# Enhancement Technique for ECG Signal Protection Using Dual-Layer MEHC and DNA Computing

Fatma Zohra Besmi[1]
*Department of Electrical Systems Engineering, LIST Laboratory*
*University of Boumerdes, Faculty of Technology*
35000 Boumerdes, Algeria
f.besmi@univ-boumerdes.dz

Samia Belkacem[2]
*Department of Electrical Systems Engineering*
*University of Boumerdes, Faculty of Technology*
35000 Boumerdes, Algeria
s.belkacem@univ-boumerdes.dz

Noureddine Messaoudi[3]
*Department of Electrical Systems Engineering, LIST Laboratory*
*University of Boumerdes, Faculty of Technology*
35000 Boumerdes, Algeria
n.messaoudi@univ-boumerdes.dz

***Abstract*—DNA-based molecules have recently become a central focus in encryption research due to their exceptionally high data storage capacity and low computational requirements. Building on this concept, the present study proposes a hybrid ECG encryption method—termed DNA-MEHC—that integrates DNA sequence encoding with the Modified Gorti-Enhanced Homomorphic Cryptosystem to provide two layers of security for ECG signal protection. The proposed scheme operates through a four-stage pipeline: the raw ECG signal is first binarized, then converted into a high-entropy DNA sequence. This sequence is subsequently mapped to an integer stream, which is finally encrypted using the MEHC algorithm. Decryption is performed by reversing these steps in the correct order. Experimental results demonstrate perfect signal reconstruction (zero Mean Squared Error), strong security validated by histogram and correlation analyses, and a low signal-to-noise ratio between the encrypted and original signals. Collectively, these findings indicate that the proposed method is both practical and effective, addressing the critical need for secure ECG data protection and reliable transmission in telemedicine and IoT-based healthcare systems.**

***Index Terms*—MEHC Algorithm, DNA cryptography, ECG signal, security**

## I. Introduction

The increasing use of medical devices for continuous patient monitoring has intensified the need to secure sensitive biological data [1]. ECG signals are especially critical, as they reflect vital cardiac activity and support immediate clinical decision-making. Any alteration or tampering can lead to serious consequences, making strong security measures essential to protect the integrity and confidentiality of patient information [2].

Cryptography safeguards the confidentiality and integrity of data by transforming information into an unreadable form for unauthorized users [3]. While traditional methods such as AES are highly secure for transmission, they follow an "all-or-nothing" model that requires full decryption before processing. This exposes plaintext during computation and creates vulnerabilities, making such approaches less suitable for cloud-based medical analytics where sensitive data must be processed without direct access [4].

In the work of Jamal Kh-Madhloom et al. (2021) [5], a multilayer ECG encryption method that combines AES with DNA computing was introduced to enhance privacy in fog-based healthcare systems. By reducing the effective ECG message length, their approach strengthens encryption while lowering computational complexity. Overall, the multilayer AES–DNA scheme improves robustness and security for ECG data transmission in IoT-enabled medical environments.

Building on prior work, this research introduces a multilayer cryptosystem that integrates DNA computing with the MEHC algorithm [6], designed for secure operation in biological and cloud–fog environments. The method protects DNA-encoded data from plaintext attacks using a primary key and dynamic rule-based key generation. The main contributions are:

- **A Novel Multilayer Cryptosystem (DNA-MEHC):** Development of a resilient multilayer cryptosystem that integrates DNA computing techniques with the Modified Enhanced Homomorphic Cryptosystem (MEHC) to provide strong encryption for DNA sequences.
- **Suitability for DNA-Computing Environments:** A design tailored for secure computation within biological and DNA-based platforms.
- **Enhanced Security for Fog-Based DNA Storage:** A mechanism that safeguards DNA sequences in distributed infrastructures against plaintext and statistical attacks.
- **Advanced key management:** A structured main-key and rule-key system that increases encryption complexity and

overall robustness.

The remainder of this paper is organized as follows: Section 2 presents the proposed model in detail, Section 3 discusses the experimental results, and Section 4 concludes the study.

## II. Methodology

This section presents a detailed description of DNA-MEHC, the proposed data encryption framework that integrates DNA computing with the MEHC scheme. The flowchart of the DNA-MEHC cryptosystem is illustrated in Fig. 1.

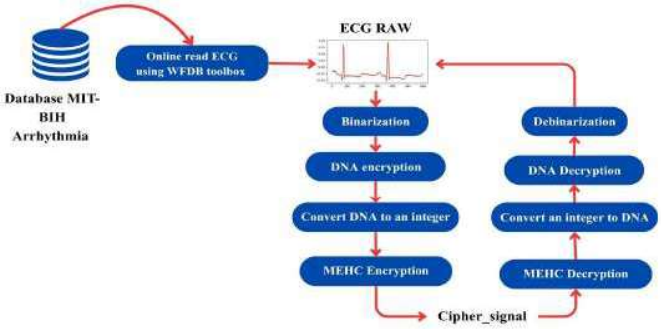


Fig. 1. Flowchart of the proposed cryptosystem DNA-MEHC

The following subsections outline each phase of the proposed technique. Every step plays a critical role in the overall workflow and is designed with algorithmic considerations in mind to enhance the system's performance and security.

### A. ECG Binarization

In this phase, the raw ECG signal is converted into a sequence of binary bits to prepare it for subsequent DNA-based encoding.

### B. DNA Encryption

In the DNA encryption phase, the binary message is transformed into a DNA sequence [7]. This conversion is performed using eight distinct DNA encoding rules, as presented in Table I [8].

TABLE I
Mapping Rules of DNA encryption

| Rule | A | T | C | G |
|---|---|---|---|---|
| 1 | 00 | 11 | 01 | 10 |
| 2 | 00 | 11 | 10 | 01 |
| 3 | 01 | 10 | 00 | 11 |
| 4 | 01 | 10 | 11 | 00 |
| 5 | 10 | 01 | 00 | 11 |
| 6 | 10 | 01 | 11 | 00 |
| 7 | 11 | 00 | 01 | 10 |
| 8 | 11 | 00 | 10 | 01 |

To ensure that each message sample is encoded uniquely, the system employs a dynamic rule-selection mechanism. The rule applied to the i-th sample is determined using the following equation:

$$Rule_{index} = (x_i \bmod 8) + 1 \tag{1}$$

This computation produces a value between 1 and 8, indicating which of the eight DNA encoding rules should be used.

