Received: November 9, 2023. Revised: February 8, 2024.

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, DH, and AES

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: The connected digital environment generates massive amounts of data that must be protected from unauthorized disclosure. Technological advancements and the creative techniques attackers use can exacerbate data security breaches. Security protocols and cryptographic algorithms are the two components of information security, the last being information security's basis and fundamental technology. The cryptographic conception will improve and assure security while also protecting network resources that are exchanged. The goal of this study is to demonstrate the few encryption algorithms that are used to encrypt data on an unsecured network. This research presents a new hybrid encryption strategy for encrypting data. MRDAES encrypts data using Rivest, Shamir, Adleman (RSA), Diffie Hellman (DH), and the Advanced Encryption System. The data will be encoded in two stages: the first by producing the encoded data using the XOR function, and the second by using AES to encode data and obtain the final result to be shared with intended reception with high-security complexity compared to other methods in terms of performance and avalanche effect. The proposed study examines the three most widely used cryptographic symmetric and asymmetric algorithms, RSA, Diffie-Hellman, and AES, and how they operate and impact security and complexity when integrated into a unified hybrid (MRDAES) computation with the proper adjustments. The study also presents an approach for increasing data security while minimizing the number of mathematical equations and obtaining high-security complexity while slightly increasing execution time with chosen large random prime numbers. The results indicate that the new hybrid technique (MRDAES) has more efficient performance and avalanche effect inputs with a minor increase in execution time. The proposed approach MRDAES produced more advanced complexity than classical RSA existing methods and others. According to avalanche effect data, the proposed technique provides better results with a higher percentage than existing algorithms on modified RSA Random Bit Insertion Algorithm (RBMRSA) and classical Rivest, Shamir, and Adleman (RSA). The proposed approach enhances the avalanche effect by 88% compared to 48% achieved by an RBMRSA, with a 40% increase and 87.80% compared to RSA.

Keywords: Encoding, Decoding, RSA, DH, AES, RBMRSA, Avalanche effect, MRDAES.

1. Introduction

Considering the expanding popularity of network technology, various computers, and communication technologies represent an individual's daily environment, the introduction and growth of personal communication, emails, online e-payment, automated retail business control, and fintech transactions, among other things. They collect, analyze, store, display, and convey information in digital multimedia formats as separate entities to provide society with political, financial, economic, armed forces, and cultural facilities or when integrated with other physical products. So, in today's digital world transformation, we are situated in a digital era. We can now accomplish most of our work on many virtual digital internet and various applications platforms [1]. Since most digital social work data and transactions are carried at rapid speeds by computer networks as carriers, regardless of whether it is private or commercial information, since information security is in danger of being compromised or decoded, resulting in varied degrees of brokenness, it should be one of our top priorities for each individual. In this regard and manner, we should employ almost every kind of information securely and efficiently has become a critical pillar in ensuring the growth of digital humanity's environment: how to prevent information from being illegally stolen, eavesdropped on, forged, retrieved, and tampered with during the transmission and processing of information on the publicly accessible network, i.e., the issue of information authentication and confidentiality, has become a problem that people are scared about; as a result, the theory of information authentication and confidentiality has become a problem that people are focused on[2]. The concept of cryptography is a major answer to the problem of data insecurity. Cryptography is a process for ensuring the secrecy of messages. The term "composing mystery" has a unique significance in Greek. In plaintext, the cipher text is a functioning cycle that varies during the actual message. The scrambling conversation loop recovers plaintext from cipher text [3]. Over the past years, several cryptographic methods have been developed to ensure the highest message security level during transmission over insecure networks and carrier layers. Asymmetric and symmetric encryption methods are two distinct categories of cryptographic encryption techniques. One uses a symmetric key for the data encoding, while the other uses an asymmetric key. In symmetric-key cryptography, data is encoded and decoded with an identical key. However, asymmetric-key cryptography decodes and encodes it using two separate keys. Both techniques have their own set of positive and negative aspects. The symmetric "private" key approach has the benefit of being quick and simple to use. The asymmetric encryption technique is a low-cost, high-efficiency strategy for data security that employs a single safe key, making it less secure. Asymmetric algorithms, "Public key", on the other hand, are slow and difficult, but they provide a higher level of security [4]. Asymmetric key encryption can eliminate the key distribution problem by using asymmetric keys. This procedure implements both symmetric and public keys. A public key is used for encryption, while a private key is used [5-6]. Many challenges may arise regarding data security and protection during transmission [7], [8]. As a result, an efficient and comprehensive strategy for ensuring the safe transfer of sensitive and critical data and its authentication via public networks became necessary [9]. The hybrid encryption technique is intended to be secure and effective [10]. Hybrid cryptography takes advantage of the combined capabilities of private and public key-encoding cryptosystems. It uses the efficiency of the asymmetric "Public key" and the simplicity of the symmetric "Private key". This research aims to provide an enhanced cryptographic method combining three separate symmetric and public key algorithms to encode and decode data in multiple stages. One of this paper's main achievements is the invention of a hybrid algorithm based on RSA, Diffie Hellman (DH) key exchange, and AES to achieve stronger and more sophisticated security. An effective hybrid proposed solution was developed to address and prevent the security vulnerabilities described above. In this article, the RSA algorithm keys generation (e,d) are used as input for Diffie Hellman, which will encrypt data by XORing it with a key as a first-stage encryption. The previous encryption result will be encrypted by using AES as the second phase, and the previous steps will be reversed for decryption. As a result, the proposed algorithm MRDAES will provide increased security, avoid restrictions, and treat disadvantages While maintaining the execution time and not increasing it significantly. It was the main advantage of the suggested technique, which was not addressed in the prior study since past studies focussed just on one direction: improving security or time complexity. The remainder of this article has been structured as follows: Section 2 provides the literature review, Section 3 explains the proposed hybrid algorithm, and Section 4 represents the findings of the security auditing, performance assessment, and discussion. Section 5 has the conclusion, and Section 6 includes the references.

