

Implementing and developing multi-stage cryptography technique for low-cost long-range communication system

Eyad M. Hamad¹, Samer Alabed¹, Amer Alsaraira¹, Omar A. Saraereh²

¹Department of Biomedical Engineering, School of Applied Medical Sciences, German Jordanian University, Amman, Jordan

²Department of Electrical Engineering, Faculty of Engineering, The Hashemite University, Zarqa, Jordan

Article Info

Article history:

Received Jun 14, 2023

Revised Aug 2, 2023

Accepted Aug 30, 2023

Keywords:

Chipers

Communication system

Cryptography

Emergency system

Long-range technology

Security

ABSTRACT

The requirement for a secure emergency communication system has become imperative in tandem with the industrial revolution. Additionally, the development of technology has led to increasingly robust penetration techniques that pose a threat to communication system security, leaving data vulnerable to unwanted third parties. This paper introduces a novel, powerful security approach that ensures a secure emergency communication system. Moreover, this research focuses on several cryptographic techniques among various symmetric and asymmetric ciphers, including advanced encryption standards, substitution, and transposition. The article presents an affordable and secure communication system that can transmit data over long distances with low power consumption using long-range technology. This system features a unique function that transmits updated locations, directing rescuers to the designated location.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Eyad M. Hamad

Department of Biomedical Engineering, School of Applied Medical Sciences

German Jordanian University

Amman, 11180 Jordan

Email: Eyad.Hamad@gju.edu.jo

1. INTRODUCTION

The vulnerability of cellular networks and wireless technologies during natural disasters or destructive events has been widely reported [1]–[3]. These technologies require cell towers and expensive infrastructure to operate, which are susceptible to damage, leading to communication disruptions and obstructing help requests. For example, Hurricane Harvey caused extensive damage to cell towers and call centers, resulting in the internet being disabled in nearly two thousand homes [4]. Similarly, during the Baltimore riots in 2015, cell towers were unable to handle the overload, resulting in the paralyzation of police communications and approximately a hundred death cases from police officers [5]. Communication devices have revolutionized the way we connect and exchange information across the globe. However, in certain regions or during emergencies, existing communication systems may prove unreliable or inaccessible, leading to significant challenges in communication and coordination. To address these limitations and provide a solution that is affordable, power-efficient, and secure, this research proposes the development of a low-cost communication device capable of transmitting messages over long distances while prioritizing energy conservation and message security [6]–[11].

The primary objective of this research is to create a communication device that offers an efficient means of transmitting messages in areas with limited infrastructure or during critical situations where traditional communication channels may be compromised. To enhance its versatility and usefulness, the proposed device will also incorporate a global positioning system (GPS) feature to enable location sharing,

ensuring that aid can be dispatched promptly in emergencies. The successful development and deployment of such a low-cost communication device hold vast potential to bridge communication gaps, enhance emergency response capabilities, and empower individuals and communities with reliable means of information exchange. This research endeavors to contribute to the advancement of communication technology, especially in regions where conventional communication infrastructure is limited, while also prioritizing the safety and security of transmitted messages [6]–[11].

The implementation of this project involves two main aspects: hardware and software. The hardware component centers on long-range (LoRa) technology, combined with elements like Arduino, keyboard, screen, and solar panels. On the software front, the emphasis lies on cryptography and a user-friendly interface, encompassing essential factors such as affordability, energy efficiency, user-friendliness, indoor coverage, and robust security. This proposed device has the potential to serve as a valuable resource during emergencies, potentially saving lives and offering assistance to those in distress. The objective of this research is to present a comprehensive design and execution of such a device, evaluating its performance in various scenarios, including natural disasters and human-induced destructive events. Ultimately, this study aims to contribute to the enhancement of communication resilience and emergency response systems.

2. METHOD

The long-range low-power wireless modulation, known as LoRa, represents a cutting-edge wireless technology that has gained significant attention and recognition in recent years [12], [13]. Studies have consistently demonstrated LoRa's outstanding capability to facilitate long-range communication with reliable coverage, making it a preferred choice for various applications, particularly in remote and challenging environments. The integration of chirp pulses and chirp spread spectrum (CSS) in LoRa's data transmission mechanism contributes to its robust performance and efficient utilization of radio frequency resources.

A crucial aspect of LoRa's appeal is its ability to safeguard sensitive data from unauthorized access. Through the implementation of advanced cipher algorithms, LoRa ensures end-to-end encryption with a robust 128-bit key. This security feature instills confidence in users, enabling them to transmit and receive data with enhanced privacy and protection. The LoRa Alliance, a consortium of leading technology companies and organizations, has diligently specified the technical parameters and standards for LoRa's operation. Data transmission occurs over specific radio frequency bands, including 433 MHz, 868 MHz, and 915 MHz. These well-defined frequency bands enable interference-free communication and ensure the coexistence of various LoRa-based applications.

LoRa's efficiency in transmitting small data chunks with low bit rates over extensive distances is truly remarkable. This unique capability is particularly advantageous for internet of things (IoT) applications, where devices often need to communicate essential information using minimal energy and bandwidth resources. Such efficiency translates into prolonged battery life and reduced operational costs for IoT deployments, further solidifying LoRa's position as a cost-effective and sustainable solution. The competitiveness of LoRa is reinforced by research that compares it with other IoT technologies, such as SigFox and weightless standards. Previous studies have consistently shown that LoRa exhibits the highest raw spectral efficiency among these technologies. Factors considered in the comparison include raw spectral efficiency, data rate, and spreading factors, among others. LoRa's superior spectral efficiency ensures optimal utilization of available frequency bands and makes it an ideal choice for IoT applications with stringent data transmission requirements.

In summary, long-range low-power wireless modulation is a wireless technology that uses chirp pulses and chirp spread spectrum to send data [12], [13]. Recent studies have shown that LoRa is capable of providing long-range communication with reliable coverage. It is also capable of protecting data from unauthorized access using cipher algorithms. The LoRa Alliance specifies that LoRa uses 128-bit end-to-end encryption and transmits data using radio frequency signals on the 433 MHz, 868 MHz, and 915 MHz frequency bands. LoRa's ability to transmit small chunks of data with low bit rates over long distances is remarkable. Previous research indicates that LoRa has the highest raw spectral efficiency when compared with other IoT technologies such as SigFox and weightless standards. The comparison was based on features such as raw spectral efficiency, rate, and spreading factors, among others.