### C. Convert DNA to integers

In this phase, each DNA base (A, T, C, G) is converted into an integer value (0, 1, 2, 3) using a predefined numerical mapping. Specifically, Adenine (A) is mapped to 0, Thymine (T) to 1, Cytosine (C) to 2, and Guanine (G) to 3.

### D. MEHC Cryptosystem

The MEHC algorithm is employed as a secondary encryption layer to further strengthen data confidentiality and implement a defense-in-depth strategy. It consists of four distinct procedures, which are summarized in the table below.

**Key generation:**

1) Two large prime numbers p and q are generated using a Linear Congruential Generator (LCG), ensuring that $p > q$. Their primality is verified using the Rabin–Miller probabilistic test. In this study, 512-bit primes are used to guarantee strong cryptographic security.
2) Compute the modulus: $m = p * q$
3) Compute: $g = m^2 + 1$
4) Select a prime number $Q$ that satisfies the condition $Q < \left\lfloor \frac{p}{2} \right\rfloor$. Its primality is also confirmed using the Miller–Rabin test.
   - *Public Key:* {g}
   - *Private Key:* {p, q, r, Q}
   - *Evaluation Key:* The evaluation key $e_k$ is computed by concatenating the parameters $p$, $q$, and $Q$, hashing them using SHA-256, and reducing the resulting hash modulo $g$. A second reduction is then applied to constrain the key within a small predefined range suitable for the evaluation phase.

**Encryption:**

The DNA integer signal is encrypted using the parameters $Q$, $g$, and a random vector $r$:

$$C = \left(\text{DNA\_int\_signal} + r \cdot Q + r \cdot g\right) \mod g \tag{2}$$

**Evaluation:**

Upon receiving the ciphertext $C$, the evaluator produces an evaluated ciphertext $C'$ using a linear polynomial:

$$C' = N \times C + e_k \tag{3}$$

where $N$ is a random scalar and $e_k$ is the evaluation key. This step enables homomorphic operations to be performed on the encrypted data prior to decryption.

**Decryption:**

Decryption begins by reversing the linear evaluation function, followed by applying MEHC decryption with the private key to recover the plaintext:

$$C = \frac{C'}{N^{-1}} - e_K \tag{4}$$

$$\text{Dec\_Sig} = C \mod Q \tag{5}$$

After the MEHC decryption step, the resulting integer signal is reconverted into its corresponding DNA sequence. This DNA-decoded signal is then translated back to binary form and debinarized to reconstruct the original ECG signal.

## III. Experimental Results and Security Analysis

Experiments were conducted on a system with an Intel® Core™ i5-8350U processor, 8 GB of RAM, and a clock speed of 1.70 GHz.The proposed cryptosystem was evaluated using two widely recognized ECG datasets: the MIT-BIH Arrhythmia Database and the AHA (American Heart Association) Database. The proposed cryptosystem was implemented in Python (version 3.13.0, 64-bit).

The performance and security of the proposed algorithm were evaluated using several key metrics, including Mean Squared Error (MSE), Signal-to-Noise Ratio (SNR), histogram analysis, and correlation coefficients.

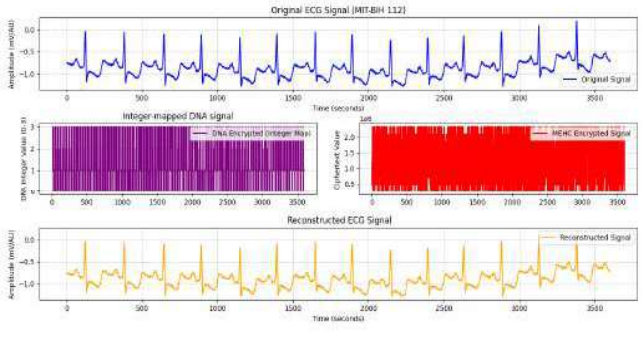


Fig. 2. Results of DNA-MEHC cryptosystem (record 112 from MIT-BIH Arrhythmia database)

Figure 2 illustrates that encrypting the signal using only the DNA algorithm leaves parts of the original signal visually discernible. By adding the MEHC encryption layer, the ciphertext becomes visually indistinguishable, enhancing security. These results indicate that the proposed DNA-MEHC approach effectively secures the signal while enabling accurate reconstruction upon decryption.

### A. Histogram analysis

Figure 3 illustrates that the histogram of the encrypted ECG signal is highly uniform and substantially different from that of the original signal, thereby rendering statistical analysis attacks on the ciphertext extremely difficult.

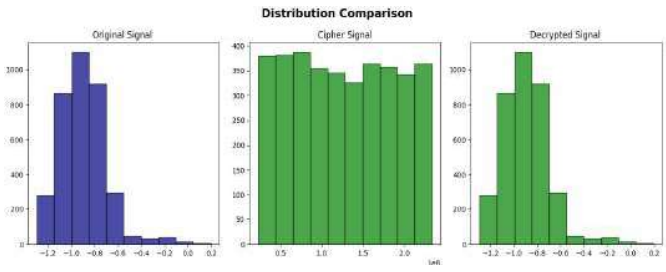


Fig. 3. Histograms of original, encrypted and decrypted ECG signals (record 112 from MIT-BIH database)

Upon decryption, the signal accurately recovers the original distribution, confirming the proposed scheme's lossless reversibility and high reconstruction fidelity.

### B. Correlation coefficient analysis

The correlation analysis, depicted in the scatter plots and quantified by the corresponding coefficients (Figs. 4–5), demonstrates the strong decorrelation capability of the proposed encryption scheme.

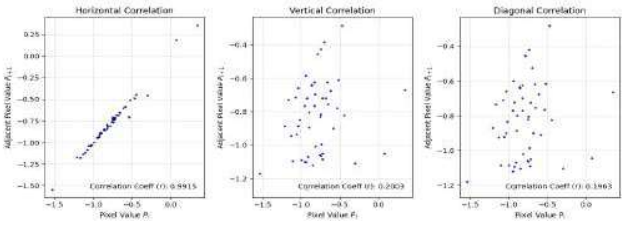


Fig. 4. Horizontal, vertical, and diagonal correlations of the original ECG signal(record 112 from MIT-BIH Arrhythmia database)

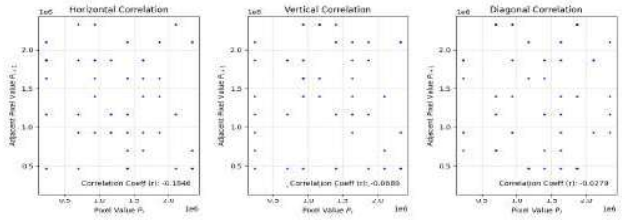


Fig. 5. Horizontal, vertical, and diagonal correlations of the encrypted ECG signal (record 112 from MIT-BIH Arrhyhmia database)

The original ECG signal shows high horizontal correlation ($r = 0.9915$), reflecting the predictable structure of time-series data. After encryption, correlations are effectively randomized, with horizontal, vertical, and diagonal correlations reduced to $r = -0.1846$, $-0.0689$, and $-0.0279$, respectively. This transformation—from a tightly clustered linear pattern to a uniformly scattered distribution—demonstrates strong diffusion, effectively removing statistical redundancy and enhancing resistance to differential cryptanalysis.