2. Literature review

In [11], Many researchers consider the research to be precious. Researchers who looked into utilizing RSA for file encoding found that it could only encrypt very small file sizes. In addition, the method enables RSA to use powerful key management benefits. Due to the RSA technique's slow performance, the major challenge of protecting large amounts of data was not resolved. Although the level of security in the AES approach was not considered, the "cipher text misappropriation" of the AES technique to promote file encryption to resolve inappropriate data combining to be processed may be attacked depending on specific criteria. There may be some variation in the security degree of protection and protection efficacy, although the AES and RSA algorithms have been utilized extensively in cryptosystems. The suggested hybrid algorithm would require more time and resources since the encryption will be completed by combining and applying AES and RSA full processes. Provide an AES key, an RSA public key, and an RSA private key, then encrypt the AES key-generated cipher text using the RSA public key before encrypting data with the AES key. The research successfully encrypts and decrypts files of a specific size and determines how long it takes to do each step. There could still be some gaps in the study; for example, future research will focus on the possibility of data tampering and forgery when the double key is broken and address large file encryption.

In [12], This study aims to raise awareness of the necessity of data security in Cloud Computing, particularly in the development of home computing, which the global Coronavirus pandemic has prompted. To address the data concerns of privacy and integrity, a genetic algorithm-based (GA-based) cryptosystem was provided to secure data in the cloud. By creating keys for encryption and decryption that are integrated with the cryptographic method, these cryptosystems protect the privacy and integrity of cloud data. To test and validate 10 distinct datasets, the algorithm was tested using the following parameters: throughput, key size, avalanche effect, and execution time. The implementation was based on the crossover and mutation technique processes, which used nature-inspired genetic algorithm operations with randomness and improved high-security levels during data uploading and downloading to and from the cloud and during transmission at the receiver. The Caesar cipher first converts plaintext to ciphertext, and then 128-bit chromosomes of the encrypted text are created. Random point crossover is then done between the ciphertext’s 128-bit chromosomes and a 128-bit key. The child is then mutated by randomly flipping one bit to produce the encrypted text. The simulation results demonstrated the cryptogram’s robustness since it outperforms state-of-the-art encryption algorithms such as Data Encryption System (DES), Advanced Encryption System, Triple Data Encryption System (3DES), Blowfish, and RSA. The authors want to concentrate on reducing the suggested model’s space complexity to alleviate the problem of memory requirements. The algorithm’s ability to encrypt various sorts of data, including photos, video, and audio, was similarly limited. It also gets a low residual percentage for avalanche impact because the maximum avalanche effect is 20%.

In [13], the Authors attempted to circumvent the RSA encryption vulnerability of sending the key “e” and modulus “n” in the clear by applying a new approach of disguising the key “e” and modulus “n.” It employs a mechanism for selecting between a pair of distinct algorithms. Algorithm 1 conceals the encryption key, while Algorithm 2 conceals the modulus. The two algorithms are chosen using an effective random number generator on the Linux /dev/random device. Using this approach increases the time an attacker takes to crack the cryptosystem, increasing the security of the RSA algorithm. The suggested method aims to have publicly sent values different from those used in the traditional RSA algorithm, which conceals the actual parameters from others. The implementation of this idea uses two different algorithms and randomly chooses between them. However, it will take more time to implement without ensuring increased security complexity.

In [14], network applications and systems are growing due to the ongoing development of social information technology, notably the rapid development of Internet technology. A serious obstacle network applications confront is safeguarding sensitive data so that external masquerading and attacks may be successfully avoided. Therefore, the author extensively studies computer security technology, creatively devises a hybrid encryption strategy, depending on the triple DES technique for a more effective data encryption security factor, and uses the RSA algorithm to encrypt the triple DES algorithm key to accredit the data. These goals are to promote the research process of information security in the entire society, improve the security factor of computer data communication, and strengthen computer security management. After the data was encoded, only the 2nd and 3rd batches were corrupted by 0.012% and 0.011%, respectively, with 0.11% and 0.10% of the data corrupted, respectively, the third and fourth sets of data encrypted with the 3DES encryption technique performed poorly in terms of security.