2.1. Cryptography

Cryptography is an essential tool in securing data from unauthorized access, achieved by converting information into an unreadable format through the use of mathematical algorithms and cryptographic techniques [14]–[17]. Its name is derived from the ancient Greek terms “krypto” meaning secret and “graphein” meaning message. Cryptography involves two primary processes: encryption and decryption. Encryption is the process of converting plaintext into ciphertext, while decryption is the opposite process of converting ciphertext back to plaintext [14], [15], [17]. To decrypt the message and access the original

content, a secret key or password is required. Cryptography's main goal is to safeguard confidential information by implementing an unintelligible layer of text, making it possible for only intended individuals to decrypt the encrypted message using a key shared between them. Cryptography is also referred to as the art of secrets, as it ensures that all necessary information is protected from attackers.

2.2. Cryptography key

It is essential to understand the two primary types of cryptographic keys: symmetric keys and asymmetric keys [16]–[20]. Symmetric key encryption involves generating one private key, which is then shared between two authorized individuals. Without the private key, no one else can view the message's content. Using the same private key, the intended recipient can decrypt the message and restore it to its original format [16], [18], [20]–[24]. Examples of symmetric keys include advanced encryption standards (AES), blowfish (BF), and data encryption standards (DES). On the other hand, asymmetric key encryption employs a public key to encrypt the plaintext and a private key to decrypt it. The private key is kept secret and can only be decrypted by the authorized recipient, while the public key is accessible to anyone else. The asymmetric algorithm is reversible, meaning that if two individuals are communicating, one can encrypt the message using a public key, while the other can decrypt that message using a private key. Examples of asymmetric encryption include the Rivest, Shamir, Alderman (RSA) system and the elliptic curve cryptosystem (ECC).

2.2.1. Symmetric encryption

We propose a new encryption system that utilizes one or more symmetrical encryption techniques to modify characters, numbers, and symbols and encrypt plaintext with a private key. Our system incorporates the encryption methods outlined in references [16], [18], [20]–[22] to enhance security. We aim to provide a more robust and effective method of data encryption that can be applied in various settings to ensure the protection of sensitive information. As demonstrated, symmetric key algorithms exhibit superior performance compared to asymmetric algorithms.

- a. AES: the AES has gained widespread popularity as a reliable symmetrical encryption key for protecting data against potential threats. Its adoption was initiated by the National Institute of Standards and Technology (NIST) in 1997, in response to the vulnerabilities of DES. The latter has been rendered obsolete due to its short key length, which facilitated penetration within a brief period. Thus, AES emerged as a viable solution for data protection, offering enhanced security features. Notably, on November 26, 2001, AES was officially ratified as a federal standard. Its superiority lies in its capability to support a wide range of key lengths, which adds an additional layer of protection against malicious attacks. The AES employs keys that are 128, 192, and 256-bit in length, with 10, 12, and 14 rounds of encryption, respectively, as outlined in [24]. The algorithm comprises three layers, with each layer performing a specific mathematical function.
- b. Transposition: as a symmetric cryptographic algorithm, the transposition algorithm relies on reordering the plaintext elements to produce ciphertext [14]. There are various techniques under the transposition algorithm, such as the simple columnar and rail fence techniques.
 - Rail fence: the technique involves writing the plaintext diagonally and then reading it as a sequence of rows [14].
 - Simple columnar: as a symmetric cryptographic algorithm, the simple columnar transposition technique involves writing the plaintext in a rectangular shape, row by row, and then reading it column by column [13], [14]. The number of rows and columns in the rectangle must be taken into consideration. Moreover, both the sender and the receiver must be aware of the key used to rearrange the rectangle columns.
- c. Substitution: as a common practice, cipher algorithms frequently employ the substitution technique to convert plaintext to ciphertext (encryption) and vice versa (decryption) by substituting one character or group of characters with another. This technique utilizes a table of letters, with the first row arranged in alphabetical order and the second row arranged in a cryptographic sequence. The order of the exchanged letters between the sender and the receiver is sometimes determined by the key. Therefore, both parties must possess the same table to encrypt and decrypt the message.

2.2.2. Asymmetric encryption

Instead of using symmetric keys, asymmetric key encryption utilizes two keys: one public key to encrypt and one private key to decrypt [25]–[33]. RSA is a widely recognized example of asymmetric cryptography [33], and numerous researchers have favored it as the most popular and well-known algorithm. Furthermore, RSA is included in asymmetric encryption, which also encompasses the elliptic curve

cryptography algorithm [27]–[32]. This algorithm was invented eight years after RSA's creation. Later, many techniques have been proposed on one or more of the previously mentioned approaches [34]–[38].

- RSA: in [25], [27] the RSA encryption algorithm is an example of asymmetric cryptography, which is named after its three creators: R. Rivest, A. Shamir, and L. Adleman. This algorithm's security is based on the fact that finding two large prime numbers is relatively easy while factoring the primes' product is incredibly challenging [27]. Nonetheless, modern computer advancements have made it easier to factor in large primes, resulting in possible RSA attacks. In RSA, the plaintext is encrypted using a public key to generate ciphertext, while a private key is utilized to decrypt the plaintext.

To encrypt and decrypt data using RSA, the public key, known to everyone in the network domain, is used in addition to the private key, which is kept secret except for the intended recipient. The RSA algorithm includes the following steps [25], [26]:

- a. Key generation: key generation should be prior before data encryption and decryption, as shown below. m : plaintext, C : ciphertext, n : modular value, e : public exponent, d : private exponent.

- 1) Select two prime numbers a and b . Note that, a and b should be random integers that have similar bit lengths.

- 2) Compute a modular value $\rightarrow n = a \times b$.

- 3) Compute Euler's totient function:

$$\emptyset(n) = (a - 1) \times (b - 1) \quad (1)$$

- 4) Randomly select an integer to be the public encryption key (e) where $1 < e < \emptyset(n)$ and the greatest common divisor of e , $\emptyset(n)$ is 1.

- 5) Determine the private decryption key (d) as (2):

$$d = e - 1(\text{mod } \emptyset(n)), \text{ so that } d = ((\emptyset(n) \times i) + 1)/e \quad (2)$$

- 6) The public encryption key (PK) includes the modulus n and the public exponent e :

$$PK = (e, n) \quad (3)$$

- 7) The private decryption key (PR) includes the modulus n and the private exponent d :

$$PR = (d, n) \quad (4)$$

- b. RSA encryption: the process of converting plain text to cipher text is known as RSA encryption. The encryption procedure is described in the following steps:

- The receiver must first share the sender's public key (e, n) with the sender prior to actually sending data to the intended recipient.