### C. MSE and SNR metrics

The quality of the digital ECG signals is evaluated using the Signal-to-Noise Ratio (SNR) and Mean Squared Error (MSE) metrics. The MSE measures the difference between the original and reconstructed signals, with values close to zero indicating high similarity and larger values reflecting greater distortion [5].

The SNR quantifies the level of distortion introduced by the encryption process. Lower SNR values indicate stronger obfuscation of the original signal, which is desirable for security, as it shows that the ciphertext bears minimal resemblance to the original waveform.

Tables II and III show MSE and SNR for ECG signals from the MIT-BIH Arrhythmia and AHA databases. Zero MSE values indicate accurate signal reconstruction, while very low SNR values (-123 dB to -136 dB) demonstrate that the encryption effectively hides signal characteristics, ensuring secure transmission.

TABLE II
MSE AND SNR VALUES FOR REPRESENTATIVE ECG SIGNALS (SOME RECORDS FROM MIT-BIH ARRHYTHMIA DATABASE)

| ECG Signal Name | MSE | SNR (dB) |
|---|---|---|
| 100 | 0 | -132.0417 |
| 104 | 0 | -132.3239 |
| 107 | 0 | -124.4750 |
| 112 | 0 | -124.5268 |
| 121 | 0 | -124.6095 |
| 124 | 0 | -123.6247 |
| 202 | 0 | -133.1735 |
| 217 | 0 | -127.1155 |
| 221 | 0 | -132.2832 |
| 228 | 0 | -132.0509 |
| 232 | 0 | -136.0213 |
| 234 | 0 | -131.7951 |

TABLE III
MSE AND SNR VALUES FOR REPRESENTATIVE ECG SIGNALS (RECORDS FROM AHA DATABASE)

| ECG Signal Name | MSE | SNR (dB) |
|---|---|---|
| 0001 | 0 | -133.3805 |
| 0201 | 0 | -134.9630 |

### *D. Performance Comparison With MLAESDNA*

To assess the effectiveness of DNA-MEHC, it was compared with the multilayer AES-DNA (MLAESDNA) encryption scheme [5].

Table IV summarizes the comparison in terms of design, keyspace, encryption strength, reconstruction quality, processing capability, computational cost, and best use cases.

TABLE IV
COMPARISON OF MLAESDNA AND DNA-MEHC ENCRYPTION APPROACHES

| **Feature** | **MLAESDNA [5]** | **Our proposed (DNA-MEHC)** |
|---|---|---|
| Core Design | Multilayer AES combined with DNA encoding | DNA encoding combined with MEHC |
| Encryption Strength | High statistical security | High obfuscation (very low SNR) |
| Reconstruction Quality | MSE = 0 | MSE = 0 |
| Processing Encrypted Data | Not possible (must decrypt first) | Possible due to homomorphic operations |
| Computational Cost | Higher, multiple AES rounds | Lower, efficient for cloud processing |
| Best Use Case | Secure storage and transmission | Privacy-preserving cloud analytics |

DNA-MEHC combines DNA encoding with MEHC, providing dual-layer security and strong obfuscation, as reflected by extremely low SNR values. It achieves perfect reconstruction (MSE = 0) and supports computations on encrypted data via homomorphic operations, making it well-suited for privacy-preserving cloud analytics.

In contrast, MLAESDNA relies on multiple AES rounds with DNA encoding, offering strong statistical security but requiring decryption for processing and higher computational cost.

## IV. CONCLUSIONS

This study presented DNA-MEHC, a hybrid cryptosystem that integrates DNA computing principles with the Modified Gorti Enhanced Homomorphic Cryptosystem (MEHC) to secure ECG signals. The proposed framework demonstrates strong performance across all evaluation metrics. Signal reconstruction achieves perfect fidelity, as indicated by an MSE of zero for all tested signals, while the encryption process produces extremely low SNR values (approximately $-123$ to $-136$ dB), confirming effective signal obfuscation.

Correlation analysis further validates the scheme's robust decorrelation capability. The originally high correlations in the ECG signal are reduced to near-zero values after encryption, demonstrating effective diffusion and the elimination of statistical patterns.

Overall, DNA-MEHC offers a reliable and efficient approach for privacy-preserving ECG data management, with significant potential for secure biomedical signal processing and telemedicine applications.

## ACKNOWLEDGMENT

This study was supported by the Algerian Ministry of Higher Education and Scientific Research through funding for PRFU Project.

## REFERENCES

[1] N. Rafie, A.H. Kashou, P.A. Noseworthy, "ECG Interpretation: Clinical Relevance, Challenges, and Advances," *Hearts*, vol. 2, No. 4, pp. 505–513, 2021. doi: https://doi.org/10.3390/hearts2040039.

[2] S. Shanmugasundaram, M. Chinnasamy, and L. S. Annaman, "An ECG Signal Encryption and Classification Using Sparse Autoencoder and Optimized Neural Network Techniques," *Traitement du Signal*, vol. 42, pp. 557–568, 2025. doi: 10.18280/ts.420147.

[3] D. Liu, M. Caceres, T. Robichaux, D. V. Forte, E. S. Seagren, D. L. Ganger, B. Smith, W. Jayawickrama, C. Stokes, and J. Kanclirz, "An Introduction To Cryptography," in *Next Generation SSH2 Implementation*, pp. 41–64. Burlington: Syngress, 2009. doi: 10.1016/B978-1-59749-283-6.00003-9.

[4] C. Mascia, M. Sala, and I. Villa, "A survey on functional encryption," *Advances in Mathematics of Communications*, vol. 17, pp. 1251–1289, 2023. doi: 10.3934/amc.2021049.

