Received: February 25, 2023. Revised: April 16, 2023.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A Hybrid Algorithm For Enhancement of the Data Security during Network Transmission Based on RSA and DH

Omar Salah[1]* **Ahmed El-Sawy[2]** **Mohamed Taha[2]**

[1]*Computer Science, Faculty of Computer Science & Information System, October 6 University, Egypt*
[2]*Computer Science, Faculty of Computers and Artificial Intelligence, Benha University, Egypt*
* Corresponding author's Email: O.Salaaheldin@gmail.com

Abstract: Due to the tremendous technological transformation, more technologies and internet of things (IoT) devices are employed in today's digital world. The majority of these technologies are linked through a network. They produce enormous amounts of information at incredible speeds, leading to zillions of digital data moving via network connections. Maintaining comprehensive and high security for any exchangeable data is vital. Networked data need security and privacy. Multiple cryptographic techniques are currently available to maintain sending messages and data security. Regardless of its simplicity, private key cryptography is unproductive for authorization. As it often covers all of the components of information security, asymmetric cryptography is much more secure than private key encryption, but it takes much longer. The purpose of this paper is to demonstrate the few encryption techniques that are used on an insecure network to encrypt data. To encrypt the data, this paper proposes a new hybrid encryption technique. The suggested approach, MRSADH, encrypts and decrypts the data using Rivest, Shamir, and Adleman (RSA) and Diffie Hellman (DH) and produces the encoded data using the XOR function to be sent to the recipient in the shortest time and with high-security complexity compared to other methods in terms of performance and avalanche effect. The proposed study examines the two most widely used cryptographic algorithms, RSA and Diffie Hellman, and how they work and impact security and speed when integrated into a unified hybrid (MRSADH) computation with necessary adjustments. The study also presents a method that uses Asymmetric and Symmetric key encryption to improve data security while reducing the number of mathematical equations, which tends to result in a quicker execution time.

Keywords: Encryption, Decryption, Public key, Private key, RSA, Diffie Hellman, MRSADH.

1. Introduction

The Internet, or World Wide Web "WWW", has hugely impacted global culture, economics, and technology after the late 1980s and early 1990s, including the development of social media platforms like Facebook, discussion forums, blogs, web-based retail sites, and everyday financial transactions. The number of active users has increased from 144 million in 1998 to approximately 5 billion by April 2022, with the Internet being used by more than 65% of the world's nations [1]. Thus, when combined with everyday activities, information technology is the foundation of today's society, used in almost all aspects of life. Information is transferred through many channels in our ordinary routine for everyday tasks and activities such as internet shopping, e-cash, clandestine military activities, social networking, and financial transactions. This communication mandates the efficient exchange of secure information [2]. In [3], security may be applied to any resource; examples include software security, communications, information security, and specific equipment's physical security of specific equipment. Nagendra and colleagues [4], Cryptography is the most robust and efficient technique of conveying data that no one except the intended receiver can examine. It is also known that encryption is an ordinarily utilized tool for preserving sensitive data privacy. As a result, encryption is used in many large data applications. The primary information security need has led to various cryptographic algorithms implementing security on multiple dimensions for significant

security objectives such as confidentiality, integrity, and availability. Cryptography is one such safety standard. Information security is greatly aided by cryptography [5]. The word "cryptography" comes from Greek and means "study of concealed secrets." It may be characterized as approaches or methods used to guarantee information communication security between two parties. It is an excellent and reliable technique for guaranteeing data and network security [6]. The information is kept absolutely confidential and is of the highest integrity.

Several techniques, including encryption, decryption, signature, and creating pseudo-random numbers, are used to achieve this. Cryptography is based on four essential concepts that ensure the confidentiality of the information, data integrity, inauthenticity, and non-repudiation. Cryptography protects secrecy by providing a set of principles that restrict access to sensitive information. On the other hand, data integrity is maintained by ensuring consistency and dependability throughout the application's lifespan. Encryption is the way of transforming data into ciphertext, while decryption is the way of converting ciphertext into readable data (plaintext). Secret information, such as passwords and keys, is used in decryption and encryption techniques [7]. Previous research [8, 9] highlighted specific RSA (Rivest, Shamir, and Adleman) drawbacks by analyzing the impact of the relaxed method with weak public and private keys, the integer factorization issue, and certain other relatively low selection attacks. The above weaknesses do not severely compromise the RSA cryptosystem's overall security but allow erroneous parameter selection and comprehension of the underlying mathematics. An overview of previous findings, detailed explanations of specific attacks, and how the suggested methodology would avoid them are provided. This study's primary contributions are devolved a hybrid algorithm depending on RSA and Diffie Hellman (DH) key exchange to achieve better security in the shortest time. An effective hybrid proposed algorithm was developed to address and avoid the security issues mentioned above. In this research paper, RSA algorithm keys generation (e,d) is used as input for Diffie Hellman, then will encrypt and decrypt data by XORing it with a key. So, the proposed algorithm MRSADH will be used to accelerate the conventional RSA algorithm process, which will lead to enhanced security and avoid limitations and treat drawbacks. It was the major advantage of the proposed methodology, which was not focused on in the previous study because various earlier studies concentrated exclusively on one direction: increasing security or time complexity.

