log problems and hard number multiplications.
Nivetha A., et al. [3], 2015							The features of this modified RSA encryption algorithm include: 1. Combine public and private keys with 4 prime numbers. 2. More complex factored variables that can easily analyzed with more advanced tools and gear. 3. Enhanced security and quicker encryption method. 4. Faster and more efficient than the original RSA encryption, demonstrated via experiments. 5. Use of a serial subtraction operation instead of a divide operation; this entails faster computation and reduced mathematics involved.
Hashim H.							The main feature of this modified RSA cryptosystem is:

R. [7], 2016							1. the increase in the number of private keys. The modification provides new "k" numbers, which enhances security. 2. this improvement enables enhancing security of RSA cryptosystem, applied to the matrices, particularly those used for image representation, protecting them against some possible attacks.
Mansour, A. H. [17], 2017							The following features are included in the modified RSA Digital Signature private and public key generator: 1. Utilizes "Strong prime" concept, to enhance security. 2. Formula for generating primes: The scheme uses a formula where the prime numbers are expressed as **$2^{(2p_0 + 1)}$ and $2^{(2q_0 + 1)}$,** based on Gordon's algorithm. This formula helps generate strong primes efficiently. 3. Optimization of key generation time, relying on probabilities associated with strong primes. Overall, these modifications aim to improve both security and efficiency in RSA Digital Signature key generation process.
Mezher A. E. [4] , 2018							This modified algorithm where numerous publics as well as private keys are deployed in encryption and decryption processes, improving the level of protection. It claims to have more strength against a brute-force attack and to take longer to crack than the existing RSA algorithm.
Islam M. et al [8],2018							The modified approach of the RSA cryptosystem proposed has several features: 1. the number of "n" unique prime numbers used here will make the problem N harder to factor, hence increase the algorithm's complexity. 2. This technique offers an enhanced level of security than the usual RSA due to its double encryption and decryption system involving two "N" large units, each generating both private and public keys. 3. Despite some operations being more exhaustive and delaying than usual RSA, such as key generation time, "N" variable checking, encryption and decryption, overall performance is kept efficient

							through increased level of enhanced security measures 4. The altered process is more secure and can hardly be penetrated by would-be attackers or foes.
Kamardan, M. G., et al [2], 2018							The Modified Multi Prime RSA Cryptosystem is an improvement on the standard RSA cryptosystem that produces keys from a pool of prime numbers. Here are some of the edition's new features. 1. It is more difficult for attackers to guess values and extract private keys. 2. Using more primes reduces computational complexity, which speeds up encryption and decryption when compared to standard RSA. 3. Users have greater control over basic generation since they may choose the number of primes that best meets their demands or chosen level of security. 4. Using a large number of primes reduces the amount of storage required for the public and private keys.
Lizy, R. et al. [13], 2023							The following features are included in this enhancement: 1. The improved RSA method's faster encryption and decryption operations result in shorter processing times. 2. By processing more data in less time, the system becomes more efficient. 3. By strengthening RSA's cryptographic characteristics, the improvement makes it more resistant to attacks resulting from input or key alterations. As a result, this method of protecting digital data becomes more reliable and efficient.
Gupta, C., & Reddy, N. S. [15], 2022							The features of enhancing the security of the DH key exchange protocol using RSA cryptography include: 1. Added an additional layer of encryption to prevent decoding of the transferred keys and unwanted access. 2. strengthens the defend against man-in-the-middle attacks. 3. It becomes easier for parties to exchange and securely keep public keys.

							4. Because RSA uses bigger key sizes, attackers find it computationally challenging to crack or guess private keys using exhaustive search techniques. 5. Forward secrecy is accomplished by combining Diffie-Hellman with RSA. This is because each session creates distinct temporary encryption keys that are destroyed after usage, making it more difficult for a later-arriving attacker to decipher earlier conversations. 6. Both Diffie-Hellman and RSA are widely supported cryptographic algorithms, making their combination compatible with various systems and protocols already in place.

3. Comparison between Standard RSA and Modified RSA

This section explores various RSA modifications studied and presented in the past decade and comparison with standard RSA, highlighting their algorithm and the significant efforts made by previous researchers. The purpose of this comparison was to evaluate the efficiency of these algorithms with respect to time required for "key generation, encryption, and decryption" processes. we compared the different RSA methods include the encryption and decryption times, key generation time, performance that used in the algorithm, **Table 3** and **Table 4**.

Table 3 shows compare RSA methods according of key generation, encryption, decryption schemes and the mathematical modifications with some other studies.