[5] J. Kh-Madhloom, M. K. A. Ghani, and M. R. Baharon, "ECG encryption enhancement technique with multiple layers of AES and DNA computing," *Intelligent Automation and Soft Computing*, vol. 28, pp. 493–512, 2021. doi: 10.32604/iasc.2021.015129.

[6] F. Z. Besmi, S. Belkacem, and N. Messaoudi, "Using Modified Gorti-enhanced Homomorphic Cryptosystem to Improve Security of ECG Signal," *Journal of Telecommunications and Information Technology*, pp. 46–55, 2025. doi: 10.26636/jtit.2025.2.2002.

[7] E. Şatir, O. Kendirli, "A symmetric DNA encryption process with a biotechnical hardware," *Journal of King Saud University - Science*, vol. 34, No. 3, 2022. doi: https://doi.org/10.1016/j.jksus.2022.101838.

[8] M. M. Elamir, M. S. Mabrouk and S. Y. marzouk, "Secure framework for IoT technology based on RSA and DNA cryptography," *Egyptian Journal of Medical Human Genetics*, vol. 23, No. 116, 2022. doi: https://doi.org/10.1186/s43042-022-00326-5.

CANADIAN ASSOCIATION FOR ARTIFICIAL INTELLIGENCE AND FUTURE STUDIES

# CERTIFICATE OF PARTICIPATION

THIS IS TO CERTIFY THAT

## Fatma Zohra Besmi

attended the

## International Conference on Advancement in Healthcare Technology and Biomedical Engineering (AHTBE 25)

**Annacis Research and Event Centre, Vancouver, BC, Canada**
**August 29-30, 2025**

Dr. Ghazanfar Latif
**Conference General Chair**

Dr. Jaafar Alghazo
**Conference General Chair**

# QRS Detection in ECG Signals Utilizing a Partially Homomorphic Encryption Technique-Based Modified RSA Algorithm

Fatma zohra Besmi[1][0009-0007-8216-0831], Samia Belkacem[2][0000-0003-0912-3392] and Noureddine Messaoudi[1][0000-0002-7228-5784]

[1] University of Boumerdes, Faculty of Technology, Department Engineering of Electrical Systems, LIST Laboratory, 35000 Boumerdes, Algeria
[2] University of Boumerdes, Faculty of Technology, Department Engineering of Electrical Systems, 35000 Boumerdes, Algeria
f.besmi@univ-boumerdes.dz

**Abstract.** This paper presents a secure and innovative method for encrypting electrocardiogram (ECG) signals by seamlessly incorporating the Pan and Tompkins algorithm for QRS detection alongside a partially homomorphic encryption (PHE) technique—the modified RSA algorithm (MRSA). This integrated approach results in a highly secure and efficient encryption scheme. To enhance cryptographic complexity and prime factorization, our MRSA algorithm uniquely determines 'n' using three random prime integers (p, q, and s), generated via a Linear Congruential Generator (LCG). Significantly, the system's public and private keys utilize 'g' instead of 'n', providing an additional security layer. The encryption process begins by processing raw ECG signals through the initial four steps of the Pan and Tompkins algorithm, yielding a refined signal (x6). Then, the MRSA algorithm encrypts this signal (x6) with the public key (e, g). After decrypting the data with the private key (d, g), the heart rate is assessed to determine whether it is regular or irregular. Our approach ensures data integrity and patient privacy, with results showing high accuracy (99.86%), sensitivity (98.57%), and positive predictive value (97%) in heart rate classification and close-to-ideal decryption. The MRSA algorithm's homomorphic properties permit secure computations on encrypted data, making it valuable for remote diagnostics and medical research.

**Keywords:** Encryption, Heart Rate Classification, Modified RSA (MRSA), Partially Homomorphic Encryption, QRS Detection.

## 1 Introduction

Although there are many medical records, the electrocardiogram (ECG) is one of the most important, as it provides important information about the patient's heart health. Discovered by Wilm Ithowen in 1902, it represents the electrical activity of the heart [1]. The electrocardiogram (ECG) catches the electrical rhythm of the heart properly over time using an electrode or lead. It records electrical changes that occur as the heart

muscle depolarizes and repolarizes during each heartbeat. While ECG signals are traditionally recorded using 12 traditional leads, single-lead ECGs are becoming increasingly popular for modern applications [2]. This change is due to their low complexity and low data volume, making them more desirable and general options. Heart activity and condition can be determined by the morphology of an ECG signal, especially its peaks and their duration [3]. On a specific ECG, the P wave, QRS complex, and T wave describe the electrical activity of the heart. P waves indicate atrial depolarization, while the QRS complex indicates ventricular contraction [4].

Health care has been made more efficient and appropriate by making the ECG record digital. This data can be accessed, intercepted, and changed without permission as it is being sent across the network [5]. This is a big danger, since it could lead to breaches of patient privacy, stealing their identity, committing medical fraud, or misdiagnoses. Consequently, safeguarding ECG data has become essential for healthcare professionals and institutions [6].

One of the suggested methods for ECG encryption is partially homomorphic encryption (PHE). This technique enables one addition or multiplication operation on encrypted data and generates an encrypted result that, when decoded, corresponds to the result of the operations as though they had been performed on the plaintext [7]. RSA is a public key algorithm that offers multiplicative partially homomorphic encryption [8]. This means that if two plaintext messages, m1 and m2, are encrypted using the public key, the product of their ciphertexts (E(m1) ·E(m2)) can be decrypted using the private key to yield the product of the original messages (m1·m2) [9]. This cryptosystem maintains the privacy of the decryption key while making the encryption key publicly available. Only the private key may be used to decrypt messages encrypted with the public key for an acceptable length of time [10]. Factorization attacks are the primary weakness of the RSA algorithm, which is based on the 'e' and 'n' public keys used for encryption [11].

In the research conducted by Shaikh et al. [12], electrocardiogram (ECG) encryption is accomplished by employing a methodology that integrates the Pan and Tompkins algorithm for the detection of the QRS complex alongside the Partial Homomorphic Encryption technique—RSA algorithm. This approach facilitates the identification of cardiac irregularities and the computation of heart rate while ensuring the protection of sensitive information. Specifically, following the processing of the moving window coordinates (x6), calculations for encryption and decryption are executed, thereby modifying the signal for security purposes. Upon decryption, the resultant output denotes whether the heart rate is normal or abnormal. The study, which utilized the MIT-BIH arrhythmia dataset for testing, exhibited an accuracy of 90% and efficiency in safeguarding ECG signals.