- To generate the cipher text, the sender encrypts the data using (5):

$$C = me(\text{mod } n) \quad (5)$$

- c. RSA decryption: the process of attempting to recover the plain text using the private key (d, n) is known as RSA decryption.

$$m = Cd(\text{mod } n) \quad (6)$$

2.3. Hardware implementation

This work went through many enhancements. The first design used an Arduino microcontroller with long range wide area network (LoRaWAN) to transmit and receive data. In addition, the means of input was a keyboard, and a liquid crystal display (LCD) was used to display the output as shown in the following block diagram shown in Figure 1.

After that, a solar panel was added to power up the system in an eco-friendly way. In addition, the LoRa shield was utilized instead of LoRa R01 for additional features of stability and a more extended range. This stage of the design is shown in the following block diagram in Figure 2.

Finally, a GPS module was inserted into the system's features which finalizes the system demonstrated in Figure 3. The block diagram in Figure 4 represents the process implemented in secure emergency communication system (SECS) and all potential participants in such a system (sender/receiver, and intruder). The system can process both speech or voice messages inputted using a mic or a text message inputted using a keyboard. If the message was entered as a voice, a speech-to-text (STT) converter algorithm would be used to convert this message to text. Furthermore, with a GPS, the sender can share their location

information with the plaintext of the sent message. The plaintext will be processed later in a microcontroller. Moreover, using an encryption algorithm, the plaintext will be encrypted to protect the confidentiality of any conversation from getting compromised during the transmission process. Data will get transmitted and received using LoRa module, which is mounted on the microcontroller using LoRa shield and is considered the main module in this system. Data transmitted and received are all cyphertext to avoid any eavesdropping from the unwelcome recipient.

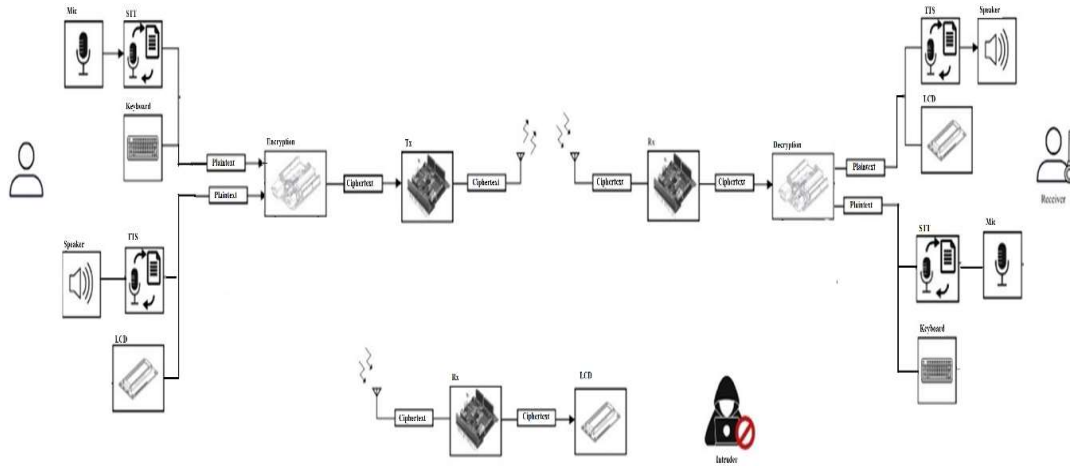


Figure 1. Block diagram of the initial system design

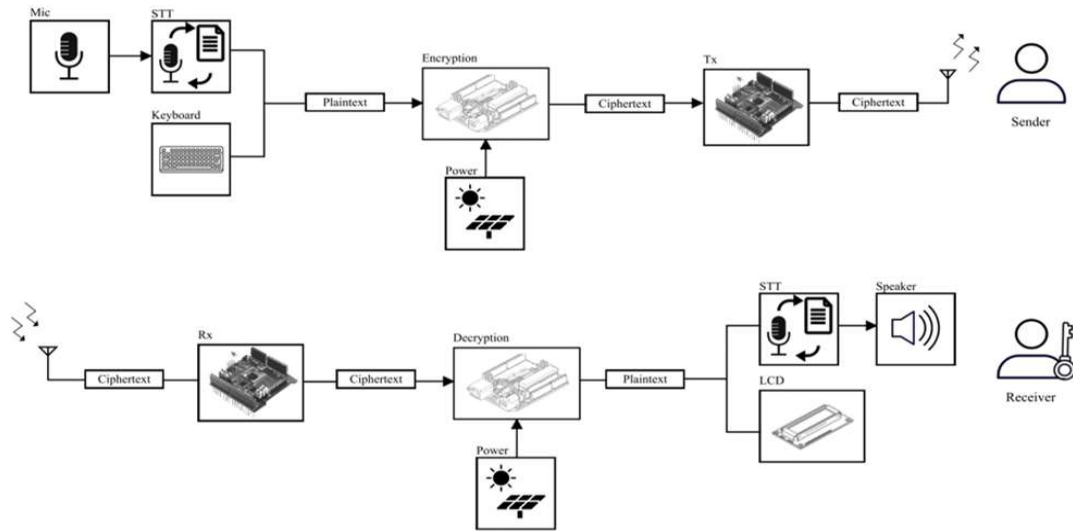


Figure 2. Block diagram of the second design of the system

Any intruder who uses a module that has the same free-sending frequency will receive a meaningless ciphertext. In other words, only targeted LoRa that has compatible encryption and decryption algorithms will be able to retrieve ciphertext to plaintext. The receiver will have two output options, either to hear the message using a speaker after converting the received text to speech using text-to-speech (TTS) converter algorithm or to display the message using LCD. Arduino processor (ATmega 328P) will have all algorithms (such as TTS/STT, encryption/decryption) saved and run them when required to do so.