Table 3: RSA techniques that rely on the generation, encryption, and decryption of keys

Algorithm	Key Generation	Keys	Encryption	Decryption
Standard RSA	$n= p*q$ $d \leftarrow e^{-1} \bmod \Phi(n)$	Public Key= K1 (e, n), Private Key= K2 (d, n)	$c \leftarrow M^e \bmod n$	$M \leftarrow c^d \pmod n$
Modified RSA based on Prime Number [8]	$n= p*q$ $d \leftarrow e^{-1} \bmod \Phi(n)$ $f \leftarrow g^{-1} \bmod \Phi(n)$	Public Key= K1 (e, f, n), Private Key= K2 (d, g, n)	$c \leftarrow (M^g \bmod n)^f \bmod n$	$c \leftarrow (M^e \bmod n)^d \bmod n$
Modified RSA based on Four Keys [3]	$n=p*q*r*s.$ $f(n)=(p-1)*(q-1)*(r-1)*(s-1)$ $d=e^{-1} \bmod f(n)$	Public key = (e,n) Private Key = (d,N).	$c \leftarrow M^e \bmod n$	$M \leftarrow c^d \pmod n$

Main difference among RSA and Modified RSA is the changes or enhancement applied to the base RSA algorithm. Customized RSA algorithms try to enhance security, speedup or efficacy for the normal RSA algorithm. Another change includes the utilization of numerous prime numbers instead of 2 within the RSA algorithm. By this change, we can get better performance of the algorithm. Such changes or improvements are carried out on modified RSA algorithms with the intention of overcoming the disadvantages and weaknesses of a classic RSA algorithm and to ensure better security and efficiency.

Table 4: Comparison of Standard RSA and Modified RSA

Algorithm	Key Generation	Encryption & Decryption
Standard RSA	Selecting two large prime numbers, computing their product as the modulus, and finding the public and private exponents.	Encryption is performed by raising the plaintext message to the power of the public exponent and taking the modulus of the result. Decryption is done by raising the ciphertext to the power of the private exponent and taking the modulus
Modified RSA based on Prime Number	the prime number selection process is altered. Instead of using random prime numbers, specific criteria or algorithms are employed to generate the prime numbers.	The encryption and decryption procedures remain the same as in standard RSA. The modifications in this variant are focused on the prime number selection process and do not directly impact the encryption and decryption operations
Modified RSA based on Four Keys	generate four key pairs, consisting of a public and private key, by selecting two large prime numbers, computing their product as the modulus, and finding their exponents.	The session key is encrypted four times using each of the four public keys, once with each key pair. The recipient, then uses the four private keys to decrypt the encrypted session key values, obtaining the original session key.
Modified RSA Based on Diffie-Hellman Key	combines the Diffie-Hellman key exchange algorithm with RSA, where the session key from Diffie-Hellman is used in the RSA cryptosystem.	The encryption and decryption may involve combining the Diffie-Hellman key exchange algorithm with the RSA encryption and decryption operations.

Table 4 show examples showing that certain modifications to the RSA algorithm can indeed increase the speed of encryption.

Table 5: Comparison of algorithms based on time *[22]*

Algorithm	Time (µsecond)		
	Key Generation	Encryption	Decryption
RSA	997	999	1998
n Prime numbers RSA	998	1998	13992
RSA-Diffie key exchange	1000	998	999
Diffie key exchange-RSA	999	1000	999

Overall, Modified RSA combines a number of upgrades and adjustments to the original RSA algorithm in order to overcome its shortcomings and improve its security and efficiency. These changes seek to raise the RSA scheme's complexity, improve security, decrease duplicate messages, improve efficiency, and speed up the decryption process.

4. Conclusion

The traditional RSA Cryptosystem, which relies on two prime numbers, is an effective algorithm for preventing unauthorized access over the internet. However, it has drawbacks such as high computational time. To address these issues, the authors propose a modification to the basic RSA algorithm, enhancing data security. This paper surveys existing research on RSA encryption, evaluates their security and implementation, and focuses on the RSA algorithm's susceptibility to cryptanalysis assaults. To strengthen and increase the security of RSA algorithm, the authors suggest the modified of RSA, increasing the efficacy of asynchronous cryptography and reducing the average time for data transmission.

References

[1] Mohamad, M. S. A., Din, R., & Ahmad, J. I. , "Research trends review on RSA scheme of asymmetric cryptography techniques.," Bulletin of Electrical Engineering and Informatics, vol. 10, no. 1, pp. 487-492, 2021.