This study proposes a security approach focused on securing ECG signals in healthcare contexts. We apply the Pan and Tompkins technique for preprocessing and recognizing QRS complexes. Building on previously discussed work, we propose a partially homomorphic encryption (PHE) technique based on a modified RSA algorithm, which we term MRSA. This algorithm preserves the partial homomorphic capabilities of the standard RSA algorithm, enabling secure computations directly on encrypted ECG data—a significant advantage for applications like remote diagnostics and

collaborative medical research. To address the inherent challenges of cryptographic strength, our MRSA algorithm innovatively derives 'n' from three distinct random prime integers (p, q, and s), generated with a Linear Congruential Generator (LCG), thereby enhancing cryptographic complexity and making prime factorization significantly harder. An additional layer of security is incorporated by having the system's public and private keys rely on 'g' instead of 'n'.

The organization of the rest of the paper is as follows: Section 2 describes in depth the proposed algorithm, whereas Section 3 analyzes experimental findings and discusses them. Finally, Section 4 concludes the article.

## 2 Materials and Methods

A novel approach is proposed to avoid security problems while sending the patient's ECG records via networks. The Pan and Tompkins approach is used to examine and process an electrocardiogram (ECG) signal to identify the QRS complex. This ECG is subsequently encrypted using the proposed MRSA method. The sender encrypts the ECG data using the public key (e, g). By encrypting the signal, the signal would be changed. The recipient securely decrypts the encrypted signal using the secret key (d, g). The final result was in the form of a normal or abnormal heart rate. This work directly aids the therapeutic professionals in diagnosis and restorative analysts in their ongoing research. The study's step-by-step methodology is presented as a flowchart in Fig. 1.

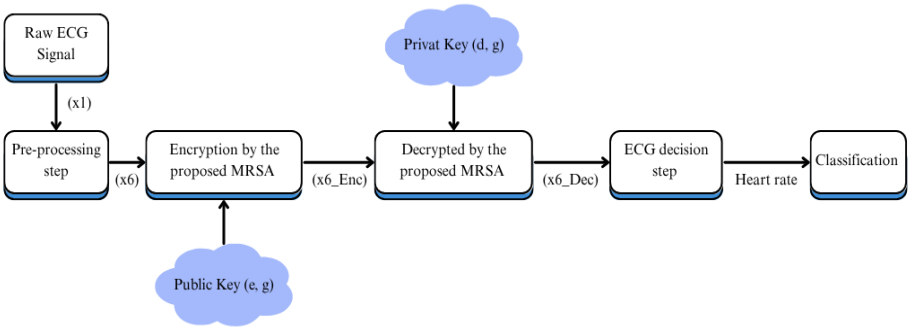


**Fig. 1.** A detailed flowchart of the study's methodology.

This study utilized raw electrocardiogram (ECG) data from the MIT-BIH arrhythmia database [13], a widely recognized standard for evaluating arrhythmia detectors and conducting cardiac flow research globally. The ECG signals utilized are 21600 samples long, recorded at a sampling rate of 360 Hz.

### 2.1 Signal processing steps

In this stage, the raw ECG signal is first passed through a bandpass filter. This filter reduces unwanted noise, keeping the important characteristics of the average QRS

complex [14]. After filtration, the signal undergoes discrimination, which exposes the steep slopes of the QRS complex by removing lower-frequency P- and T-waves. Next, the signal is squared point-by-point [15]. This operation ensures all data points are positive and nonlinearly amplifies the derivative's output, further emphasizing higher frequencies and mitigating false detections caused by large T-wave amplitudes. Finally, Moving Window Integration (MWI) is applied to extract waveform features, with a typical window width of 150 ms, and avoid merging or splitting QRS complexes [16].

### 2.2 Partially Homomorphic Encryption Technique—Modified RSA Algorithm (MRSA)

The RSA algorithm is one of the first significant advancements in encryption that utilized an asymmetric (public) key. This key is secure provided that it is adequately lengthy [17]. The fundamental concept behind our proposed MRSA is to increase the difficulty of breaking the encryption by making prime factorization even more challenging than in traditional RSA.

To significantly boost cryptographic complexity and make prime factorization considerably more challenging, our technique calculates 'n' using three distinct random prime integers (p, q, and s). These primes are generated by a Linear Congruential Generator (LCG). Crucially, 'g' is passed instead of 'n' in both the public and private keys. This architecture significantly improves security over standard RSA, as the public and private key exponents (e and d) can only be determined by knowing these three prime values. Because 'n' is never explicitly transmitted in any key, identifying 'e' and 'd' becomes exceptionally difficult, thus preventing easy decryption of messages. Furthermore, identifying three factors of 'n' using factorization techniques is intrinsically more challenging than factoring two, ensuring the algorithm's continuous security and overcoming a key limitation of traditional RSA. The steps for the MRSA algorithm are described below.

**MRSA Algorithm Design**

**Step 1:** Obtain the ECG signal (x6) after MWI

**Step 2:** Transform (x6) into the integer.

**Step 3:** Create keys for the MRSA Algorithm

1. Select p, q and s three primes using the LGC generator (The primality of these numbers is verified using the Miller-Rabin test), such that $p \neq q \neq s$
2. Compute $n = p * q * s$
3. Compute $\varphi(n) = (p-1) * (q-1) * (s-1)$
4. Chose an integer e such that $1 < e < \varphi(n)$ and $gcd(e, \varphi(n)) = 1$
5. Determined d as $d \equiv e\text{^}(-1) \ mod \ \varphi(n)$
6. Calculate $g = n - 2$
7. The public key (e, g)
8. The private key (d, g)

**Step 4:** Encrypt the signal (x6) with a public key.

$$x6_{Enc} = x6^{e} mod(g + 2)$$

**Step 5:** Decrypt the signal $x6_{Enc}$ using the private key.

$$x6_{Dec} = x6_{Enc}^{d} mod(g + 2)$$

### 2.3 Decision-Making

After decryption, the signal is reconverted to its original form to permit further analysis. Then, we used the decision phase of the Pan and Tompkins algorithm to detect QRS complexes by applying adaptive thresholds to the signal to differentiate it from noise. The precisely determined R-peak location is significant, as it permits the precise determination of the RR interval and, subsequently, the heart rate [18]. This determined heart rate is subsequently assessed as either normal or pathological (e.g., tachycardia or bradycardia), which provides important clinical information for medical experts and further guides the clinical study.