When compared, the DES encryption method performs poorly, corrupting 0.10 to 0.32% of the data over local area network transmission. It can be demonstrated that the author’s method offers the highest level of data security performance. The author uses RSA to encrypt the 3DES key instead of the 3DES encryption technique, increasing the effectiveness of data encryption. The 3DES encryption technique is the most delayed, but DES is the fastest. This is because the 3DES encoding method lengthens the key based on the original algorithm, which lengthens the processing time. Although the author’s method is less effective than the DES algorithm, the optimal encryption result is guaranteed since the difference is about 1 ms.

Consequently, the article algorithm offers the best security performance in computer communication among the three algorithms. The authors apply the RSA encryption technique to improve the single 3DES algorithm and consolidate its performance to assure data communication, data integrity, and encryption performance. Experiments demonstrate that the suggested encryption technique enhances security performance by ten times while being just one millisecond slower than previous algorithms. It performs better encryption than other algorithms and is acceptable for computer data transfer scenarios. However, this suggested approach is the key limitation since it is restricted to a 168-bit key, which leads to poor security complexity.

In [15], This paper suggests merging AES and DES algorithms to strengthen the current encoding methodology. The hybrid algorithm outperforms the traditional methods in terms of performance. Because the average time varies depending on the algorithm speed, AES and its combination with DES performed better in the average time analysis. Because of the similarity, obtaining different times for the same input for encoding and decoding is impossible. The proposed algorithm, a hybrid of two strong encryption standards, will be a reliable and trusted data encryption mechanism. Due to the use of a symmetric key, a double-key approach can also be used to defend against linear attacks. In this situation, the encryption algorithm's security may be improved further. Improving DES security by relocating the operation one bit to the right and incorporating two keys of combining one round of DES with one round of AES to minimize performance time.

In [16], During COVID-19, data security issues became increasingly pressing for the healthcare sector. Since the virus's spread in early 2020, it has been joined by an increasing number of malicious hackers hunting for deficiencies in the healthcare system's data maintenance network. Several nations, including the US, the UK, the Czech Republic, and others, have reported a wave of cyberattacks against national healthcare systems. Given the ubiquity of cyberattacks, one of the significant themes within the healthcare system is the necessity for comprehensive data security maintenance. Security techniques such as Data Encryption Standard (DES), AES, triple data encryption standards (3DES), and RSA encryption can significantly improve the healthcare system's data protection. Because of the use of four layers for encryption, including AES, DES, 3DES, and traditional RSA, 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 [17], Customers greatly benefit from this virtual form of E-banking due to its immense practicality and usability. Electronic banking, often known as e-banking or digital Banking, is an easy digital platform for managing our bank accounts from anywhere and anytime using the internet and a mobile device, laptop, or desktop computer. E-banking provides practically all of the services customers formerly had to visit bank offices and wait in lengthy lines to obtain. E-banking benefits the bank and the client by lowering transaction costs, personnel salaries, and the number of branch offices. The most difficult aspect of Internet banking is security. Technology should protect Customers' accounts securely so they do not experience fraudulent online banking transactions. The authors suggested that the process of implementing digital signatures be presented, after which Elgamal with Digital signatures may be used with suitable code.

Maintaining security for an E-Banking System is a continuous process, and the server receives the message from the consumer. Separate the encrypted message, DS, and other customer credentials, like customer ID and password, from the message. Obtaining the information required for database connection from the server makes a Digital signature out of the encrypted message. Compare the computed Digital signature to the one received by the user. Decrypt the message if both Digital signatures are the same. Otherwise, an error message is displayed. In addition to employing lengthy passwords, the suggested system's degree of security can be further enhanced by using complicated hash functions to implement digital signatures. It is not easy to achieve security for an E-Banking system. It is an ongoing process in which the server receives messages from the client. Separate the encrypted message, DS, and other information from the message, such as the customer ID and password. Obtaining the information required for a database connection from the database server Make a DS out of the encrypted message. Compare the computed DS to the one received by the user. If both DS are the same, the message will be decoded. If not, an error message is generated. However, the proposed solution will take longer based on the preceding sequence. It will be influenced by banking system infrastructure performance specifications such as machine CPU, memory, and customer traffic.

In [18], The project aims to provide an encrypted and secure file storage system for transferring data between clients in a far-away place. This kind of system will need correctly encrypted input using any algorithm ways and will store it wherever. Other users can download the uploaded file, but to view the data inside it, they must decrypt it using the decryption method and the information supplied by the owner to the users. The system employs public-key cryptographic techniques such as RSA and symmetric key encryption such as AES. Hashing techniques like static hashing and dynamic hashing are utilized to perform integrity. Confidentiality is also achieved as a result of data encryption. The existing system's fundamental shortcoming is that it does not consider integrity and authentication. It also employs stenography to allow users to exchange secret keys. The authors offer a system that guarantees integrity, authentication, and secrecy to address these shortcomings. In addition, the suggested system employs asymmetric cryptography rather than stenography to distribute secret keys among users. Authors intend to use asymmetric key cryptography over stenography since it is preferable because it employs a digital signature. It is entirely safe because the file is encrypted using symmetric key cryptography and stenography methods. The technology is extremely safe and stable. The data of the users is protected on a cloud server, which aids in preventing unauthorized access from the outside world; nevertheless, the primary disadvantage of the method suggested is its complexity and time consumption when compared to other suggested methodologies. The current method focuses solely on strict confidentiality and neglects integrity and authentication. The major shortcoming of this approach is that it does not consider integrity and authentication.