2. History of cryptography

The fundamental perception of using encryption dates back to unusual symbolic symbols scratched onto Old Pharaoh of Egypt sites circa 1900 BCE. It was planned to deliver messages in a way that would make them easy for the receiver to know if they knew how to interpret them—within the 6th century BCE, communicating involved wrapping a piece of paper around a room and then indicating the message it contained. When the paper was unrolled, it was then given to the recipient, who could easily understand the message if he knew the size of the particular chamber [10]. Julius Caesar employed a simple switchover code, known as the Caesar figure, 2000 years ago. In the 1200s, Roger Bacon illustrated a variety of tactics. In 1585, Blaise de Veneer explained the polyalphabetic replacement figure in a circulated work on cryptology. The administration used secret codes to communicate with a network of spies dispersed throughout India, where mystery writing was more common. We present two of humanity's extraordinary accomplishments. One of these particular finger correspondences is still used today. This type of correspondence was defined as "nirabhasa" in ancient India, where finger joints spoke to vowels and other portions were used for consonants. The second aspect of Indian advancement in ancient times is that they are responsible for the first reference in written history to using cryptanalysis for political independence [11].

2.1 Types of cryptography "symmetric & asymmetric"

As previously noted, encryption encrypts or decrypts messages that need to remain private using keys or passwords. This is constructed and achievable by two kinds of key-based cryptographic algorithms: symmetric (commonly called the secret key), which uses one key for encryption and decryption, and asymmetric (further known as the public key), which requires two separate keys: a Public Key for encryption that is shared publicly and a Private key for decryption.

2.1.1. Symmetric key cryptography:

Previous to the 1970s, the single encryption technology was symmetric-key cryptography [12]. It is classified as private cryptography or traditional techniques. It was also the most extensively utilized cryptographic technique. The encrypted message used in symmetric key encryption was known as the classical encryption method long before computers

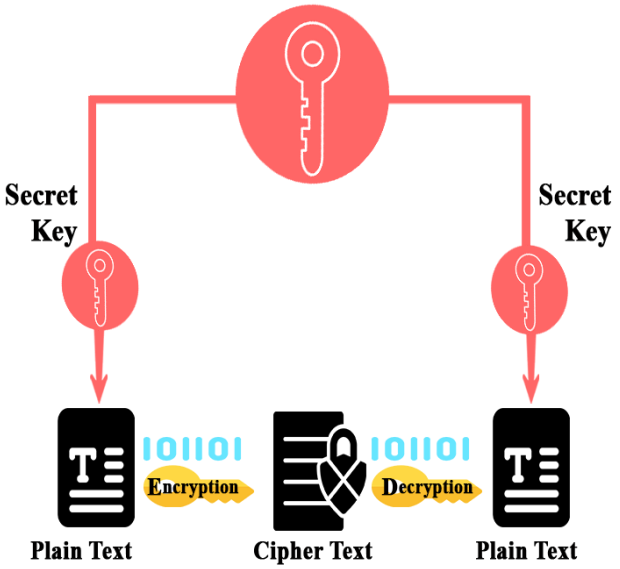

Figure. 1 Symmetric key cryptography

were invented. As computational technology has advanced, symmetric encryption employs bits and bytes as encryption keys and numerous encryption methods to turn the original message into ciphered text. In symmetric key cryptography, the plaintext of encrypted messages is retrieved using the same key used for encryption and decryption. The transmitter and receiver of the message share the secret key, which makes this possible. This explains that if a third party acquires the key, they can decode the communication. In other words, because the sender and receiver of the message both know the same shared secret, the common key will encrypt and decrypt communications. Although symmetric key data encryption is simpler and quicker than public-key algorithms, it has significant drawbacks, including the need for many parties to agree on secret keys. The length of the key, which must be carefully preserved and transferred across participants, determines the resilience of symmetric encryption. This type of encryption cannot guarantee a non-repudiation method when used to sign a message. As a result, the key must remain as secret as possible. The symmetric key cryptography encryption and decryption mechanisms are demonstrated in Fig. 1.

Data encryption standard (DES), triple data encryption standard (TRIPLEDES), advanced encryption standard (AES), RC_2, RC_4, RC_5, RC_6, and Blowfish are among the most widely used symmetric key approaches. Two fish are among the most common symmetric key approaches. Because of its improved processing capability, the 3DES technique was developed to make brute-force cyberattacks effortless [13].

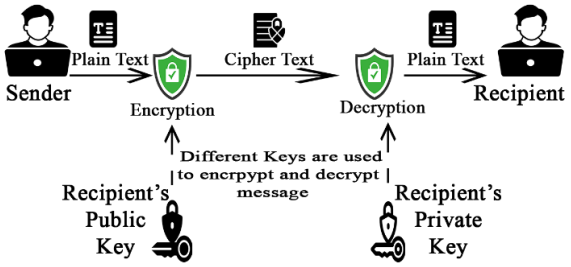

Figure. 2 Asymmetric cryptography

2.2 Asymmetric key cryptography

Asymmetric key cryptography requires two distinct keys: one for decryption and the other for encryption. The encryption public key is released to the public, while the decryption "private" key remains secret. As a result, anybody with access to the public key may encrypt the data, but only the authorized individual (who has access to the private key) can decrypt it. Fig. 2 depicts the behavior of asymmetric "Public Key" cryptography.