## 3 Results and Discussion

The proposed algorithm was implemented using Python 3.13 (64-bit). We evaluated its performance using various quantitative metrics, including histogram and correlation analyses, mean squared error (MSE), key generation, encryption, and decryption times. We also assessed the efficacy of classification using indicators such as positive predictive value (PPV), sensitivity (Se), accuracy (ACC), and detection error rate (DER).

Fig. 2 illustrates the ECG signal processing for record 103: bandpass filtering for noise reduction, differentiation to emphasize QRS slopes, squaring for positive value enhancement and frequency emphasis, and finally, moving window integration.

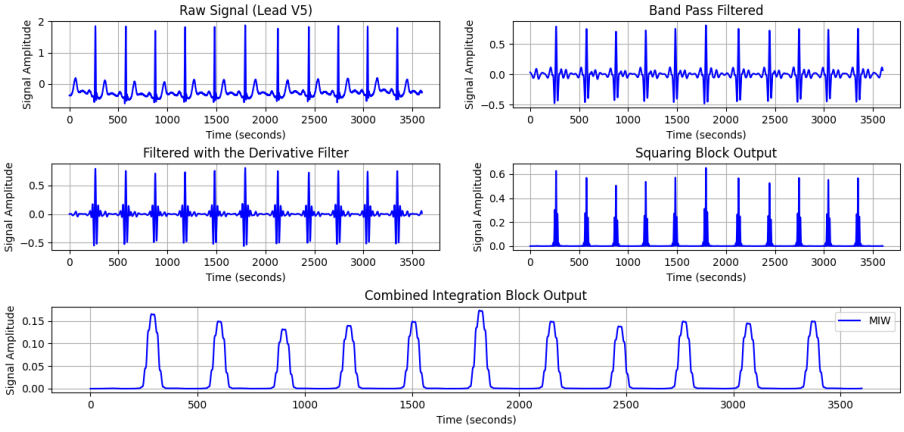


**Fig. 2.** Results of ECG processing (Record 103).

Fig. 3 displays the ECG signal after the integrated window output (x6), alongside the encrypted and decrypted signals. Our analysis shows that the original signal is

completely different from the encrypted version, as illustrated by a low correlation coefficient of approximately 0.0034. This low correlation is also visually apparent in Fig. 4, where the encrypted signal's histogram appears to be much more uniformly distributed, whereas the original signal's histogram displays distinct peaks. This demonstrates that the original data has been successfully obfuscated, guaranteeing robust privacy protection. Importantly, after decryption, as also shown in Fig. 3, we retrieve a signal that matches the original exactly, verified by an extremely low Mean Squared Error (MSE) of $8.22 \times 10^{-22}$. These results are extremely significant, clearly demonstrating the reliability and effectiveness of our encryption technique in maintaining the original signal's integrity.

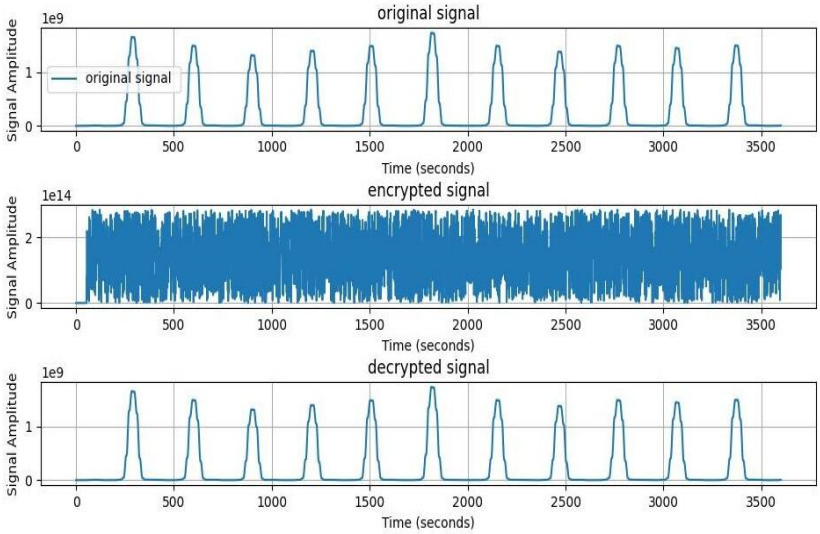


**Fig. 3.** ECG encryption/decryption results.

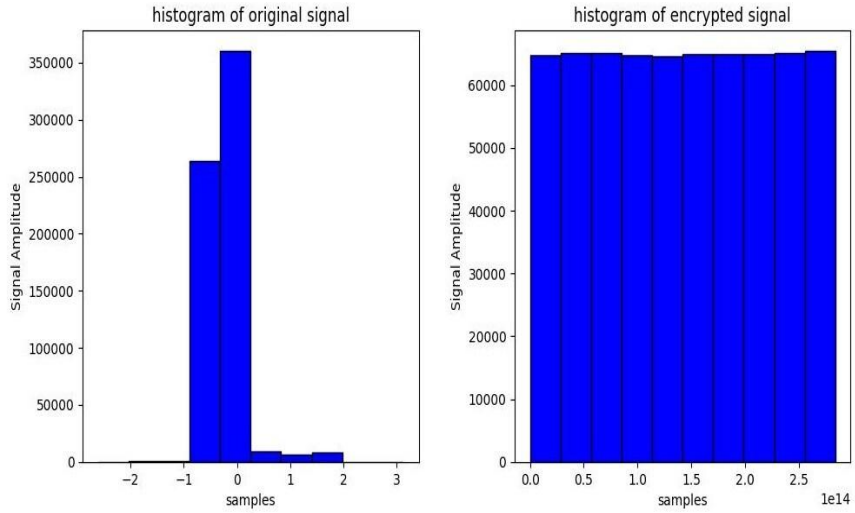


Fig. 4. Histogram analysis of original and encrypted signal.

The algorithm's homomorphic characteristic is confirmed in Fig. 5, where the decryption of the encrypted signal $C_1 \times C_2$ is shown to be identical to the product of the original squaring output (x5) and the moving window integral output (x6). The observed Mean Squared Error (MSE) of zero between these two signals confirms that the algorithm accurately performs operations on encrypted data, yielding results consistent with operations on their unencrypted counterparts.