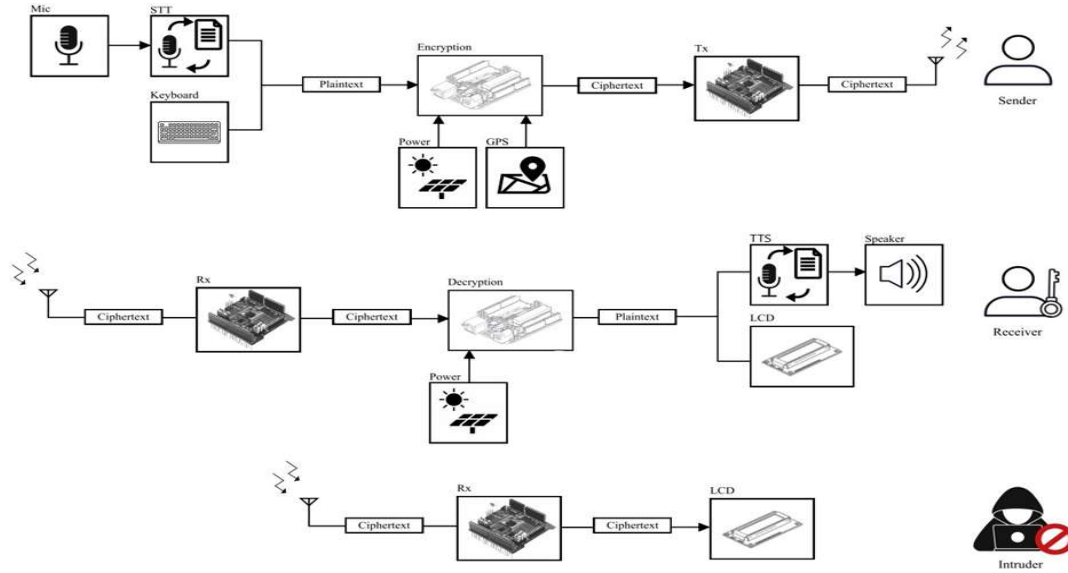


Figure 3. Block diagram of the high-level design of a two-way secure communication system

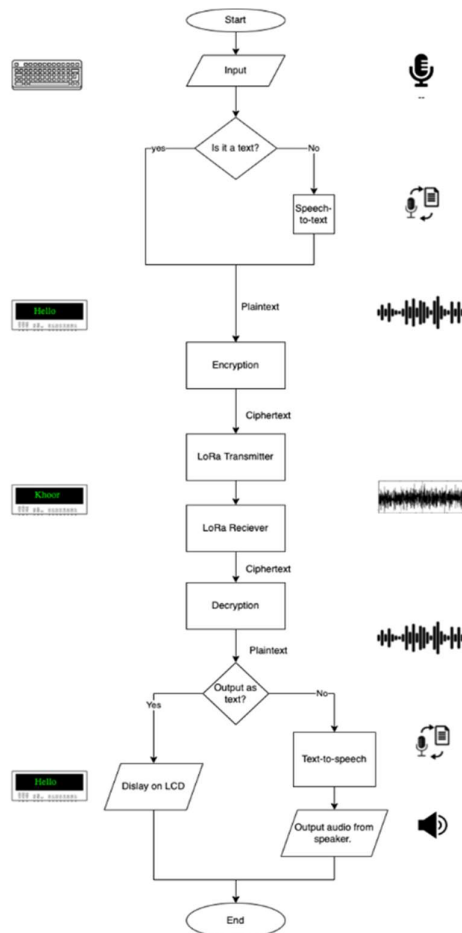


Figure 4. Flow chart of high level design

Table 1 details the connection interface between LoRa and Arduino if LoRa shield was not utilized. Otherwise, if the LoRa shield was used, it is only required to mount it over Arduino pins such that all Arduino pins enter their corresponding socket in LoRa shield. In both systems, with or without LoRa shield, the outputs will be similar except that LoRa shield has a wider transmitting range since it utilizes a better antenna. In other words, Table 1 will not be required if LoRa shield was used. As in Table 2, VCC LCD's pin can be connected to any external 5 V power source to power up the I2C and LCD module. The liquid crystal display can transmit and receive data through an SDA pin using SCL to synchronize data traffic. Table 3 shows the connection of the GPS module with Arduino.

Any secure emergency communication system user's device will have the same circuit diagram as the one presented in Figure 5 regardless of the device's purpose (either to send or receive). Since the system is based on a LoRa transmitter, both the sender and receiver will have the same components, connections, and functionality. The system is composed Arduino microcontroller, LoRa module, antenna, LCD, and GPS.

Table 1. Interfacing LoRa module with Arduino

LoRa pin number	LoRa pin name-description	Arduino pin
1	GND-ground (0 V)	GND
2	GND-ground (0 V)	GND
3	3.3V-power (3.9 V maximum)	3V3
4	Reset-reset	D9
5	DIO0-digital I/O	D2
6	DIO1-digital I/O	-
7	DIO2-digital I/O	-
8	DIO3-digital I/O	-
9	GND-ground (0 V)	GND
01	DIO4-digital I/O	-
11	DIO5-digital I/O	-
12	SCK-SPI clock input	D13
13	MISO-SPI data output	D12
14	MOSI-SPI data input	D11
15	NSS-SPI chip select input	D10
16	GND-ground (0 V)	GND

Table 2. Interfacing I2C module with Arduino

I2C LCD pin number	I2C LCD pin name-description	Arduino pin
1	GND-ground (0 V)	GND
2	VCC-power	5V
3	SDA-serial data line	A4
4	SDL-serial clock line	A5

Table 3. Interfacing GPS module with Arduino

GPS pin number	GPS pin name-description	Arduino pin
1	Tx	D0
2	Rx	D1
3	VCC-power	VIN
4	GND-ground (0 V)	GND

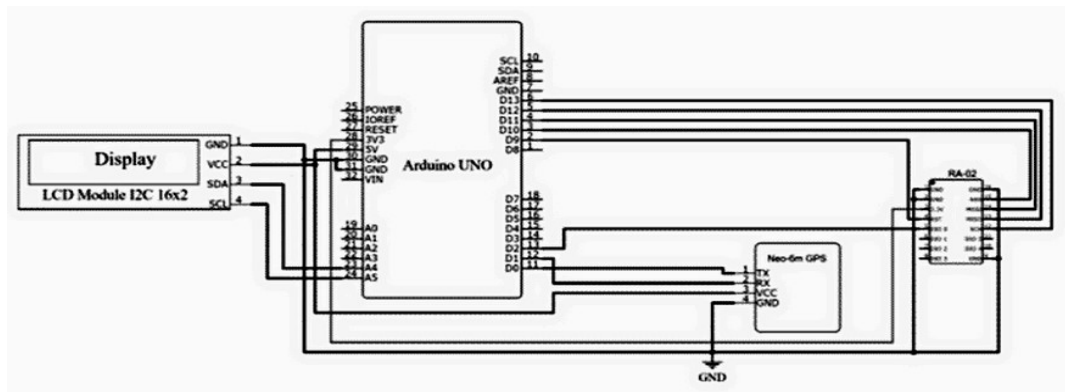


Figure 5. Schematic diagram of the circuit

2.4. Software implementation

By acknowledging all encryption techniques up to 2022, it could be recognized that the world is still suffering from relatively inefficient security transmission systems. Therefore, the need for a robust uncrackable encryption approach that meets the telecommunication era and protects the data is growing. Generally, the SECS is designed to provide a highly secure protection approach that encrypts data using a combination of symmetric and asymmetric techniques. Accordingly, the three main pillars that SECS adopts are substitution, AES, and transposition as illustrated in Figure 6. Without further due, let us expand the new approach:

- a. Initially, the three techniques will be ordered on a scale from 1 to 3 in each new cryptosystem.
- b. Hence the SECS depends on AES-128 bit, a private key of length 16-bytes should be created in advance. Assuming the following private key: PEN DEFEATS SWORDS as shown in Figure 7.
- c. Then, the first 3 characters of the private key will be sorted in ascending order as shown in Figure 8.