Even if the encryption "public-key" is shared with all users/devices participating in the session, the decryption "private key" should be only for the targeted user or device. The public key technique has many advantages, the most prominent of which is better security; private keys are not required to be transmitted to anybody, making them immune to man-in-the-middle (MITM) attempts and attack trials. Another important aspect is the effectiveness of asymmetric key cryptography algorithms to provide cryptographic non-repudiation capabilities, frequently associated with digital signatures. Authenticating the private key needs both the exchange of the private key and the confidence of a third party. As a result, non-repudiation couldn't be guaranteed since a sender could announce that the shared key was broken by any of the partners who shared the secret, allowing him to reject the previously authenticated message.

But on the other hand, because each user is personally accountable for preserving his private key, it can guarantee non-repudiation. The main downside of Asymmetric public key cryptography is its slowness over processing and time. Symmetric keys cryptography encryption techniques are thought to be more effective over time than public-key encryption approaches. The primary drawbacks of asymmetric cryptographic algorithms are their speed. Asymmetric cryptographic algorithms are significantly slower than traditional algorithms and more prone to intruder assaults but allow for key exchange. So, the ideal encryption solution is obtained by merging two cryptographic encryption

algorithms to obtain both the maximum Security of Asymmetric key systems and the fast speed of Symmetric key encryption algorithms. Asymmetric popular cryptographic techniques include Rivest, Shamir, and Adleman (RSA), Elliptic Curve, and digital signature.

3. Literature review

The literature [14–26] presents various methods for enhancing and changing security algorithms to estimate greater security in the shortest time. In [14], a model integrating the Diffie-Hellman (DH) key exchange with the asymmetric Key RSA cryptography scheme is designed to prevent the MITM attack. The model's performance was evaluated against the DH key-sharing algorithm and the RSA cryptography method. This study aims to safeguard the DH Key distribution algorithm using the RSA cryptosystem so that MITM attacks have little to no impact. Still, the scope of the described study is limited to simple integer values with the restrictions of considerable work for larger key-size bits that will lead to security breaches and vulnerabilities.

For many purposes, the internet is a vital component. Introducing secure data communication across an unprotected network is a major difficulty. In [15], a modified version of the RSA technique is presented. It utilized public-key cryptography technology to minimize the RSA algorithm's complicated computations. It has a novel approach to determining the values of k and l. The RSA algorithm's main weakness is that it takes time to produce the key. Therefore, a novel approach is provided for calculating the value of the encryption "Public Key" and decryption key "Private key". A new mathematical method has been developed for determining the plaintext (M) and ciphertext (N). By using this formula, they were able to streamline the difficult mathematics involved in figuring out the key, the ciphertext (N), and the original message. The approach is exemplified with examples and a block diagram. Based on the results, we discovered that while the security results were better than traditional RSA, there were still performance complexity issues due to many mathematical equations.

In [16], a modified RSA Random Bit Insertion Algorithm (RBMRSA) was introduced that transforms the ciphertext into a more complex structure that an attacker cannot easily decipher, even when the attacker has access to the secret key, which increased the RSA cryptosystem's security level without lengthening the keys. This increases reliability and efficiency. In this work, bit insertion is proposed to efficiently address the flaws in conventional RSA cryptosystems and accomplish a high penetration level as well as effective protection from different RSA attackers. Since RSA security requires strong primes, which of Fermat's three prime numbers is required to provide both encryption and decryption keys is tested by Fermat's little theorem. This research's main objective is to create efficient bit insertion methods for modified RSA, having the following objectives in mind:

- Explore the benefits and limitations of the traditional RSA cryptosystem.
- An improved bit insertion algorithm is presented to encrypt and decode messages in the RSA method with the three prime numbers P, Q, and R to guard against popular RSA attacks.
- Set the planned system into action and assess its performance.
- Using RSA, compare the proposed system to traditional RSA.

A hybrid strategy that provides high-level data protection must be developed, considering exchanging information through the Internet. Today's digital world makes data protection a top priority. As more vulnerable algorithms are created, data security may be compromised. Three kinds of data security are proposed to be provided by a hybrid method [17]. The first layer of protection is created when the ciphertext is created. The ciphertext is created using the RSA algorithm. Creating a quick response (QR) code is the effect of the second layer of security, while steganography is used in the third security layer. The QR code included within the image is masked using the least significant bit (LSB) technique. Steganography or cryptography can be used to secure data, but the efficiency of these methods is less than that of methods created by integrating steganography and cryptography. To overcome the issue with information security, the suggested method provides three levels of data protection. An encryption process provides the first level of protection. The RSA method is used to construct the encrypted message of the secret data. The ciphertext is encoded into a QR code to deliver the data with an additional degree of protection. Steganography offers a third degree of security. The created QR code is inserted into the cover picture using the LSB approach. Due to the use of three layers for encryption, including traditional RSA, QR Code, and LSB, the success rate is lower when compared to the proposed method, as the researchers primary concern is to encrypt the data with great care and complexity without regard for

execution time or performance for encrypting large messages.