[2] Kamardan, M. G., Aminudin, N., Che-Him, N., Sufahani, S., Khalid, K., & Roslan, R., "Modified Multi Prime RSA Cryptosystem.," In Journal of Physics: Conference Series), IOP Publishing., vol. 995, no. 1, p. 012030, (2018, April).

[3] Nivetha, A., S. Preethy Mary, and J. Santosh Kumar., "Modified RSA encryption algorithm using four keys.," International Journal of Engineering Research & Technology (IJERT), vol. 3, no. 7, pp. 1-5, 2015.

[4] Mezher, A. E., "Enhanced RSA cryptosystem based on multiplicity of public and private keys.," International Journal of Electrical and Computer Engineering, vol. 8, no. 5, p. 3949, 2018.

[5] Patel, G., & Panchal, K. Detailed, " Detailed Study on Modified RSA Algorithm," IJIRCT Journal, 2015.

[6] Bisht, N., & Singh, S., "A comparative study of some symmetric and asymmetric key cryptography algorithms.," International Journal of Innovative Research in Science, Engineering and Technology, , vol. 4, no. 3, pp. 1028-1031, 2015.

[7] Hashim, H. R. , " A new modification of RSA cryptosystem based on the number of the private keys.," American Scientific Research Journal for Engineering, Technology, and Sciences, no. 24, pp. 270-279, 2016.

[8] Islam, M. A., Islam, M. A., Islam, N., & Shabnam, B., "A modified and secured RSA public key cryptosystem based on “n” prime numbers.," Journal of Computer and Communications, vol. 6, no. 03, p. 78, 2018.

[9] Al_Barazanchi, I., Shawkat, S. A., Hameed, M. H., & Al-Badri, K. S. L., "Modified RSA-based algorithm: A double secure approach," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 17, no. 6, pp. 2818-2825, 2019.

[10] Abdeldaym, R. S., Abd Elkader, H. M., & Hussein, R. , "Modified RSA algorithm using two public key and chinese remainder theorem.," IJ of Electronics and Information Engineering, vol. 10, no. 1, pp. 51-64, 2019.

[11] Mojisola, F. O., Misra, S., Febisola, C. F., Abayomi-Alli, O., & Sengul, G., "An improved random bit-stuffing technique with a modified RSA algorithm for resisting attacks in information security (RBMRSA)," Egyptian Informatics Journal, vol. 23, no. 2, pp. 291-301, 2022.

[12] Lizy, R. F. S. , "Image encryption using RK-RSA algorithm in aadhaar card.," urkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, no. 3, pp. 4683-4693, 2021.

[13] Lizy, R. F. S., "Improvement of RSA Algorithm Using Euclidean Technique.," Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, no. 3, pp. 4694-4700, 2021.

[14] Sarjiyus, O., Baha, B. Y., & Garba, E. J., "New RSA Scheme For Improved Security.," 2021.

[15] Gupta, C., & Reddy, N. S. , "Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography," Cryptography. In Journal of Physics: Conference Series, IOP Publishing, vol. 2161, no. 1, p. 012014, 2022.

[16] Ayele, A. A., & Sreenivasarao, V. A, " modified RSA encryption technique based on multiple public keys," International Journal of Innovative Research in Computer and Communication Engineering, vol. 1, no. 4, pp. 859-864., 2013.

[17] Mansour, A. H. , "Analysis of RSA digital signature Key generation using strong prime.," Int. J. Comput, vol. 24, no. 1, pp. 28-36., 2017.

[18] Shukla, A. K., & Kapoor, V., "Data Encryption and Decryption Using Modified RSA Cryptography Based on Multiple Public Keys and 'n'prime Number," International Journal of Engineering Sciences & Research Technology, ISSN, , pp. 2277-9655., 2014.

[19] Deshpande, V., & Das, D., "Efficient searching over encrypted database: methodology and algorithms.," In Distributed Computing and Internet Technology: 15th International Conference, ICDCIT 2019, Bhubaneswar, India, January 10–13, 2019, Proceedings 15, Springer International Publishing., pp. 327-338, 2019.

[20] Yan, S. Y. , "Primality testing and integer factorization in public-key cryptography.," 2009.

[21] Bhattacharjee, C. A., Khaskel, C., Basu, D., & PM, D. R. V., "Hybrid security approachby combining diffie-hellman and RSA algorithms," International Journal of Pharmacy and Technology, vol. 8, no. 4, pp. 26560-26567, 2016.

[22] Abhishek & Dr. Vandana, "A STUDY ON MODIFIED RSA ALGORITHM IN NETWORK SECURITY," International Research Journal of Modernization in Engineering Technology and Science , 2022.