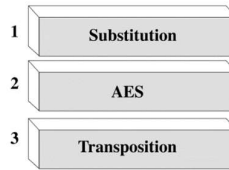


Figure 6. Sorting the chosen techniques

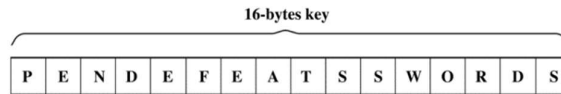


Figure 7. 16 bytes private key

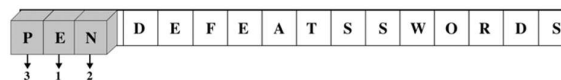


Figure 8. Selecting the first four bytes

The selected three characters of the private key will play a role to sort the execution of the three layers depicted in Figure 9. The main idea is that this order will constantly change if the private key is changed to keep the security level. With this approach, the system will be hard enough in front of any hacking attempts as it offers a new mystery to decrypt each time a new key is generated. Depending on the chosen order of the cryptographic techniques in step 1, the implementation of each layer will be as follows:

- a. Assume the plaintext is: he was in the museum. The plaintext will be encrypted first using the transpositions layer, based on what had been explained in the transposition section, a 4 by 4 matrix will be created to organize the 16-byte plaintext. However, the SECS will get the benefit of this approach by making the matrix reading depend on the 1st character in the key as follows:
 - If the key begins with a letter, the ciphertext will be read column by column.
 - If the key begins with a number, the ciphertext will be read from right to left.
 - If the key begins with a special character, the ciphertext will be read in a zigzag form.

In this example, as shown in Figure 10, the private key begins with a letter, so the ciphertext generated from this layer will be: hshseieewnmuatum.

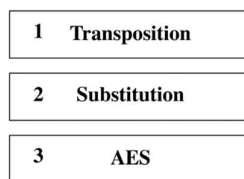


Figure 9. Rearranging the order based on the private key

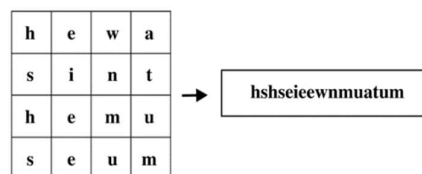


Figure 10. Transposition implementation

b. Next, the outputted ciphertext of the previous layer will be reinputted to the substitution layer. The characters of the text and the key will be translated to the equalized ASCII binary format as a primary step:

Text: hshseieewnmuatum

Binary format:

01101000 01110011 01101000 01110011 01100101 01101001 01100101 01100101 01110111 01101110
01101101 01110101 01100001 01110100 01110101 01101101

Key: PEN DEFEATS SWORDS

Binary format:

01010000 01000101 01001110 01000100 01000101 01000110 01000101 01000001 01010100 01010011
01010011 01010111 01001111 01010010 01000100 01010011

c. Then, XORing both the text and the key, as shown in Figure 11.

Which equals the next cipher-text: >8#67&'47:3\$'<*>. By returning the Binary result to its ASCII format, the ciphertext of this layer will be: 86&7 / \$#=>".&1>

d. Then, AES will be implemented in the previous substitutional text to produce the following ciphertext as shown in Figure 12.

Text	Key
01101000 01110011	01010000 01000101
01101000 01110011	01001110 01000100
01100101 01101001	01000101 01000110
01100101 01100101	01000101 01000001
01110111 01101110	01010100 01010011
01101101 01110101	01010011 01010111
01100001 01110100	01001111 01010010
01110101 01101101	01000100 01010011
Result	00111000 00110110 00100110 00110111 00100000 00101111 00100000 00100100 00100011 00111101 00111110 00100010 00101110 00100110 00110001 00111110

Figure 11. Performing logical XOR on the plaintext and the key

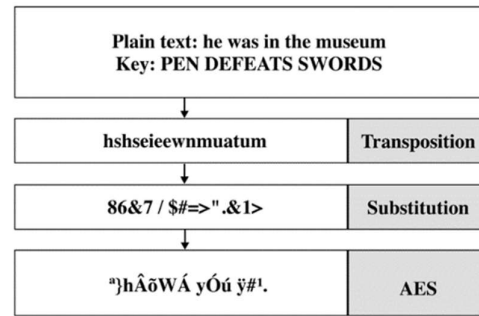


Figure 12. The process of the security system

3. RESULTS AND DISCUSSION

Several comprehensive experiments were meticulously conducted to assess and validate the prototype’s efficacy, yielding highly promising and significant results as anticipated. In the initial experiment, the focus was on evaluating the transmission process, where diverse modules were rigorously tested under varying conditions. This examination encompassed an extensive range of scenarios, including different environmental factors, signal strengths, and data payloads, ensuring a thorough assessment of the prototype’s transmission capabilities.


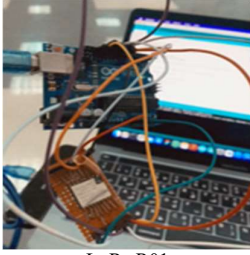


Building upon the insights gained from the first experiment, the second phase delved into an in-depth examination of the sophisticated security system incorporated into the selected module from the initial experimentation. This critical aspect of the prototype was subject to rigorous scrutiny, evaluating its ability to safeguard data from unauthorized access, potential cyber threats, and malicious intrusions. The robustness of the security system was put to the test, employing various encryption algorithms and authentication mechanisms to ascertain its resilience in real-world scenarios.