In [19], The authors thoroughly examine these difficulties, including AES algorithm implementation, full application, and algorithm comparison with other available approaches. To evaluate the suggested method's performance and fully exploit the benefits of the AES encryption technique, minimizing the round key, optimizing the key schedule, and organically integrating with the RSA algorithm is necessary. Because of its huge library, the Java language is utilized to develop the algorithm; subsequently, to demonstrate the effectiveness of the suggested approach, many metrics have been compared, such as encryption/decryption speed, entropies, and memory usage, with a traditional algorithm. Based on comparing AES and the hybrid AES algorithm findings, the suggested method has good performance and great security, but more time is consumed compared to traditional RSA and AES. The biggest downside of this recommended article's suggested solution is that the RSA public key is communicated via the internet, which allows Man in the Middle to compromise data.

Furthermore, the key will be restricted to 128 bits, which will not provide great security. The suggested algorithm outperforms in terms of encryption, but it would still need to increase its performance by optimizing the decryption time. It also needs to consider memory use as it consumes medium memory while attempting to encrypt and decode tiny file sizes.

In [20], Public-key encryption methods might be combined with symmetric encodings such as AES and DES. DES was the first recognized cryptography standard, which was replaced by AES standards in 2000. By studying and reviewing the RSA, DES, and AES techniques, the authors observed that the asymmetric encryption techniques are slower and perform far worse than the symmetric encryption algorithms such as AES. Asymmetric methods such as RSA and Diffie-Hellman are commonly employed in digital signatures and non-repudiation, as well as symmetric encryption methods such as AES secret key exchange. Despite this, symmetric encryption methods are significantly slower than asymmetric encryption algorithms such as RSA. However, symmetric encryption algorithms (AES, DES) generally ensure only congeniality and no digital signatures or non-repudiation.

Furthermore, transmitting the symmetric encryption secret key across channels and media like the internet is risky. As a result, it is clear that in a hybrid cryptosystem, symmetric cryptography like AES and DES will provide bulk data encryptions like disc encryption, database encryption, and file system encryption. In contrast, asymmetric cryptography like RSA will facilitate the secure key exchange of the symmetric algorithms, the integrity check, and the non-repudiation functions.

In [21], When users share private information when exchanging data on particular networks, it confronts certain key issues in protecting the data and regulating access to it. A practical mathematical encryption approach is necessary to address data propagation throughout the data replacement process. Time and resource consumption efficiency during the authentication process must be assessed since these factors lengthen the authentication procedure depending on the detected danger. The suggested approach enhances network security during communication sharing between network-connected hosts and nodes by adjusting cryptographic and encoding algorithms to ensure information confidentiality and integrity.

- To prevent unauthorized accessibility and unwanted data sharing, the authentication process was enhanced by employing an altered Diffie-Hellman (DH) key exchange.
- Use Distributed Hashing (DH) and a modified Zero Knowledge Proof (ZKP) approach for preventing MITM and Discrete Log attacks. Initially, a modified DH Key exchange was used to provide user authentication. A modified Zero Knowledge Proof

(ZKP) approach and a modified DH are also used to speed up the authentication procedure. The authors discuss the security and processing capabilities of recently created efficient cryptography algorithms. The recommended NC-based DH approach beat the RVV and RVV-AU algorithms in the performance analysis when measuring total delay from start to finish as the node count increased from 10 to 100. Performance evaluation is carried out with the network simulator 2. In the future, updated coding techniques that support distant networks and better security standards may be utilized to ensure authentication while delivering data. To increase data authentication and prevent data moving, sharing, and unauthorized users, the modified Diffie Hellman (DH) algorithm is recommended. Then, the effective Zero Knowledge Proof (ZKP) method was combined with the DH algorithm to verify the offense attacks, such as the man-in-the-middle attack and discrete log only. The authors advise that increased security policies be implemented to assure authentication while transmitting data and that enhanced coding techniques be provided to facilitate remote networks.

In [22], The world of the digital environment is an important part of a range of goals. It is difficult to provide secure data communication via an unsecured network. Data should be protected from unauthorized access because of the rising usage of online message exchanges. This research provides a new hybrid encryption technique for encoding data. In terms of performance and avalanche effect, the suggested approach, MRSADH, encodes and decodes 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. The suggested study looks at the two most extensively used cryptographic algorithms, RSA and Diffie Hellman, and how they affect security and speed when combined into a unified hybrid (MRSADH) computation with the appropriate alterations. The paper additionally suggests a strategy for improving data security while minimizing the number of mathematical equations, which results in a faster execution time.