In [18], Cyberattacks have become more diversified. Cyber-attacks cause major concerns in the modern digital revolution. As malicious attacks are more prevalent, digital infrastructure needs further initiatives to combat them. Maintaining strong data security has become a significant problem since it is necessary to store health, personal, professional, and financial information online for various reasons. Consequently, a method based on RSA and DH was created to enhance the requirements for data transmission security. Better security is required for the expanding number of devices. The provided method may be used to increase security since it contains more input values than traditional algorithms. Because the algorithm combines various mechanisms, the result indicates that it takes longer than the RSA algorithm. Though it takes more time, it can be said that it is more secure than the conventional RSA algorithm, which will ensure better security. In addition, we believe the proposed algorithm to be superior to this approach because it achieves greater security in the shortest amount of time.

In [19], The principles of cryptography are examined. It relies on RSA's advancement and the strength of cryptographic keys to increase the Security of RSA-using apps. RSA method improved by raising the complexity to three keys (3K). This feature enhances algorithm speed, security, and complexity while maintaining decryption and encryption speeds, and it presents a mechanism for improving cryptographic security through public key cryptography. Furthermore, the RSA algorithm provides double protection. The variation from the standard 2-key algorithm is a clear difference. Still, there is one negative: the time of encryption, which is a small difference compared to the first algorithm, and this is calculated to be a strong advantage and an excellent effect in the rate of error and the timing of encryption. And cryptography is a good way to improve data security. RSA 2key is superior to RSA 3key because it takes much less time to encrypt and decrypt data than RSA 3key. Consequently, the proposed MRSADH is better than this method in terms of time consumption.

In[20], The DH protocol is a technique. is a method that ensures communication between two users by allowing the distribution of secret keys across an unsafe connection. No user has evidence that they are communicating with the correct target person when sharing DH keys since a "Man can find shared keys in the middle." This study proposed the DRA model to improve the security of DH key exchange, especially as computational capacity and computer speeds advance. The DRA model unifies the three cryptographic algorithms DH, Rivest Shamir and Adelmann (RSA), and advanced encryption standard (AES). Researchers presented a hybrid DRA model that encrypts and decrypts the keys exchanged by the DH algorithm using both RSA and AES. The RSA method is used to encrypt the keys first, followed by the AES algorithm, and the reverse is true for decryption. Due to the comparative analysis done between their DRA model and the other alternatives, they are convinced of the dependability of our solution. We must expand our research efforts by fusing several techniques to provide better security in order to address the issues brought on by the problems produced by the increasing development of computer performance and processing capacity as well as the appearance of quantum computers. The outcomes demonstrate how well their model works. shows how effective this model is when compared to the SSEJAD model. The results given show that this model is substantially more effective than the SSEJAD model, which has replaced earlier approaches including S-WANE, New-Two-Pass, STS, and HMQV.

In [21], Cloud data storage is concerned with data security. The cloud computing does, however, provide several additional security issues that have not been fully examined. They have suggested a practical solution with multiple data integrity and privacy elements to guarantee the security of the user's data stored in the cloud. The main topics of this study are the obstacles presented by cloud data storage methods and the security of virtual environments. They offer a new method for securing cloud data storage that makes use of a public key cryptography system and the logic behind a modified RSA algorithm. This work provides a method to protect data privacy in a cloud-based environment. Therefore, only the authenticated user should use the secret key that can be properly decoded to access the data that is contained in their suggested job. It can be concluded that the time of key generation of Modified RSA (MDSA) is higher than that of RSA. The comparison of the encryption time between RSA and the proposed Modified RSA (MDSA) scheme illustrates that for the lower bit length of prime numbers, the two algorithms consume an almost identical amount of time. But with the increase in bit length, the difference between curves rises rapidly.

In [22], The presented methodology in this study uses the enhanced RSA method for key generation for authentication, enhanced Kerberos, and enhanced digital signature for authorization. The present RSA technique uses two prime numbers to generate private

and public keys. When two prime numbers are used, the RSA technique is vulnerable to various attacks, including plain text attacks, chosen cipher attacks, factorization attacks, attacks on the encryption key, and attacks on the secret key. These attacks attempt to discover the encryption and decryption keys. To overcome these challenges, they first developed the Enhanced RSA Algorithm, which increases security by using four prime integers rather than only two. In network security various techniques and properties play a crucial part in establishing network security. These features, known as security metrics, can quantify security in computer networks. This method required more time for encryption and decryption as it used four prime numbers for key generation and the standard RSA equation for encryption and decryption.

In [23], The DH protocol is described as a technique and method that ensures communication between two users by allowing the distribution of secret keys across an unsafe connection. No user has evidence that they communicate with the correct target person when sharing DH keys since a "man can find shared keys in the middle." The DRA model was suggested in this work to increase the Security of DH key exchange, particularly as computing power and speed increase. The three cryptographic algorithms, DH, RAS, and AES, are combined by the DRA model. Researchers have developed a hybrid DRA model that uses both RSA and the advanced encryption standard (AES) to encrypt and decode the keys distributed by the DH algorithm. The RSA method is used to encrypt the keys first, followed by the AES algorithm, and the reverse is true for decryption. Due to the comparative analysis done between their DRA model and the other alternatives, they are convinced of the dependability of the solution. The authors achieved the security complexity goal but with more time consuming as they used RSA and AES for securing DH key exchange.