The successful outcomes of both experiments underscore the prototype’s reliability and resilience, validating its potential as a viable solution for long-range, low-power wireless communication with enhanced data security. The results provide valuable insights into the prototype’s performance and pave the way for further refinements and optimization to meet the specific requirements of diverse applications and industries. The significance of these findings extends beyond the scope of this research, as they contribute to the advancement of wireless communication technology, opening doors to a multitude of possibilities in modernizing and transforming connectivity solutions across various domains.

a. Experiment one: measuring transceiver’s tolerated distance. This experiment aims to assess the distance capabilities of different modules and identify the most suitable one to meet the specified requirements. The results, as presented in Table 4, showcase significant findings for each module that underwent testing. Notably, the LoRa shield and LoRa R01 modules exhibited exceptional performance in effectively transmitting and receiving data over long distances. In contrast, the NRF24-L01 and HC06 modules displayed considerably lower transmission rates compared to the other tested transceivers at the specified

distance. Based on a thorough evaluation of the data provided in Table 4, it was determined that the LoRa shield module perfectly aligns with the objectives of our work. Consequently, the decision was made to eliminate all other modules and solely proceed with the implementation of the LoRa shield for the project.

Table 4. Experiment one: measuring the distance for a different module

Module	Tested distance
 NRF24-L01	≈ 150 m ≈ 0.2 km
 LoRa R01	≈ 1.5 km
 HC-06	≈ 30 m
 LoRa shield	≈ 2.3 km

- b. Experiment two: security test. In this test, the LoRa shield was utilized to upload the security system described in the previous sections into Arduino. The experiment involved two parties: a sender and a receiver. The sender transmitted the message “Hello there!” to the recipient, as shown in Figure 13. The message was encrypted before being sent and could only be decrypted by the intended recipient. This process is similar to encapsulating the message, where the sender encapsulates the message and the receiver decapsulates it. An intruder attempted to decrypt the message, but the highly secure system prevented any unauthorized access. Results of experiment 2: i) intended recipient can decrypt the encrypted message and ii) the intruder receives a misleading message.

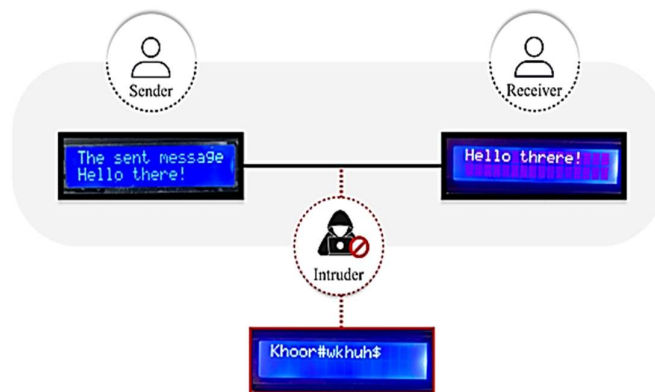


Figure 13. The sender and receiver of the security system

The secure emergency communication system has the potential to revolutionize multiple fields beyond emergencies. Its ability to securely transmit any type of data over vast distances without requiring cellular or satellite coverage makes it an ideal solution. Moreover, it can be implemented at a low cost. Some possible applications of this system are as follows:

- a. It can be combined with civilian and military robots and drones to securely send and receive data and control signals over long distances. This combination can be used in several sectors, including the oil and gas sector, electricity companies, army, and education establishments, to improve communication systems.
- b. The system can be used to establish a communication network that does not rely on any type of coverage, such as cellular, satellite, or the internet. This can be used in various sectors, including the oil and gas sector, the army, emergency and distress situations, civilian applications, bank/university/private sectors, and for building notification systems.
- c. It can be used to build an efficient and secure health and care system over long distances, without requiring SIM cards or internet and radio frequency coverage to transfer data and information between health and care establishments. The system can also be combined with sensors to monitor patients and detect any sudden changes in their health.
- d. The system can detect accidents and send the location to the nearest emergency establishment immediately when an accident occurs, potentially saving lives.
- e. The system can be used to build an efficient IoT system. It can operate using low energy and can be used in wireless networks, satellite applications, and social media.

4. CONCLUSION

To summarize the contents of our research paper, various investigations were carried out on transceivers. The findings indicate that the LoRa shield module represents a breakthrough in communication networks, thanks to its exceptional capabilities that enable users to utilize the system efficiently and effectively. The primary objective of this research was to evaluate the transmission of data over the air and identify the best module to enhance the secure emergency communication system. The results of the first phase of the study were significant, with the LoRa shield module outperforming all other modules. The second part of the research involved exploring different cipher algorithms, with a new approach proposed that utilized AES, transposition, and substitution. The paper's primary focus was on the use of LoRa in a secure system, with its potential applications spanning various sectors, including the military, education, and beyond. These findings bode well for the future of communication networks, as they promise reduced costs and energy consumption, as well as a more sustainable environment facilitated by the use of solar panels. Future research should focus on refining the system further to meet the needs of the labor market, as well as developing a fully functional secured mobile phone.