In [23], a modified RSA Random Bit Insertion Algorithm (RBMRSA) was made available, which transforms the ciphertext into a more complex structure that an attacker cannot easily decipher, even if the attacker has access to the secret key, increasing the RSA cryptosystem's security level without lengthening the keys. This promotes dependability and efficiency. This study offers bit insertion as an expedient way to remedy weaknesses in traditional RSA cryptosystems while achieving a high penetration level and effective security against various RSA attackers. Due to RSA security necessitates strong primes, Fermat's Little Theorem tests which of Fermat's three prime decryption keys. The primary goal of this research is to develop effective bit insertion techniques for modified RSA while keeping the following goals in mind:

The three prime integers P, Q, and R are used in an enhanced bit insertion algorithm to encrypt and decode messages in the RSA method, protecting against well-known RSA attacks.

- Examine the advantages and drawbacks of the conventional RSA cryptosystem.
- Implement the envisaged system and evaluate its effectiveness.
- Determine how the suggested system compares against conventional RSA using RSA.

3. The proposed algorithm (MRDAES)

This section discusses the proposed hybrid cryptographic method for protecting and maintaining information in three sections. The proposed integration of the MRDAES technique consists of three parts. In the MRDAES algorithm's first key exchange, the message is encrypted using XOR in the second step, and the output is encoded and decoded using AES in the third stage.

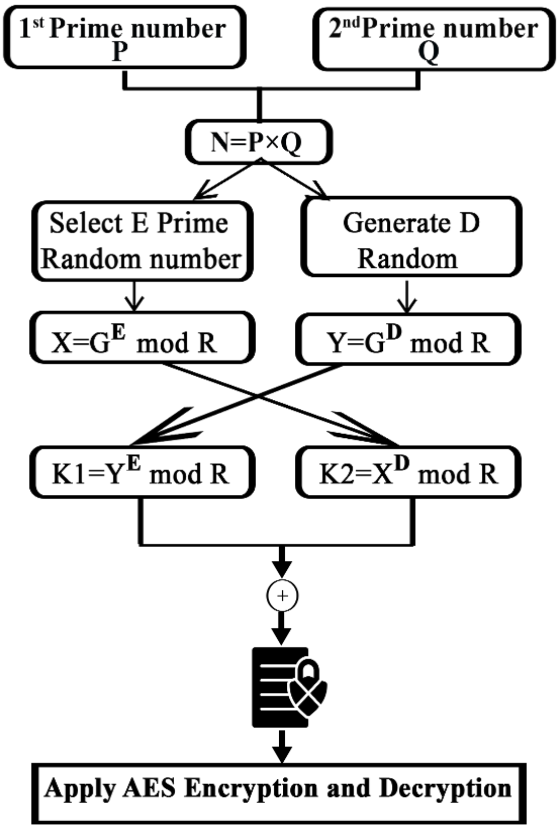

Figure. 1 The Proposed Algorithm (MRDAES)

However, using the modified RSA and DH techniques, two keys are created on both ends: the sender key for encryption and the receiver key for decoding incoming messages. The first and second phases are centered on the MRDAES encoding procedure. The key-generation process occurs during the first stage, the encryption phase (e,d). The key generation method requires two independent random prime numbers to construct both pairs of keys (public and secret keys, creating encryption and decryption keys) for use in the DH (p, q). The outcome of the first step of our suggested approach (MRDAES), which encrypts data using XOR to construct the first encoded message and then applies AES, was collected in the third phase (Ciphertext). AES decoding is also used in the third stage, followed by XORing a cipher text with the decryption key. Fig. 1 depicts the various stages of MRDAES, with the processes mentioned below:

3.1 The first stage (key generation) is as follows:

This step of the encryption method begins with the receiver supplying both the Secret and public keys. The intended receiver produces the public and secret keys in this modified RSA system by performing the following mathematical operations. Key creation is the necessary first stage of the encryption process. The key generation phase is the most reliable for predicting different prime values, p and q. The key creation procedure and two prime numbers, p, and q, generate the public key. The encryption and decryption keys generated by the DH Algorithm use the secret keys “d” and “e” as inputs and will be used for the first encoding process as data is encoded twice.

From RSA:

1. Choose two random prime numbers, p and q.

2. Then, compute modulus $n=(p\times q)$ (for maximum factorization difficulty, use prime integers with large values). (1)

3. Determine $\Phi= (p - 1)(q - 1)$. (2)

4. The exponent e should then be chosen so that $1<e< \Phi(n)$ and $\gcd(e, \Phi(n)=1$. (3)

5. Next, a secret component *d* must be generated with the formula

$d= e-1 \bmod \Phi(n)$, where (n, e) is the public key and d is the secret key. (4)

Second, use the (DH) algorithm. The DH method has grown in popularity due to its invisibility inside a networking system. This approach is commonly employed (SSL) when data is encrypted over the internet using transport layer security (TLS) or secure socket layer (SSL). The secure shell (SSH) protocol also commonly uses the DH algorithm. The previous RSA phases will determine the following stages for applying the DH algorithm.

6. Assume that $G=n(p\times q)$ and R, S, and G prime constants that are generated automatically (5)

7. Finally, convert the E and D values into secret integers so that A=e and B=d.
8. Decide on one of the following as an encryption and decryption key.