In [24], It's a very well-known public-key implementation method, named after Massachusetts Institute of Technology (MIT) researchers who initially developed the idea in 1977. Their names were Leonard Adleman, Adi Shamir, and Ronald Rivest. AES stands for Advanced Encryption Standard. RSA is a symmetric key encryption mechanism frequently used to protect data where secrecy is critical. The algorithm's security is based on the rigidity of assessing many compounds and a complex number for a given odd integer (e) computation of the unit of moral origins. The public-key encryption key is made up of an integer pair (P, Q). The outcome of multiplying two primes is typical. Use RSA's key feature, variable key size, and cipher block to better security. The public keys are shared with all users, but the secret key is only recognized by one (the recipient). The primary disadvantage of this key coding is that it is more time-consuming than symmetric methods. There are two types of keys: public keys and private decryption keys. Although the encryption "public key" is generally known, the decryption "private key" is kept confidential. Asymmetric cryptography encrypts data using the encryption key, which can only be decrypted with the secret key.

4. The Proposed algorithm (MRSADH)

This section explains the proposed methods for securing and safeguarding information in two rounds. There are two aspects to the proposed integration of the MRSADH method. The initial exchange of MRSADH algorithm keys. The message is encrypted and decrypted in the second step using the XOR function. However, two keys are generated on both ends using the modified RSA and DH method: the sender key for encryption and the receiver key for incoming message decryption. The MRSADH encryption process is the core of the first phase. The key-generating process occurs during the first step, the encryption phase (e,d). For use in the DH, to create both pairs of keys (public and secret key producing encryption and decryption keys), the key generation process requires two separate random prime integers (p, q). The result of the first step of our proposed methodology (MRSADH), which encrypts data using XOR to produce the encrypted text, was acquired in the second phase (Ciphertext). Decryption is performed in the third stage by XORing a cipher text with the decryption key. Fig. 3 demonstrates the several stages of MRSADH, and the steps are described below:

4.1 The first phase (key generation):

The encryption procedure begins with this phase, which entails the receiver producing both the Secret and public key. In this modified RSA scheme, the intended recipient generates the public and secret keys using the following mathematical computations. The critical and essential initial stage in the encryption process is key generation. Different prime values p and q can be most reliably predicted through the key generation phase. The public key is created using the key construction technique and two different prime values, p, and q. The secret keys "d" and encryption keys "e" are inputs for the DH Algorithm's encryption and decryption key generation.

Using RSA:

1. Randomly choose the two prime numbers p and q while (1)

2. Next, calculate modulus $n = (p \times q)$ (use prime integers with big values to maximize factorization complexity). (2)

Find Φ= (p – 1) (q – 1). (3)

4. After that, the exponent e should be selected so that1<e< Φ (n) and gcd (e, Φ (n))=1. (4)

5. Next, a secret component d must be created using the formula d = e−1 mod Φ (n), where (n, e) is the public key and d is the secret key. (5)

secondly, using (DH) algorithm:

Due to the DH algorithm's invisibility within a networking system, it has gained popularity. When data is encrypted over the internet using transport layer security (TLS) or secure socket layer, this technique is typically used (SSL). The secure shell (SSH) protocol also regularly uses the DH algorithm. The next steps for using the DH algorithm will depend on the RSA steps listed before.

6. Assume that $G = n(p \times q)$ and R, S, and G are automatically created prime constants. (6)

7. Finally, make E and D's values from above into secret integers so that A=e and B=d. (7)

8. Determine the following as an encryption and decryption key. (8)
X= (G^A) mod R
Y= (G^B) mod R

9. Either $K_A = (Y^A)$ mod R or (9)
$K^A = ((G^B \text{ mod } R)^A)$ mod R
$K_A = ((GB)^A)$ mod R ➔ $K_A = (G^{BA})$ mod R
$K_B = (X^B)$ mod R or
$K_B = ((GA \text{ mod } R)^B)$mod R
$K_B = ((G^A)^B)$ mod R ➔ $KB = (G^{AB})$ mod R
So that KA = KB = K.

4.2 Encryption process:

To encrypt our plain input text, we XOR it with the session key (K) we received in step 9.

4.3 Decryption process:

To get our plain input "original message", we XOR encoded with the session key (K) for decryption.

5. Experiment, results, and discussion

Data protection is essential, so cryptography is a powerful technique for achieving information privacy, secrecy, authentication, and integrity. Following our planned ' 'methodology's successful implementation of the described algorithms, multi-level cryptography was enforced through RSA and DH (MRSADH). To produce the public and private keys for the following stage, RSA procedures are implemented. The proposed approach also includes generating an encryption key using the RSA public and private keys mentioned above and utilizing the encryption key to encrypt data. Finally, encrypt and decode the data (Arabic and English) with an encryption key obtained from DH and XOR. In this study, the coding process calculation comes from the combination of the RSA and DH algorithms that will be implemented in the software. This study's coding technique utilizes hybrid cryptographic algorithms based on a combination of the RSA algorithm, a sample of asymmetric cryptography, and the DH algorithm, an example of symmetric cryptography (MRSADH) in Python.

The software makes it easier to test the coding output. Because a laptop machine is used to determine the performance of the key generation, encryption, and decryption processes, the laptop's capabilities are as follows:

- a) Using the Windows 10 Operating System and visual studio code version: 1.69.2 (user setup)
- b) Supporting hardware: Laptop HP Intel(R) Core (TM) i7-8565U CPU @ 1.80GHz, 1.99 GHz, 8 GB RAM, a 1TB hard disk.