REFERENCES

- [1] S. Alabed, "Performance analysis of two-way DF relay selection techniques," *ICT Express*, vol. 2, no. 3, pp. 91–95, Sep. 2016, doi: 10.1016/j.ict.2016.08.008.
- [2] D. Taleb, S. Alabed, and M. Pesavento, "Optimal general-rank transmit beamforming technique for single-group multicasting service in modern wireless networks using STTC," in *WSA 2015: 19th International ITG Workshop on Smart Antennas, Ilmenau, Germany*, 2015, pp. 1–7.
- [3] S. Alabed, "Performance analysis of bi-directional relay selection strategy for wireless cooperative communications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, p. 97, Dec. 2019, doi: 10.1186/s13638-019-1417-1.
- [4] F. C. Commission, "Communications Status Report for Areas Impacted by Hurricane Harvey," 2018. [Online]. Available: <https://docs.fcc.gov/public/attachments/DOC-346419A1.pdf>
- [5] U.S. Department of Justice, Civil Rights Division, *INVESTIGATION OF THE BALTIMORE CITY POLICE DEPARTMENT*. 2016, pp. 1–163. [Online]. Available: https://www.justice.gov/d9/bpd_findings_8-10-16.pdf. Access date: 8 Nov 2023.
- [6] Y.-W. Ma and J.-L. Chen, "Toward intelligent agriculture service platform with lora-based wireless sensor network," in *2018 IEEE International Conference on Applied System Invention (ICASI)*, IEEE, Apr. 2018, pp. 204–207, doi: 10.1109/ICASI.2018.8394568.
- [7] P. Lu, "Design and Implementation of Coal Mine Wireless Sensor Ad Hoc Network Based on LoRa," in *2022 3rd International Conference on Information Science, Parallel and Distributed Systems (ISPDS)*, IEEE, Jul. 2022, pp. 54–57, doi: 10.1109/ISPDS56360.2022.9874124.
- [8] S. Alabed, M. Pesavento, and A. Klein, "Distributed differential space-time coding for two-way relay networks using analog network coding," *21st European Signal Processing Conference (EUSIPCO 2013), Marrakech, Morocco*, pp. 1–5, 2013.
- [9] S. Mishra, S. Nayak, and R. Yadav, "An Energy Efficient LoRa-based Multi-Sensor IoT Network for Smart Sensor Agriculture System," in *2023 IEEE Topical Conference on Wireless Sensors and Sensor Networks*, IEEE, Jan. 2023, pp. 28–31, doi: 10.1109/WiSNeT56959.2023.10046242.
- [10] A. I. Ali, S. Z. Partal, S. Kepke, and H. P. Partal, "ZigBee and LoRa based Wireless Sensors for Smart Environment and IoT Applications," in *2019 1st Global Power, Energy and Communication Conference (GPECOM)*, IEEE, Jun. 2019, pp. 19–23, doi: 10.1109/GPECOM.2019.8778505.
- [11] E. Zanaj, G. Caso, L. De Nardis, A. Mohammadpour, Ö. Alay, and M. G. Di Benedetto, "Energy Efficiency in Short and Wide-Area IoT Technologies—A Survey," *Technologies*, vol. 9, no. 1, Mar. 2021, doi: 10.3390/technologies9010022.
- [12] I. B. F. De Almeida, M. Chafii, A. Nimr, and G. Fettweis, "In-phase and Quadrature Chirp Spread Spectrum for IoT




- Communications,” in *2020 IEEE Global Communications Conference, GLOBECOM 2020 - Proceedings*, IEEE, Dec. 2020, pp. 1–6, doi: 10.1109/GLOBECOM42002.2020.9348094.
- [13] P. Edward, S. Elzeiny, M. Ashour, and T. Elshabrawy, “On the Coexistence of LoRa-and Interleaved Chirp Spreading LoRa-Based Modulations,” in *International Conference on Wireless and Mobile Computing, Networking and Communications*, IEEE, Oct. 2019, pp. 1–6, doi: 10.1109/WiMOB.2019.8923211.
- [14] S. Yoyalakshmi and R. Chakaravathi, “Development of an Efficient Algorithm in Hybrid Communication for Secure Data Transmission using LoRa Technology,” in *Proceedings of the 2020 IEEE International Conference on Communication and Signal Processing, ICCSP 2020*, IEEE, Jul. 2020, pp. 1628–1632, doi: 10.1109/ICCSP48568.2020.9182233.
- [15] S. Alabed, A. Alsaraira, N. Mostafa, M. Al-Rabayah, Y. Kotb, and O. A. Saraereh, “Implementing and developing secure low-cost long-range system using speech signal processing,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 3, pp. 1408–1419, Sep. 2023, doi: 10.11591/ijeecs.v31.i3.pp1408-1419.
- [16] C. Wheelus and X. Zhu, “IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework,” *IoT*, vol. 1, no. 2, pp. 259–285, Oct. 2020, doi: 10.3390/iot1020016.
- [17] N. A. F. Abbas, N. Abdulredha, R. K. Ibrahim, and A. H. Ali, “Security and imperceptibility improving of image steganography using pixel allocation and random function techniques,” *International Journal of Electrical and Computer Engineering*, vol. 12, no. 1, pp. 694–705, Feb. 2022, doi: 10.11591/ijece.v12i1.pp694-705.
- [18] F. Mallouli, A. Hellal, N. S. Saeed, and F. A. Alzahrani, “A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms,” in *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, IEEE, Jun. 2019, pp. 173–176, doi: 10.1109/CSCloud/EdgeCom.2019.00022.
- [19] R. F. A. -Kader, S. H. El-Sherif, and R. Y. Rizk, “Efficient two-stage cryptography scheme for secure distributed data storage in cloud computing,” *International Journal of Electrical and Computer Engineering*, vol. 10, no. 3, pp. 3295–3306, Jun. 2020, doi: 10.11591/ijece.v10i3.pp3295-3306.
- [20] W. A. Awadh, A. S. Alasady, and A. K. Hamoud, “Hybrid information security system via combination of compression, cryptography, and image steganography,” *International Journal of Electrical and Computer Engineering*, vol. 12, no. 6, pp. 6574–6584, Dec. 2022, doi: 10.11591/ijece.v12i6.pp6574-6584.
- [21] T. L. Prasanna, N. Siddaiah, B. M. Krishna, and M. R. Valluri, “Implementation of the advanced encryption standard algorithm on an FPGA for image processing through the universal asynchronous receiver-transmitter protocol,” *International Journal of Electrical and Computer Engineering*, vol. 12, no. 6, pp. 6114–6122, Dec. 2022, doi: 10.11591/ijece.v12i6.pp6114-6122.
- [22] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson, 2017.
- [23] D. K. Sharma, N. C. Singh, D. A. Noola, A. N. Doss, and J. Sivakumar, “A review on various cryptographic techniques & algorithms,” *Materials Today: Proceedings*, vol. 51, pp. 104–109, 2022, doi: 10.1016/j.matpr.2021.04.583.
- [24] Y. Alemami, M. A. Mohamed, and S. Atiewi, “Advanced approach for encryption using advanced encryption standard with chaotic map,” *International Journal of Electrical and Computer Engineering*, vol. 13, no. 2, pp. 1708–1723, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1708-1723.
- [25] S. M. Hassan and G. G. Hamza, “Real-time FPGA implementation of concatenated AES and IDEA cryptography system,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 1, Apr. 2021, doi: 10.11591/ijeecs.v22.i1.pp71-82.
- [26] S. K. Singh, D. P. K. Manjhi, and D. R. K. Tiwari, “Data Security using RSA Algorithm in Cloud Computing,” *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, no. 8, pp. 11–16, 2016, doi: 10.17148/IJARCC.2016.5803.
- [27] M. AbuTaha, M. Farajallah, R. Tahboub, and M. Odeh, “Survey Paper: Cryptography Is The Science Of Information Security,” *International Journal of Computer Science and Security (IJCSS)*, vol. 5, no. 3, pp. 298–309, 2011.
- [28] M. Preetha and M. Nithya, “A Study And Performance Analysis of RSA Algorithm,” *International Journal of Computer Science and Mobile Computing*, vol. 2, no. 6, pp. 126–139, 2013.
- [29] L. Alliance, “The Things Network.” <https://www.thingsnetwork.org/docs/lorawan/security/> (accessed Oct. 26, 2021).
- [30] F. Marlind and I. Butun, “Activation of LoRaWAN End Devices by Using Public Key Cryptography,” in *2020 4th Cyber Security in Networking Conference, CSNet 2020*, IEEE, Oct. 2020, pp. 1–8, doi: 10.1109/CSNet50428.2020.9265530.
- [31] A. Zourmand, A. L. Kun Hing, C. Wai Hung, and M. Abdulrehman, “Internet of Things (IoT) using LoRa technology,” in *2019 IEEE International Conference on Automatic Control and Intelligent Systems, I2CACIS 2019 - Proceedings*, IEEE, Jun. 2019, pp. 324–330, doi: 10.1109/I2CACIS.2019.8825008.
- [32] J. VenkataGiri and A. Murty, “Elliptical Curve Cryptography Design Principles,” 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), Bangalore, India, 2021, pp. 889–893, doi: 10.1109/RTEICT52294.2021.9573662.
- [33] S. Seniman, B. Siregar, R. M. Pelle, and F. Fahmi, “Securing sensor data transmission with ethernet elliptic curve cryptography secure socket layer on STM32F103 device,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 1, pp. 507–515, Apr. 2021, doi: 10.11591/ijeecs.v22.i1.pp507-515.
- [34] M. A. Alazzawi, M. T. Almalchy, A. Al-Shammari, A. S. Al-Khaleefa, and H. M. Albehadili, “LSKA-ID: A lightweight security and key agreement protocol based on an identity for vehicular communication,” *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 21, no. 4, pp. 784–796, Aug. 2023, doi: 10.12928/TELKOMNIKA.v21i4.24388.
- [35] M. Parmar and P. Shah, “Internet of things-blockchain lightweight cryptography to data security and integrity for intelligent application,” *International Journal of Electrical and Computer Engineering*, vol. 13, no. 4, pp. 4422–4431, Aug. 2023, doi: 10.11591/ijece.v13i4.pp4422-4431.
- [36] M. S. Jabbar and S. S. Issa, “A crypto-steganography healthcare management: Towards a secure communication channel for data COVID-19 updating,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 29, no. 2, pp. 1102–1112, Feb. 2023, doi: 10.11591/ijeecs.v29.i2.pp1102-1112.
- [37] T. H. Hameed and H. T. Sadeeq, “Modified Vigenère cipher algorithm based on new key generation method,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 28, no. 2, pp. 954–961, Nov. 2022, doi: 10.11591/ijeecs.v28.i2.pp954-961.
- [38] A. S. Abd and E. A. R. Hussein, “Design secure multi-level communication system based on duffing chaotic map and steganography,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 25, no. 1, pp. 238–246, Jan. 2022, doi: 10.11591/ijeecs.v25.i1.pp238-246.