$X= (GA) \bmod R$
$Y= (GB) \bmod R$ (6)

9. Either $KA =(YA) \bmod R$ or
$KA = ((GB \bmod R)A) \bmod R$
$KA = ((GB)A) \bmod R \Rightarrow KA=(GBA) \bmod R$
$KB =(XB) \bmod R$ or
$KB = ((GA \bmod R)B) \bmod R$
$KB = ((GA)B) \bmod R \Rightarrow KB=(GAB) \bmod R$
So that, $KA = KB = K$. (7)

3.2 Decryption Process:

We reversed the abovementioned steps to obtain our plain “original message” message by first decrypting the data encoded using AES, followed by the output decoding using XOR and the session key (K) for decryption.

4. Experimental results and discussion

Cryptography is a powerful technology for achieving information privacy, secrecy, authentication, and integrity, which are critical. Following the successful implementation of the specified algorithms with our proposed methodology,’ multi-level cryptography was implemented using RSA, DH, and AES (MRDAES). RSA processes generate public and private keys for the next stage. The suggested method includes creating an encryption key with the RSA public and private keys indicated above and then using the encryption key to encrypt data as the first phase of encoding. Using the encryption key obtained from DH and XOR, the data Finally, AES is applied to encode the previous result. The coding process calculation in this study is derived from a combination of the RSA, DH, and AES algorithms that will be implemented in the software. The software facilitates testing the code

Table 1. Cryptographic Encoding Time

	PN	Proposed Alg.	RSA
1st PN	(1008001,281)	22.6485	14.906
2nd PN	(9804787,349)	478.5029	414.563
3rd PN	(9969919,409)	590.1747	517.906
4th PN	(10028279,541)	742.2502	710.375

Table 2. Cryptographic Decoding Time

	PN	Proposed Alg	RSA
1st PN	(1008001,281)	15.362	0.0005
2nd PN	(9804787,349)	21.929	0.0027
3rd PN	(9969919,409)	27.601	0.0017
4th PN	(10028279,541)	32.893	0.00202

result. Because the performance of the key generation, encryption, and decryption procedures is measured using a laptop machine, the laptop's capabilities are as follows:

a) Using Windows 10 and Visual Studio Code Version: 1.69.2 (user setup)

b) Supporting hardware: HP Intel(R) Core (TM) i7-8565U CPU @ 1.80GHz, 1.99GHz, 8 GB RAM, and 1TB hard disc.

4.1 Security auditing and performance evaluation

This section will examine the efficiency and security of the proposed MRDAES approach. The MRDAES algorithm will be used in this proposed study, and the results will be compared to numerous other approaches.

4.1.1 Security auditing and performance evaluation

The efficiency of any given encoding and decoding mechanism is determined by how long it takes to accomplish any cryptographic function. The speed or slowness of the algorithm depends on how long it takes to execute. Tables 1 and 2 present the encryption and decryption results for the proposed approaches: MRDAES and conventional RSA. Comparing MRDAES to classical RSA, Tables 1 and 2 demonstrate that the computational complexity of the encryption and decryption techniques is higher than that of standard RSA. This indicates that the algorithm will get more difficult as execution time grows. Fig. 2 compares the encryption timings of the proposed MRDAES method, and traditional RSA when plotted against identical message sizes. Fig. 3 depicts a graphical comparison of the decryption timings for the proposed MRDAES and Classical RSA algorithms. Table 3 and Table 4 show that the MRDAES encryption algorithm takes the shortest time, while the hybrid encryption in [19] takes the

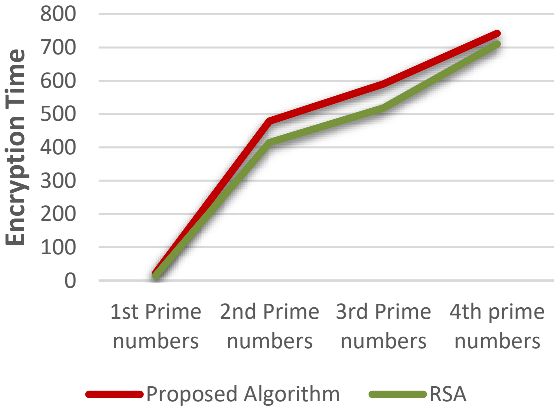

Figure. 2 Encryption time

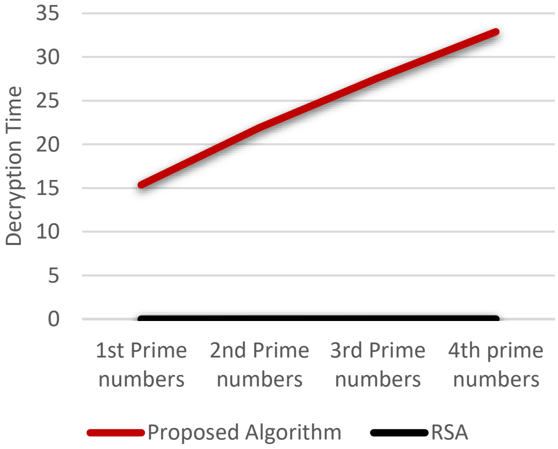

Figure. 3 Decryption time

Table 3. Encryption time

Date Size (Char)	MRDAES	Hybrid encryption in [19]	Time-Difference
1	0.165	0.183	9.84%
5	0.358	0.963	62.82%
10	1.777	4.213	57.82%
20	4.714	19.867	76.27%

Table 4. Decryption time

Date Size (Char)	MRDAES	Hybrid encryption in [19]	Time-Difference
1	0.131	0.405	67.65%
5	0.553	1.895	70.82%
10	1.665	16.153	89.69%
20	4.962	315.064	98.43%

longest. This is due to the mathematical operation of merging AES and RSA encryption algorithms based on the original algorithm, resulting in a longer operation time. The [19] technique is less efficient than the MRDAES algorithm, which guarantees optimal encryption in less time but requires more complexity. Overall, the proposed approach outperforms other algorithms regarding computer communication security.