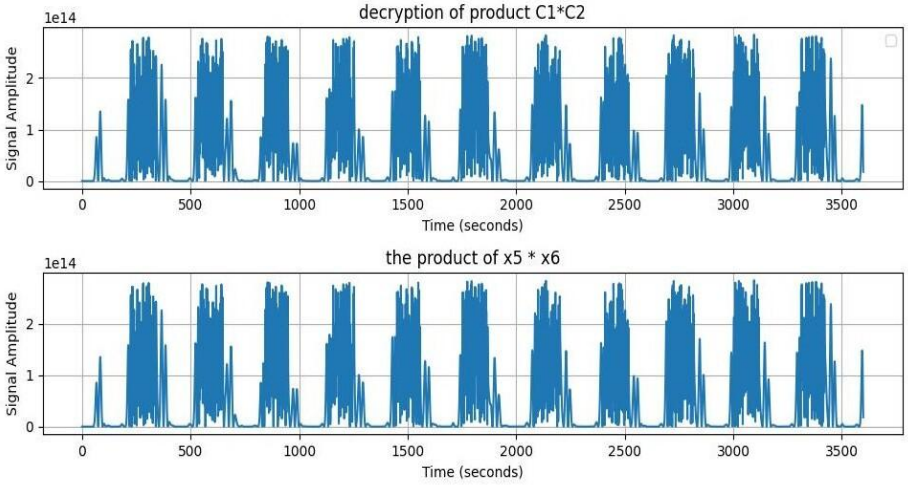


**Fig. 5.** Verification of homomorphic property.

The graphs below illustrate the time complexity of both algorithms, using fixed values of (p, q, and s) for varying signal sizes. Instead of 'n', our modified RSA algorithm

employs 'g' as the modulus. The following graphs present a comparison of the two algorithms concerning key generation speed, encryption speed, decryption speed, and total execution time.

Despite its enhanced security, the modified RSA algorithm shows only a slight increase in time complexity. MRSA has a faster key generation than RSA, as shown in the Table 1.

**Table 1:** Comparative key generation times.

| Size of prime numbers | Key Generation time of | |
|---|---|---|
| | MRSA Algorithm | Correct record detection |
| 16 bits | 0 s | 0,00014 s |
| 32 bits | 0,0001 s | 0,0012 s |
| 64 bits | 0,0001 s | 0,00138 s |
| 128 bits | 0,00026 s | 0,00326 s |
| 256 bits | 0,00054 s | 0,01242 s |
| 512 bits | 0,00228 s | 0,06674 s |
| 1024 bits | 0,00394 s | 0,9825 s |
| 2048 bits | 0,02272 s | 8,3726 s |

Fig. 6 and Fig. 7 show slightly longer encryption and decryption times due to the added steps.

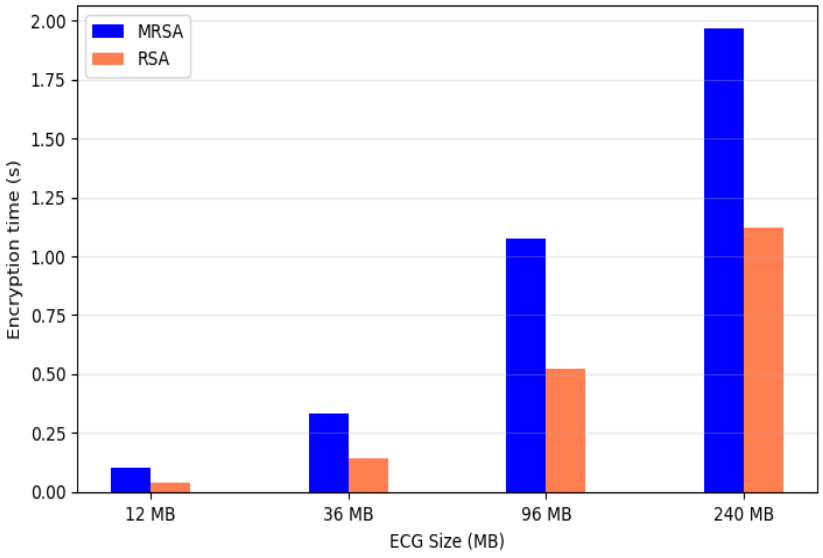


**Fig. 6.** Encryption time comparison between RSA and MRSA.

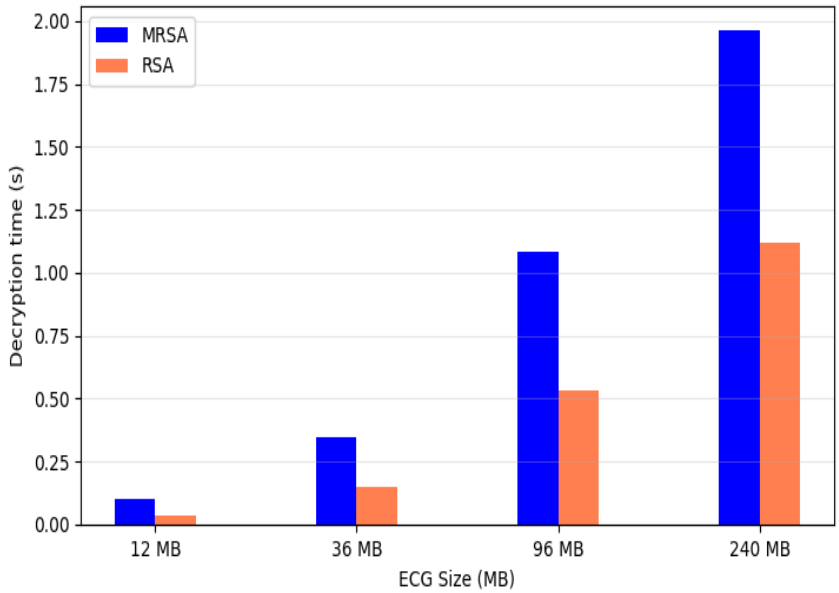


**Fig. 7.** Decryption time comparison between RSA and MRSA.

Our algorithm's performance, as compared with the study by Shaikh et al. [12], is summarized in Table 2. This comparison focuses on critical metrics, including accuracy, sensitivity, positive predictive value, and Detection Error Rate (DER). Our findings revealed that all 20 tested records yielded results that matched the database after using our proposed method to secure the ECG signal.

**Table 2.** Comparison between our proposed method and the study of Shaikh et al.

| Method | Record used | Correct record detection | ACC (%) | Se (%) | PPV (%) | DER (%) |
|---|---|---|---|---|---|---|
| [12] | 20 | 18 | 90 | - | - | - |
| Our method | 20 | 20 | 99.99 | 99.79 | 99.86 | 0.01 |

To further evaluate our algorithm's performance, we used 48 ECG records. Of these, 47 yielded results that perfectly matched the database. However, record 108 was an outlier; our algorithm classified its heart rate at 115 bpm, whereas the database range for this record is 44-78 bpm. These evaluation results are presented in Table 3.