5.1 Analysis of security and performance assessment

This section will look at the effectiveness and security of the proposed MRSADH technique. This proposed study will employ the MRSADH algorithm, and the outcomes will be contrasted with those from several other methods.

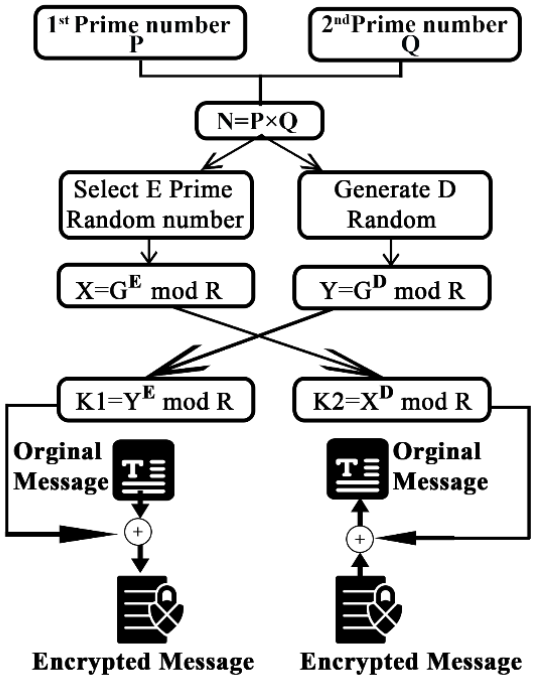

Figure. 3 The proposed (MRSADH) hybrid cryptosystem

Table 3. Encryption time

	Prime numbers	Proposed Algorithm	RSA
1st Prime numbers	(1008001,281)	10.578125	14.9063
2nd Prime numbers	(9804787,349)	437.71875	414.563
3rd Prime numbers	(9969919,409)	504.46875	517.906
4th prime numbers	(10028279,541)	666.328125	710.375

5.1.1. Execution time:

The effectiveness of any specific encryption and decryption technique depends on the time it takes to perform any cryptographic process. The period of execution identifies the algorithm's speed or slowness. The proposed algorithm MRSADH and classical RSA's encryption and decryption results are displayed in Tables 3 and 4, respectively. It is evident from the results in Tables 3 and 4 that the computational complexity of the MRSADH encryption and decryption algorithms is greater than that of classical RSA, indicating that the algorithm will be quite complex with the shortest time for execution.

Table 4. Decryption time

	Prime numbers	Proposed Algorithm	RSA
1st Prime numbers	(1008001,281)	0.0017703	0.00056
2nd Prime numbers	(9804787,349)	0.0009049	0.00277
3rd Prime numbers	(9969919,409)	0.0005246	0.00172
4th prime numbers	(10028279,541)	0.0005579	0.00202

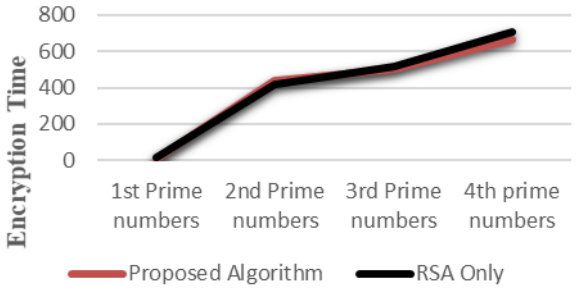

Figure. 4 Encryption time

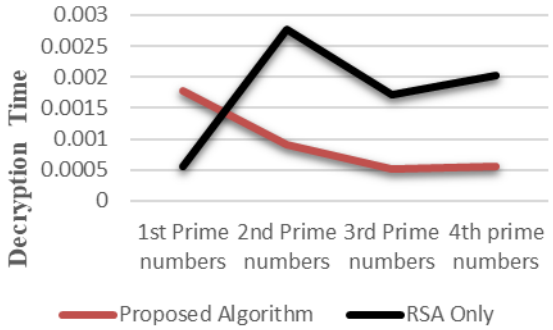

Figure 5. Decryption time

Fig. 4 compares the encryption times for the proposed MRSADH algorithm and classical RSA when plotted against identical message sizes. Fig. 5 includes a graphical comparison of the decryption times for the proposed MRSADH and Classical RSA algorithms.

Furthermore, when compared to other papers, we notice that all improvements are made only to enhance security, with little care for performance, as seen In [1,8]. Fig. 6 compares the time complexity for generating keys only In [1] to the proposed method and the time complexity for all of our suggested steps, including encryption.