4.1.2 Avalanche effect

The avalanche effect refers to the alterations in ciphertext produced by a small change or variation in plain message [23]. A good cipher or encryption method must generate radically different outputs for a little change in the input. The degree of change in the ciphertext is related to the amount of security of an algorithm, i.e., the larger the avalanche effect of the algorithm, the higher its security level. As a result, doing statistical analysis will be difficult and tricky for an attacker. The purpose of flipping only one bit in the avalanche effect (%) is to evaluate the sensitivity of the proposed method by investigating if even the slightest change in the plaintexts results in a radical or massive change in the ciphertext.

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

Changing one bit in the plaintext of MRDAES generated an 88% change in the ciphertext, compared to an estimated 0.2% for RSA and 47.52% for RBMRSA in [23], where the figure in% stands for the avalanche effect. The graphical representation of the avalanche effect is presented graphically in Fig. 4.

4.1.3 Discussion

The results of the studies indicated that, in terms of security complexity, the proposed approach delivered outstanding and useful outcomes when compared to alternative algorithms. MRDAES raised security complexity while raising execution time somewhat and minimizing MITM threats. Comparing the proposed approach to traditional RSA and cutting-edge algorithms may help you comprehend the results in Tables 1 and 2. The findings indicated that the suggested MRDAES outperformed standard RSA approaches regarding security complexity. The experimental findings showed that, compared to previous algorithms, the proposed hybrid algorithm MRDAES produced remarkably successful results. Table 1 presents the results of comparing the proposed and state-of-the-art algorithms. The outcomes demonstrated that, with a slightly increased execution time, the suggested technique MRSAES could produce a better complexity than other traditional RSA algorithms. Fig. 4 illustrates that the avalanche effect results of MRSAES showed an 88% rise in strength in addition to improving complexity, compared to an estimated 0.2% for RSA and 47.52% for RBMRSA. It illustrates that the new techniques take longer, so the user will use the proposed algorithm to assess whether he requires additional security while disregarding time execution.

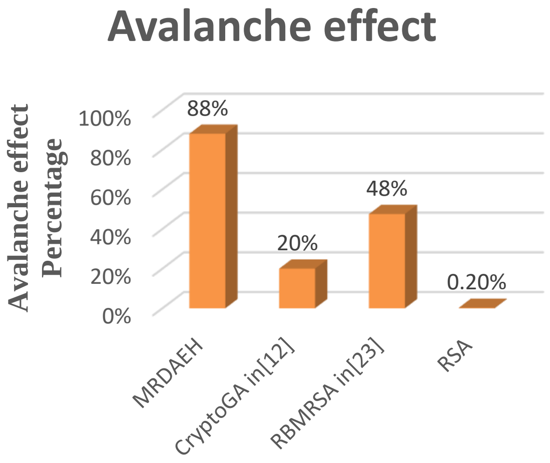

Figure. 4 Avalanche effect

5. Conclusion and future work

Cybersecurity incidents have become everyday headlines in today’s IT Digital Transformation world. An effective cryptographic procedure is required to tackle the problem of data dispersion during data transmission while exchanging data on particular networks, as it confronts certain significant obstacles in safeguarding the data and regulating access to the information that is transferred. Data integrity and authentication help establish an effective cryptographic method. Customized encryption and coding between communicating entities achieve data privacy and communication integrity. Initially, user authentication was created using a modified RSA and Diffie-Hellman (DH) Key exchange. Furthermore, the authentication process’s speed is increased by using the XOR and AES methods in conjunction with a modified DH. Our future efforts will center on building an online cryptography solution capable of effectively addressing today’s actual digital world transformation advancement concerns.

Conflicts of Interest

The authors declare no conflicts 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. Kumar Singh, M. Kumar Roy, S. Karforma, and S. Mukhopadhyay, “IMPLEMENTATION OF E-BANKING TRANSACTION SYSTEM USING ELGAMAL DS”, *Journal of Data Acquisition and Processing*, Vol. 38, No. 2, pp. 1883-1888, 2023.

[2] G.Qianru, “Application Research of Data Encryption Algorithm in Computer Security Management”, *Wireless Communications and Mobile Computing*, pp. 1463724, 2022.

[3] S. R. Maniyath and T. V, “An efficient image encryption using deep neural network and chaotic map”, *Microprocessors and Microsystems*, Vol. 77, PP. 103134, 2020.