BIOGRAPHIES OF AUTHORS






Eyad M. Hamad    is an associate professor at the German Jordanian University, specializing in biomedical engineering. His areas of expertise include BioMEMS techniques, lab-on-a-chip systems, point-of-care diagnostics, semiconductor fabrications, microfluidics, bioinformatics, and sensor applications. He is an active member of prestigious associations such as IEEE EMBS, Jordan Engineer Association (JEA), Institute of Engineering and Technology (IET) UK, and VDI Germany. Throughout his academic and professional journey, he has consistently demonstrated a commitment to excellence, pushing the boundaries of knowledge in biomedical engineering. His research endeavors have resulted in numerous publications in esteemed scientific journals and conferences, contributing to the advancement of biomedical engineering and fostering collaborations. He is dedicated to teaching and mentoring the next generation of engineers. He can be contacted at email: eyad.hamad@gju.edu.jo.






Samer Alabed    is currently an associate professor and the Head of Department of Biomedical Engineering at the German Jordanian University, Jordan. He was an associate professor of Electrical Engineering at the College of Engineering and Technology in the American University of the Middle East (AUM), Kuwait, from 2015 to 2022. He also worked in Darmstadt University of Technology, Darmstadt, Germany, from 2008 to 2015. He received his Ph.D. degree in electrical engineering and information technology from Darmstadt University of Technology, Germany. During the last 18 years, he has worked as an associate professor, assistant professor, researcher, and lecturer in several German and Middle East universities and supervised tens of master students and several Ph.D. students. He received several awards and grants from IEE, IEEE, DAAD, DFG, ERC, EU, AUM. He was invited to many conferences and workshops in Europe, US, and North Africa. Further information is available on his homepage: <http://drsamerlabed.wixsite.com/samer>. He can be contacted at email: samer.alabed@gju.edu.jo.



Amer Alsaraira    holds a PhD in Biomedical Engineering from Monash University since the year 2009. He is currently an assistant professor at Biomedical Engineering Department at German Jordanian University-Jordan since 9/2022. Alsaraira also worked as an assistant professor at the Department of Electrical Engineering at the American University of Middle East (AUM) – Kuwait, for the period between 8/2019-9/2022 and worked as an assistant professor at Biomedical Engineering Department at Hashemite University-Jordan for the period between 12/2009 and 9/2019. He is teaching various courses for the undergraduate students, supervising their graduation projects, supervised undergraduate students, and a member of many committees at the department. He participated in many training workshops to support the university efforts toward gaining ABET accreditation. His current research is in the fields of modeling and simulation of biomedical systems, wireless networks, and DSP. He can be contacted at email: Amer.Alsaraira@gju.edu.jo.



Omar A. Saraereh    received the B.S. degree in Telecommunication Engineering from Mutah University, Jordan, in 1999, the M.Sc. degree in Digital Communication Systems in U.K., and the Ph.D. degree in Electrical and Electronic Engineering from Loughborough University, U.K., in 2005. From 2001 to 2005, he was a member of staff with the Centre for Mobile Communication Research, Loughborough University. He has more than 17 years of academic and practical experience in electrical engineering, mobile communications, various antennas design, fabrication and measurements, radiation hazards and health effects, and wireless communications. He was a high-level consultant and a turnkey solution originator in countless business and charitable sectors, and an international public speaker and a trainer on a variety of business and people management topics. He is currently a full professor with the Department of Electrical Engineering, Hashemite University, Jordan. He has published many articles in various international journals and conferences. He can be contacted at email: eloas2@hu.edu.jo.