Also, the proposed MRSADH and Modified DH "MDH" in [25] were compared using the following

Table 5. Key generation time

Algorithm	Algorithm in[14]	RSA	DH	MRSA DH
Time	0.0056461	0.006082	0.008837	0

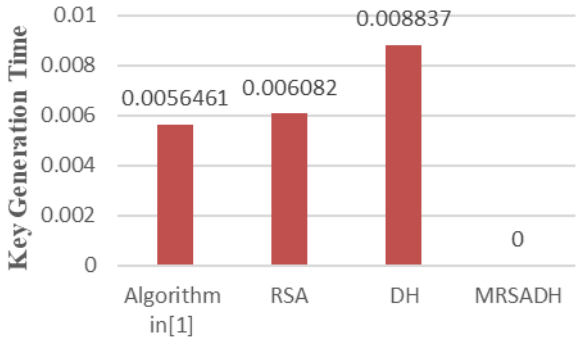

Figure. 6 Asymmetric key generation

Table 6 MRSADH and MDH COMPARISON

Key Size	MRSADH	MDH in [25]	TimeDifference
64 – bits	1.2362679	27.72387	95.54%
128– bits	30.1546777	66.71367	54.80%
512– bits	180.79456	271.9631	33.52%

criteria: 64 bits, 128 bits, and 512 bits key lengths by selecting random prime numbers. Table 6 compares the performance of the proposed Algorthim MRSADH and MDH. MRSADH produces much faster results than MDH.

5.1.2. Avalanche effect

The avalanche effect is the variance in ciphertext caused by a little change or variation in plaintext [16]. For a small change in the input, a successful cipher or encryption method must produce entirely different results. The degree of changes in the ciphertext is proportional to an algorithm's level of security, i.e., the higher the algorithm's avalanche effect, the higher its security level. As a result, it will be challenging for an attacker to perform statistical analysis. The goal of flipping just one bit in the avalanche effect (%) is to test the sensitivity of the proposed algorithm by examining whether even the smallest change in the plaintexts would completely produce a radical or huge change in the ciphertext.

$$\text{Avalanche effect (plaintext)} = \frac{\text{Count of changed bits in ciphertext}}{\text{Total bits in the ciphertext}} \times 100$$

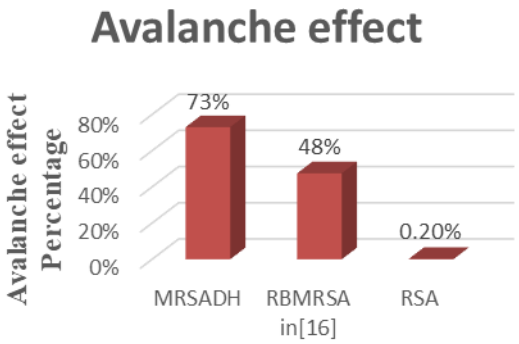

Figure. 7 Avalanche effect

Compared to an estimated 0.2% for RSA and 47.52% for RBMRSA in [16], changing one bit in the plaintext of MDRSA caused a 71% change in the ciphertext, where the value in% stands for the avalanche effect. Fig. 7 provides a visual representation of the percentage of the avalanche effect.

5.1.3. Discussion

The experiments' conclusions showed that, compared to other algorithms, the proposed algorithm produced outstanding results. MRSADH succeeded in achieving better security complexity with a lower execution time and preventing MITM attacks. Comparing the proposed method with traditional RSA and cutting-edge techniques may help you better understand the results in Table 3 and Table 4. The findings demonstrated that the proposed MRSDH produced faster encryption and decryption time than conventional RSA algorithms. Consequently, the proposed method achieved a better execution time compared to Ref [16], Ref [18], Ref [19], and Ref [22], as all this work compared results with standard RSA, and it shows that the new algorithms took more time. Table 5 clarifies that the proposed algorithm is more efficient for generating the key in no time with randomly selected prime numbers, which will increase the efficiency of the proposed algorithm and lead to its reliable use in our daily digital transactions. In addition to increasing security complexity and decreasing execution time, MRSADH achieved a high avalanche effect compared to Ref [16], as shown in Fig. 7.

6. Conclusion and future work

The digital world is a major aspect of a variety of objectives. Delivering secure data communication across an unsecured network is a significant challenge. Data should be secured from unwanted access because of increased online message sharing.

To further improve information security, a hybrid technique is proposed for securely sharing messages over the internet. To provide levels of privacy protection, the proposed hybrid algorithm combines RSA and Diffie-Hellman (MRSADH) to achieve better security. Depending on RSA and Diffie Hellman, a hybrid security approach to messages was created. Python programming language was used to implement this method. Overall, the results demonstrated that a hybrid algorithm is a promising approach for protecting the transmission of private and sensitive communications across an untrustworthy network. The proposed solution is suitable for high-security cases without much execution time. Our future upcoming work will focus on developing an online cryptography method that will effectively tackle today's real-world digital transformation challenges.

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

Conceptualization, Omar Salah;

methodology, Omar Salah, Mohamed Taha; software, Omar Salah; validation, Mohamed Taha, and Ahmed El-Sawy; investigation, Mohamed Taha, Ahmed El-Sawy.

Resources, Omar Salah; writing—Omar Salah; writing—review and editing; Mohamed Taha, Ahmed El-Sawy; supervision, Ahmed El-Sawy, Mohamed Taha.

References

[1] A. Liaqat and F. Liaqat, "Covid-19 Impact on the Internet, User Experience and Economy in Pakistan", In: *Proc. of the 6th International Multi-Topic ICT Conference (IMTIC)*, Jamshoro & Karachi, Pakistan, pp. 1-5, 2021.

[2] A. Gupta , S. Gupta, and N. Yadav, "Enhancement of security using B-RSA algorithm", *Inventive Communication and Computational Technologies*, pp. 439-450, 2020.