[4] S. Urooj, S. Lata, S. Ahmad, S. Mehfuz, and S. Kalathil, “Cryptographic Data Security for Reliable Wireless Sensor Network”, *Alexandria Engineering Journal*, Vol. 72, PP. 37-50, 2023.

[5] A. Taha, D. S. Elminaam, and K. Hosny, “AN IMPROVED SECURITY SCHEMA FOR MOBILE CLOUD COMPUTING USING HYBRID CRYPTOGRAPHIC ALGORITHMS”, *Far East Journal of Electronics and Communications*, Vol. 18, No. 4, PP. 521-546, 2018.

[6] M.N. Praphul and K.R.Nataraj, “FPGA Implementation of Hybrid Cryptosystem”, *International Journal of Emerging Science and Engineering*, Vol. 1, No. 8, PP. 14-19, 2013.

[7] M. Iavich, S. Gnatyuk, E. Jintcharadze, Y. Polishchuk, and R. Odarchenko, “Hybrid Encryption Model of AES and ElGamal Cryptosystems for Flight Control Systems”, In: *Proc. of 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control*, pp. 229-233, 2018.

[8] P. Li, J. Li, Z. Huang, C.Z. Gao, W.B. Chen, and K.Chen, “Privacy-preserving outsourced classification in cloud computing”, *Cluster Computing*, Vol. 21, pp. 277-286, 2018.

[9] M. Hamdi, J. Miri, and B. Moalla, “Hybrid encryption algorithm (HEA) based on chaotic system”, *Soft Comput*, Vol. 25, No. 3, pp. 1847-1858, 2021.

[10] S. Tariq, M. Khan, A. Alghafis, and M. Amin, “A novel hybrid encryption scheme based on chaotic Lorenz system and logarithmic key generation”, *Multimed Tools Appl*, Vol. 79, No. 31, pp. 23507-23529, 2020.

[11] S. Sani, P. Taneja, and S. Kalta, “A Comparative Analysis of Cryptographic Algorithms: AES & RSA and Hybrid Algorithm for Encryption and Decryption”, *International Journal of Innovative Science and Research Technology*, Vol. 7, No. 8, pp. 1725-1732, 2022.

[12] M. Tahir, M. Sardaraz, Z. Mehmood, and Sh. Muhammad, “CryptoGA: a cryptosystem based on genetic algorithm for cloud data security”, *Cluster Computing*, Vol. 24, pp. 739-752, 2021.

[13] K. Balasubramanian, M. Arun, and K. R. Sekar, “An Improved RSA Algorithm for Enhanced Security” *Indian Journal of Cryptography and Network Security*, Vol. 2, No. 2, pp. 1-4, 2022.

[14] Q. Gong, “Application Research of Data Encryption Algorithm in Computer Security Management”, *Wireless Communications and Mobile Computing*, Vol. 2022, pp. 1-7, 2022.

[15] W. A. Shukur, L. K. Qurba, and A. Aljuboori, “Digital Data Encryption Using a Proposed W-Method Based on AES and DES Algorithms”, *Baghdad Science Journal*, Vol. 1, 2023.

[16] A. Kavitha, B. S. Rao, N. Akhtar, S. M. Rafi, P. Singh, S. Das, and G. Manikandan, “A Novel Algorithm to Secure Data in New Generation Health Care System from Cyber Attacks Using IoT”, *International Journal of Electrical and Electronics Research*, Vol. 10, No. 2, pp. 270-275, 2022.

[17] A. K. Singh, M. K. Roy, S. Karforma, and S. Mukhopadhyay, “IMPLEMENTATION OF E-BANKING TRANSACTION SYSTEM USING ELGAMAL DS”, *Journal of Data Acquisition and Processing*, Vol. 38, No. 2, pp. 1883-1888, 2023.

[18] A. SadanandGhadi, “Secure File Storage Using Hybrid Cryptography”, *International Journal of Innovative Science and Research Technology*, Vol. 5, No. 12, pp. 185-188, 2020.

[19] Z. Lu and H. Mohamed, “A Complex Encryption System Design Implemented by AES”, *Journal of Information Security*, Vol. 12, pp. 177-187, 2021.

[20] A. Hamza and B. Kumar, “A Review Paper on DES, AES, RSA Encryption Standards”, In: *Proc. of 9th International Conference on System Modeling & Advancement in Research Trends*, Moradabad, India, pp. 333-338, 2020.

[21] P. Kanagala, "Implementing cryptographic-based DH approach for enterprise network", *Optik*, Vol. 272, pp. 170252, 2023.

[22] M. Salah, A. El-Sawy, and M. Taha, "A Hybrid Algorithm For Enhancement of the Data Security during Network Transmission Based on RSA and DH", *International Journal of Intelligent Engineering and Systems*, Vol. 16, No. 3, pp. 614-624, 2023.

[23] F. O. Mojisola, S. Misra, C. F. Febisola, O. A. Alli, and G. Sengul, "An improved random bitstuffing technique with a modified RSAalgorithm for resisting attacks in information security (RBMRSA)", *Egyptian Informatics Journal*, Vol. 23, No. 2, pp. 291-301, 2022.