**Table 3.** Summary of MRSA's performance.

| Method | Record used | Correct record detection | ACC (%) | Se (%) | PPV (%) | DER (%) |
|---|---|---|---|---|---|---|
| Our method | 48 | 47 | 99.86 | 98.57 | 97 | 0.14 |

## 4 Conclusions

This research proposes an innovative security method for protecting sensitive ECG signals during network transmission in healthcare. It merges the Pan and Tompkins approach for preprocessing with a partially homomorphic encryption method, specifically the modified RSA algorithm (MRSA), addressing the need for secure and privacy-preserving management of patient heart data. The MRSA method significantly enhances security through a more intricate key generation process, making it highly resistant to factorization attacks. Our comprehensive experimental findings, using the MIT-BIH Arrhythmia Database, confirm the technique's efficacy and dependability. It achieved exceptional accuracy (99.86%), sensitivity (98.57%), and positive predictive value (97%) in heart rate classification, alongside minimal mean squared error during decryption, validating data integrity and encryption strength. The demonstrated homomorphic property facilitates secure computations on encrypted data, crucial for healthcare analytics. Despite a slight increase in computing time, the MRSA algorithm's superior security justifies this trade-off, especially for sensitive ECG data. This study establishes a strong foundation for advancing secure and efficient healthcare systems, benefiting clinicians and medical research.

## Acknowledgements

This study was supported by the Algerian Ministry of Higher Education and Scientific Research through funding for PRFU Project.

## References

1. Maddio, S.: The electrostatic foundation of the electrocardiogram. URSI Radio Sci. Bull. 2020, 78–82 (2020). https://doi.org/10.23919/URSIRSB.2020.9318446.
2. Singh, A.K., Krishnan, S.: ECG signal feature extraction trends in methods and applications. Biomed. Eng. Online. 22, 22 (2023). https://doi.org/10.1186/s12938-023-01075-1.
3. Anbalagan, T., Nath, M.K., Vijayalakshmi, D., Anbalagan, A.: Analysis of various techniques for ECG signal in healthcare, past, present, and future. Biomed. Eng. Adv. 6, 100089 (2023). https://doi.org/10.1016/j.bea.2023.100089.
4. Belkacem, S., Messaoudi, N., Dibi, Z.: Artifact removal from electrocardiogram signal: A comparative study. In: 2018 International Conference on Signal, Image, Vision and their Applications (SIVA). pp. 1–5. IEEE (2018). https://doi.org/10.1109/SIVA.2018.8661013.
5. Georgieva-Tsaneva, G., Cheshmedzhiev, K., Tsanev, Y.-A., Dechev, M., Popovska, E.: Healthcare Monitoring Using an Internet of Things-Based Cardio System. IoT. 6, 10 (2025). https://doi.org/10.3390/iot6010010.
6. Rajasree, G., Kumar, R.M.S.: Secure transmission and monitoring of ECG signals based on chaotic mapping algorithms. Automatika. 65, 957–972 (2024).

https://doi.org/10.1080/00051144.2024.2306758.
7. Ryu, J., Kim, K., Won, D.: A Study on Partially Homomorphic Encryption. Proc. 2023 17th Int. Conf. Ubiquitous Inf. Manag. Commun. IMCOM 2023. 31–34 (2023). https://doi.org/10.1109/IMCOM56909.2023.10035630.
8. Mahmood, Z.H., Ibrahem, M.K.: New Fully Homomorphic Encryption Scheme Based on Multistage Partial Homomorphic Encryption Applied in Cloud Computing. In: 2018 1st Annual International Conference on Information and Sciences (AiCIS). pp. 182–186. IEEE (2018). https://doi.org/10.1109/AiCIS.2018.00043.
9. Munjal, K., Bhatia, R.: Analysing RSA and PAILLIER homomorphic Property for security in Cloud. Procedia Comput. Sci. 215, 240–246 (2022). https://doi.org/10.1016/j.procs.2022.12.027.
10. Intila, C., Gerardo, B., Medina, R.: A study of public key 'e' in RSA algorithm. IOP Conf. Ser. Mater. Sci. Eng. 482, 012016 (2019). https://doi.org/10.1088/1757-899X/482/1/012016.
11. Aggarwal, D., Maurer, U.: Breaking RSA Generically Is Equivalent to Factoring. IEEE Trans. Inf. Theory. 62, 6251–6259 (2016). https://doi.org/10.1109/TIT.2016.2594197.
12. Shaikh, M.U., Adnan, W.A.W., Ahmad, S.A.: Secured Electrocardiograph (ECG) Signal Using Partially Homomorphic Encryption Technique–RSA Algorithm. Pertanika J. Sci. Technol. 28, 231–242 (2020). https://doi.org/10.47836/pjst.28.s2.18.
13. Moody, G.B., Mark, R.G.: The impact of the MIT-BIH Arrhythmia Database. IEEE Eng. Med. Biol. Mag. 20, 45–50 (2001). https://doi.org/10.1109/51.932724.
14. İhsan, A., Doğan, N.: An innovative image encryption algorithm enhanced with the Pan-Tompkins Algorithm for optimal security. Multimed. Tools Appl. 83, 82589–82619 (2024). https://doi.org/10.1007/s11042-024-18722-x.
15. Bali, J., Nandi, A., Hiremath, P.S., Patil, P.G.: Detection of sleep apnea in ecg signal using pan-tompkins algorithm and ann classifiers. Compusoft. 7, 2852–2861 (2018).
16. Imtiaz, M.N., Khan, N.: Pan-Tompkins++: A Robust Approach to Detect R-peaks in ECG Signals. In: 2022 IEEE International Conference on Bioinformatics and Biomedicine (BIBM). pp. 2905–2912. IEEE (2022). https://doi.org/10.1109/BIBM55620.2022.9995552.
17. Jasim, A.H., Kashmar, A.H.: An Evaluation of RSA and a Modified SHA-3 for a New Design of Blockchain Technology. In: Artificial Intelligence for Smart Healthcare. pp. 477–489 (2023). https://doi.org/10.1007/978-3-031-23602-0_28.
18. Ahmed, A.A., Madboly, M.M., Guirguis, S.K.: Securing Signal Encryption Based on Reduced Round Homomorphic AES. Int. J. Intell. Eng. Syst. 16, 440–454 (2023). https://doi.org/10.22266/ijies2023.0630.35.