[3] P. Matta, B. Pant, and U. K. Tiwari, "DDITA: A Naive Security Model for IoT Resource Security", In: *Smart Innovations in Communication and Computational Sciences: Proceedings of ICSICCS 2017*, pp. 199-209, 2019.

[4] P. Matta, M. Arora, and D. Sharma, "A comparative survey on data encryption Techniques: Big data perspective", In: *Materials Today: Proceedings*, Vol. 46, pp. 11035-11039, 2021.

[5] C. Gupta and N. S. Reddy, "Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography", *Journal of Physics: Conference Series*, Vol. 2161, No. 1, p. 012014, 2022.

[6] S. R. Maniyath and V. Thanikaiselvan, "An efficient image encryption using deep neural network and chaotic map", *Microprocessors and Microsystems*, Vol. 77, p. 103134, 2020.

[7] V. C. Osamor and I. B. Edosomwan "Employing scrambled alpha-numeric randomization and RSA algorithm to ensure enhanced encryption in electronic medical records", *Informatics in Medicine Unlocked*, Vol. 25, p. 100672, 2021.

[8] M. Mumtaz and L. Ping, "Forty years of attacks on the RSA cryptosystem: A brief survey", *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 22, No. 1, pp. 9-29, 2019.

[9] M. A. Islam, Md. A. Islam , N. Islam and B. Shabnam, "A Modified and Secured RSA Public Key Cryptosystem Based on "n" Prime Numbers", *Journal of Computer and Communications*, Vol. 6, No. 3, pp. 78-90, 2018.

[10] D. K. Sharma, N. C. Singh, D. A. Noola, A. N. Doss, and J. Sivakumar, "A review on various cryptographic techniques & algorithms", In: *Materials Today: Proceedings*, Vol. 51, No. 1, pp. 104-109, 2022.

[11] M. Sowmiya, S. Subeksha, T. Vanmathi, and P. Vidhupriya, "INFORMATION SHARING ACROSS ORGANIZATION USING SYMMETRIC KEY ENCRYPTION", *International Journal of Computer Science and Mobile Computing*, Vol. 9, No. 4, pp. 44-48, 2020.

[12] J. Jamaludin and R. Romindo, "Implementation of Combination Vigenere Cipher and RSA in Hybrid Cryptosystem for Text Security", *International Journal of Information System and Technology*, Vol. 4, No. 1, pp. 471-481, 2020.

[13] S. A. Busafi and B. Kumar, "Review and Analysis of Cryptography Techniques", In: *Proc. of 9th International Conference System Modeling and Advancement in Research Trends*, Moradabad, India, pp. 323-327, 2020.

[14] C. Gupta and N. Reddy, "Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography", *Journal of Physics: Conference Series*, Vol. 2161, No. 1, p. 012014, 2022.

[15] S. B. Das, S. K. Mishra, and A. K. Sahu, "A New Modified Version of Standard RSA Cryptography Algorithm", *Smart Computing*

Paradigms: New Progresses and Challenges, Vol. 767, pp. 281-287, 2020.

[16] F. O. Mojisola, S. Misra, C. F. Febisola ,O. A. Alli, and G. Sengul, "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.

[17] B. S. Spoorthi and S. P. Mala, "Three-Level Hybrid Data Security", *Advances in Intelligent Systems and Computing*, Vol. 1397, pp. 313–321, 2021.

[18] H. S. Mondal, M. T. Hasan, M. M. Hossain, M. M. Arifin, and R. Saha, "A RSA-Based Efficient Dynamic Secure Algorithm for Ensuring Data Security", In: *Proc. of International Joint Conference on Computational Intelligence*, pp. 643–653, 2020.

[19] I. A. Barazanchi, S. A. Shawkat, M. H. Hameed and K. S. A. Badr, "Modified RSA-based algorithm: a double secure approach", *Telecommunication Computing Electronics and Control (TELKOMNIKA)*, Vol. 17, No. 6, pp. 2818-2825, 2019.

[20] A. Ahmed, M. F. Nanne, and B. Gueye, "A hybrid model to secure the exchange of DH keys", In: *Proc. of 2021 International Conference on Computer Communication and Informatics*, Coimbatore, India, pp. 1-5, 2021.

[21] Y. K. Kumar and R. M. Shafi, "An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem", *International Journal of Electrical and Computer Engineering*, Vol. 10, No. 1, pp. 530-537, 2020.

[22] R. Balajisrinath and P. Ananthi, "NETWORK SECURITY ALGORITHM WITH ENHANCED RSA", *International Journal of Advanced Engineering Science and Information Technology*, Vol. 9, No. 5, pp. 39-43, 2022.

[23] A. Ahmed, M. F. Nanne, and B. Gueye, "A hybrid model to secure the exchange of DH keys", In: *Proc. of International Conference on Computer Communication and Informatics*, Coimbatore, India, pp. 1-5,2021.

[24] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein and H. F. A. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques", *IEEE Access*, Vol. 9, pp. 31805-31815, 2021.

[25] J. E. Avestro, A. M. Sison, and R. P. Medina, "Hybrid Algorithm Combining Modified Diffie Hellman and RSA", In: *Proc. of the 4th International Conference on Technology, Informatics, Management, Engineering & Environment*, Bali, Indonesia, 2019.